

2014

ENHANCING USABILITY USING AUTOMATED SECURITY INTERFACE ADAPTATION (ASIA)

ZAABA, ZARUL FITRI

<http://hdl.handle.net/10026.1/3025>

<http://dx.doi.org/10.24382/3201>

Plymouth University

All content in PEARL is protected by copyright law. Author manuscripts are made available in accordance with publisher policies. Please cite only the published version using the details provided on the item record or document. In the absence of an open licence (e.g. Creative Commons), permissions for further reuse of content should be sought from the publisher or author.

COPYRIGHT STATEMENT

This copy of the thesis has been supplied on condition that anyone who consults it is understood to recognise that its copyright rests with its author and that no quotation from the thesis and no information derived from it may be published without the author's prior consent.

**ENHANCING USABILITY USING
AUTOMATED SECURITY INTERFACE ADAPTATION
(ASIA)**

by

ZARUL FITRI ZAABA

A thesis submitted to Plymouth University
in partial fulfilment for the degree of

DOCTOR OF PHILOSOPHY

School of Computing and Mathematics
Faculty of Science and Environment

APRIL 2013

Abstract

Enhancing Usability using Automated Security Interface Adaptation (ASIA)

Zarul Fitri Zaaba
BIT (Hons), MSc

Many users are now significantly dependent upon computer application. Whilst many aspects are now used very successfully, an area in which usability difficulties continue to be encountered is in relation to security. Thus can become particularly acute in situations where users are required to interact and make decisions, and a key context here is typically when they need to respond to security warnings.

The current implementation of security warnings can often be considered as an attempt to offer a one size fits all solution. However, it can be argued that many implementations are still lacking the ability to provide meaningful and effective warnings. As such, this research focuses upon achieving a better understanding of the elements that aid end-users in comprehending the warnings, the difficulties with the current approaches, and the resulting requirements in order to improve the design and implementation of such security dialogues.

In the early stage of research, a survey was undertaken to investigate perceptions of security dialogues in practice, with a specific focus upon security warnings issued within web browsers. This provided empirical evidence of end-users' experiences, and revealed notable difficulties in terms of their understanding and interpretation of the security interactions.

Building upon this, the follow-up research investigated understanding of application level security warnings in wider contexts, looking firstly at users' interpretation of what constitutes a security warning and then at their level of comprehension when related warnings occurred. These results confirmed the need to improve the dialogues so that the end-users are able to act appropriately, and consequently promoted the design and prototype implementation of a novel architecture to improve security warnings, which has been titled *Automated Security Interface Adaptation (ASIA)*.

The ASIA approach aims to improve security warnings by tailoring the interaction more closely to individual user needs. By automatically adapting the presentation to match each user's understanding and preferences, security warnings can be modified in ways that enable users to better comprehend them, and thus make more informed security decisions and choices.

A comparison of the ASIA-adapted interfaces compared to standard versions of warnings revealed that the modified versions were better understood. As such, the ASIA approach has significant potential to assist (and thereby protect) the end-user community in their future interactions with security.

Table of Contents

Abstract	i
List of Figures.....	vii
List of Tables.....	xiii
Glossary of Abbreviations.....	xvii
Acknowledgement	xix
Author's Declaration.....	xxi
1 Introduction and Overview	3
1.1 Motivation.....	3
1.2 Objectives of the Research.....	4
1.3 Structure of thesis	5
2 Users Interaction with Security Tools and Technologies.....	9
2.1 An overview of security tools and technologies.....	9
2.2 Security and usability.....	10
2.2.1 Usability problems.....	12
2.2.2 End-users Perception and trust	16
2.3 Human Computer Interaction (HCI) and the Graphical User Interface (GUI)	18
2.4 The needs for understanding usability for security and protection contexts....	19
2.7 Guidelines	24
2.7.1 Purpose of warnings	25
2.8 Warnings in computer contexts	27
2.9 Problems and issues with security warnings	29
2.9.1 Attention towards warnings	31
2.9.2 Understanding of warnings	32
2.9.3 Use of technical wording	33
2.9.4 Evaluation of risks from warnings.....	33
2.9.5 User's motivation towards heeding warnings	34
2.9.6 Users' assessments of the implication of warnings	34
2.10 Gathering Evidence on the need for research into security warnings	34
2.11 Overview of warnings process and other frameworks	35
2.11.1 Communication-Human Information Processing (C-HIP)	37
2.11.2 Human in the Loop (HITL).....	38
2.11.3 Security automation for security warnings	41
2.11.4 System visualisation for security warnings.....	42
2.12 Evolution of security warnings studies	43
2.12.1 Improving the usability aspects of security warnings design.....	43
2.12.2 Related approaches to improve security warnings design	45
2.13 The classification of security warnings approaches	48
2.14 Warnings potential directions	50
2.15 Study approach.....	58
2.16 Conclusions.....	60
3 Examination of Comprehensibility of Issues in Information Security.....	65
3.1 Introduction	65
3.2 Methodology	66

3.3	Study design	68
3.3.1	Study participants	69
3.3.2	Section 1: Background and demographic	69
3.3.3	Section 2: General usage of computer and operating systems	71
3.3.4	Section 3: Usability and protection.....	77
3.3.5	Section 4: computer scenario study	89
3.4	Feedback comments.....	93
3.5	Discussion	94
3.6	Constraints.....	96
3.7	Conclusions	96
4	A Wider Evaluation of Perceived Security Warnings.....	99
4.1	Introduction	99
4.2	Methodology.....	100
4.3	Study Design	101
4.4	Questionnaire.....	101
4.4.1	Study Protocol	103
4.4.2	Study Participants	105
4.5	Results and findings	105
4.5.1	Classification of security warnings contexts.....	108
4.5.2	Misinterpreted scenarios	109
4.5.3	Results of classification	111
4.6	Users' feedback	123
4.7	Discussions	124
4.8	Constraints.....	125
4.9	Conclusions	125
5	Further Appraisal of Security Warnings in Real-Time Contexts.....	129
5.1	Motivation	129
5.2	Methodology.....	130
5.3	Study design	132
5.3.1	Survey	132
5.3.2	Study protocol	133
5.3.3	Study Participants	134
5.4	Results and findings.....	135
5.4.1	User interaction with various dialogue boxes	137
5.4.2	Conflicts with guidelines scenarios	139
5.4.3	Consistency of warning dialogues	141
5.5	Feedback comments.....	149
5.6	Constraints.....	150
5.7	Discussions	151
5.8	Focus and direction of study.....	152
5.9	Conclusions	154
6	A Novel Architecture for Automated Security Interface Adaptation (ASIA)	157
6.1	Introduction	157
6.2	Related Works	158
6.3	A novel architecture of security warnings.....	160
6.4	Process Algorithm.....	163

6.5	General Functionality descriptions	166
6.6	Processing Engines and storage.....	168
6.6.1	Engine Manager.....	168
6.6.2	Adaptation Engine	172
6.6.3	Databases	178
6.7	Conclusions	181
7	Evaluation and Validation of the Automated Security Interface Adaptation (ASIA) prototype	185
7.1	Introduction	185
7.2	Methodology	186
7.3	Study Design	187
7.4	Results and findings.....	189
7.4.1	Users' preferences in the experimental tasks (i.e. 7 tasks)	192
7.4.2	The adapted warning.....	207
7.4.3	Post-Trial Questionnaires and Interviews	210
7.4.4	Comparison of the standard security warning and the adapted warning	228
7.5	Final observations.....	250
7.5.1	Automated Security Interface Adaptation aims – Validation	251
7.5.2	Usable help technique – Validation.....	252
7.6	Discussions.....	257
7.7	Constraints.....	260
7.8	Conclusions	261
8	Conclusion and Future Work.....	265
8.1	Achievements of research	265
8.2	Limitations of the research.....	266
8.3	Suggestions for future work.....	268
8.4	The future of security warnings.....	269
	References	273
	Appendix A	287
	Appendix B.....	315
	Appendix C.....	329
	Appendix D	343
	Appendix E.....	377

List of Figures

Figure 2.1: Windows Firewall settings (Furnell et al. 2006)	13
Figure 2.2: Security warning in Internet Explorer that used a complex language (Furnell et al. 2006).....	13
Figure 2.3: PGP keys display where users unable to correctly sign and encrypt e-mail in a specified task (Whitten & Tygar 1999).....	14
Figure 2.4: Behind the scene of Sesame where user able to view the process before making a security decision (Stoll et al. 2008)	21
Figure 2.5: The active Firefox 2 phishing warning (Egelman et al. 2008)	22
Figure 2.6: The passive Internet Explorer 7 phishing warning (Egelman et al. 2008) ...	23
Figure 2.7: Hazard Control hierarchy	26
Figure 2.8: Examples of warnings in various contexts of user interface	29
Figure 2.9: Four main components of warning process via repetition variables (Originally derived from Rogers et al. 1999)	36
Figure 2.10: Communication-Human Information Processing Framework (C-HIP) based on Wogalter et al. (1999).....	37
Figure 2.11: Human in the Loop security framework (HITL) by (Cranor, 2008).....	38
Figure 2.12: Human threat identification and mitigation process originally by (Cranor 2008)	40
Figure 2.13: The Spectrum of automation approaches	41
Figure 2.14: The original File Download dialogue (Nodder, 2005).....	43
Figure 2.15: Redesigned File Download dialogue (Nodder, 2005).....	44
Figure 2.16: Five types of dialogues boxes namely warn and continue, multiple choices, security training, blank filling and clarification (Keukelaere et al. 2009).	46
Figure 2.17: Classifications approaches to improve the security warnings	49
Figure 2.18: Amendments of human threat identification and mitigation process	59
Figure 3.1: Age profile of the respondent group	69
Figure 3.2: Respondents by educational background	70
Figure 3.3: Computing experience	70
Figure 3.4: Level of concern on computer security	71
Figure 3.5: Primary operating system.....	72

Figure 3.6: Concern on updating operating system	73
Figure 3.7: Method to update their operating system	73
Figure 3.8: Usage on types of security software products	76
Figure 3.9: Preferred web browser.....	77
Figure 3.10: Reason on difficulty to understand the security warning	79
Figure 3.11: Belief regarding the security warning that appeared.....	80
Figure 3.12: Experienced with malware/threats	81
Figure 3.13: Behaviour towards the usage of computer security through the possibility of becoming a victim of malicious attack or cybercrime	82
Figure 3.14: Usage of security applications in their computers	83
Figure 3.15: Users' claimed using Internet security package vs. claimed installed security applications.....	84
Figure 3.16: Method of updating their anti-malware tools	85
Figure 3.17: Level of concern on updating their anti-malware protection tools.	85
Figure 3.18: Screenshot from various web browsers showing a security warning having detected a possible phishing website.	87
Figure 3.19: Security pop up according to various of web browsers.....	90
Figure 3.20: Point of view on other information that should be in the security warning.	92
Figure 3.21: Level of concern after completing the questionnaire	92
Figure 4.1: Questionnaire section	102
Figure 4.2: 5 likert-scales measurement with 10 questions.....	103
Figure 4.3: Notification upon successful captured every security warning	103
Figure 4.4: Dialogues that were misclassified as security warnings	110
Figure 4.5: The most popular captured security warning demonstrated by respondents.	116
Figure 4.6: In-place security warning contexts captured by respondents	119
Figure 4.7: The average respondents' on answered questionnaire in notifications contexts.....	121
Figure 4.8: The average respondents' on answered questionnaire in banners contexts.	122
Figure 4.22: Responses to phishing warning – Mozilla Firefox.....	310
Figure 4.23: Responses to phishing warning – Internet Explorer 8.....	310
Figure 4.24: Responses to phishing warning – Internet Explorer 7.....	310

Figure 4.25: Responses to phishing warning – Opera	311
Figure 4.26: Responses to phishing warning – Safari	311
Figure 4.27: Responses to phishing warning – Chrome	311
Figure 4.28: Internet Explorer 8 Security pop up respondents’ decisions	312
Figure 4.29: Internet Explorer 7 Security pop up respondents’ decisions	312
Figure 4.30: Mozilla Firefox Security pop up respondents’ decisions	312
Figure 4.31: Opera Security pop up respondents’ decisions	313
Figure 4.32: Safari Security pop up respondents’ decisions	313
Figure 4.33: Chrome Security pop up respondents’ decisions	313
Figure 5.1: Notification appeared once the software was installed	133
Figure 5.2: Custom dialogue box	134
Figure 5.3: Conflicts on security warning features.....	140
Figure 5.4: Consistency of security warnings	141
Figure 5.5: Security warning from Microsoft Outlook.....	145
Figure 5.6: Security warning to opening file in Google Chrome	145
Figure 5.7: Security warning on downloading file from Mozilla Firefox	146
Figure 5.8: Security warning once users execute the save file on computer	146
Figure 5.9: Security warning from Mozilla Firefox	147
Figure 5.10: Security warning whilst opening link from Microsoft Office	147
Figure 5.11: Security warning to view webpage	147
Figure 5.12: Security warnings with complicated information.....	149
Figure 5.9: Managing tasks using computer	328
Figure 5.10: Satisfaction on layout of security warning	328
Figure 5.11: Level of concern for computer security.	328
Figure 6.1: The architecture of Automated Security Warning Interface Adaptation (ASIA).....	163
Figure 6.2: Overall Process Algorithm	164
Figure 6.3: Engine Manager	169
Figure 6.4: Adaptation Engine	173
Figure 6.5: Table representation in User Support Data (USD)	178
Figure 6.6: Tables representation in Decision Risk Data (DRD).....	179
Figure 6.7: Tables representation in Community Decision Data	180

Figure 7.1: Task 1 security warning	193
Figure 7.2: Task 2 security warning	193
Figure 7.3: Task 3 security warning	193
Figure 7.4: Task 4 security warning	193
Figure 7.5: Task 5 security warning	194
Figure 7.6: Task 6 security warning	194
Figure 7.7: Task 7 security warning	195
Figure 7.8: Dialogue enhancement notification.....	196
Figure 7.9: Repeated task	197
Figure 7.10: The simplified security warning	197
Figure 7.11: The adapted warning.	204
Figure 7.12: Help dialogue box	205
Figure 7.13 : Simplified security warning details	205
Figure 7.14: The adapted warning details	208
Figure 7.15: Questionnaires and interviews in section 3	211
Figure 7.16: Standard security warning	213
Figure 7.17: Likert-scales range (i.e. 1 to 7)	214
Figure 7.18: Comparison between standard vs. security warning enhancement.....	224
Figure 7.20: Demographic comparison age and education background (n = 30).....	229
Figure 7.21: Users' performance score on 10 questions with regard to the standard security warning.....	232
Figure 7.22: Users' performance score on 10 questions with regard to the adapted warning.....	232
Figure 7.23: Comparison of "The security dialogue was too complex for me to understand"	234
Figure 7.24: Comparison of "I spent enough time to view the information provided"	235
Figure 7.25: Comparison of "It was easy to understand the information provided"	236
Figure 7.26: Help dialogue box in Windows XP (A) and in Windows 7 (B)	237
Figure 7.27: Comparison of "The way information was presented helped me to complete the tasks"	238
Figure 7.28: Comparison of "I could effectively complete my task using the information presented"	238
Figure 7.29: Comparison of "It was easy to find the information I needed"	239
Figure 7.30: Comparison of "The interface of security dialogue was understandable"	240

Figure 7.31: Comparison of “The security dialogue helped me to fix the problem in the way that I understood” 241

Figure 7.32: Comparison of “The available help increased my knowledge and awareness about the contents and features of the dialogue” 242

Figure 7.33: Comparison of “This dialogue had all the functionality and capability I expected it to have” 242

List of Tables

Table 2.1: Five different user interface warning contexts.....	28
Table 2.2: The main components based on Human in the loop security framework (HITL) by Cranor (2008).	39
Table 2.3: Summary of studies on how to improve security warnings.....	52
Table 2.4: Common problems with security warnings and proposed solutions.....	53
Table 2.6: Human threat identification and mitigation with the propose study	60
Table 3.1: Preferred security vendor.....	75
Table 3.2: Comparison of the security warnings from various web browsers (Zaaba et al. 2011)	88
Table 4.1: Summary table of user study 2.....	108
Table 4.2: Comparison table on education level and computing skills	111
Table 4.3: Respondents' event name classification based on the captured security warnings	113
Table 4.4: The mean respondents on answered questionnaire in dialogue box contexts.	115
Table 4.5: Mean value of security warning A based on the likert-scale.....	116
Table 4.6: Mean value on security warning B.....	117
Table 4.7: Mean value of security warning D	117
Table 4.8: Mean value on security warning E.....	118
Table 4.9: Mean value on security warning F.....	118
Table 4.10: The mean respondents' on answered questionnaire in in-place contexts..	119
Table 4.11: Design pattern for notification in Microsoft	120
Table 4.12: The mean respondents' on answered questionnaire in notification contexts.	120
Table 4.13: The mean respondents' on answered questionnaire in banners contexts. .	122
Table 4.14: The mean respondents' on answered questionnaire in balloon contexts...	123
Table 5.1: Example of Class Name and Application name from three web browsers .	130
Table 5.2: Respondents demographic background.....	137
Table 5.3: Results of the classification of dialogue box based on application name ...	139

Table 5.4: Comparison on the features of the warnings.....	143
Table 6.1: Three phases of checking.....	164
Table 6.2: General description about the entities in ASIA architecture	168
Table 6.3: Record in USD	170
Table 6.4: Tooltips detail from USD	174
Table 6.5: Tooltips detail from DRD	174
Table 6.6 : Matching icon and word from DRD.....	174
Table 6.7: Risk level bar from DRD	175
Table 6.8: Combination of user preference based on List preferences	176
Table 6.9: Details on guidance area (USD).....	176
Table 6.10: Details on guidance area (DRD)	176
Table 6.11: History information based on what others have done (CDD).....	177
Table 6.12: Statistics information based on the type of warning message	177
Table 6.13: Statistics information based on <i>Security Warning Enhancement</i>	178
Table 7.1: Summary table of demographic user study 4.....	192
Table 7.2: Users' decision upon receiving simplified security warning.....	198
Table 7.3: Reasons on choosing Run option	199
Table 7.4: Reasons on choosing Help	200
Table 7.5: Reason on choosing Cancel	200
Table 7.6: Features that help users to understand the security warning enhancement.	201
Table 7.7: Satisfaction with the information provided	202
Table 7.8: Comparison of availability of features between standard security warning and simplified security warning.	206
Table 7.9: Description of additional features available on the simplified security warning.....	207
Table 7.10: Description of the adapted warning.....	210
Table 7.11: Users decision with regard to the type of problems based on standard security warning.....	214
Table 7.12 : Statistics on users' decision with regard to standard security warning	215
Table 7.13: What do you think will happen if you click run?.....	216
Table 7.14: What do you think of the feature(s) that are available to help you make a decision in this security warning?.....	217

Table 7.15: Were there any aspects of the warning that you found hard to understand or interpret?	218
Table 7.16: Do you understand the way information was presented especially with technical wording?.....	218
Table 7.17: Do you feel that this security warning was presented with enough options to guide you?	219
Table 7.18: Do you feel satisfied with help available for this warning?	219
Table 7.19: Results on security warning enhancement based on users' preferences (classification)	221
Table 7.20: Users decision with regard to the type of problems based on security warning enhancement (preferences)	222
Table 7.21: Statistics on users' decision with regard to security warning enhancement	224
Table 7.22: What do you think of the feature(s) that are available to help you make a decision in this security warning?.....	225
Table 7.23: Were there any aspects of the warning that you found hard to understand or interpret?	226
Table 7.24: Do you understand the usage of signal icon/signal words in this security warning?.....	226
Table 7.25: Do you understand the way information was presented, especially technical wording?.....	227
Table 7.26: Do you feel that this security warning was presented with enough options to guide you?	227
Table 7.27: Do you feel satisfied with help available for this warning?	228
Table 7.28: Comparison table between pre-warning (standard) and post-warning (adapted).....	231
Table 7.29: Comparison of usability elements and users' preferences.....	244
Table 7.30: The reasons on choosing the adapted warning (effectiveness)	245
Table 7.31: The reasons on choosing the adapted warning (efficiency).....	245
Table 7.32: The reasons on choosing enhancement security warning (user satisfaction)	246
Table 7.33: The reasons on choosing enhancement security warning (preference)	248
Table 7.34: 4 users' decisions on usability set of questions.....	248
Table 7.35: Other suggestions to improve security warnings in general	249
Table 7.36: Aims of ASIA validation	251

Table 7.37: Comparison of which user questions can be answered by which user help technique (adapted from Herzog and Shahmehri (2007)) 253

Table 7.38: Details of evaluation and validation 255

Table 7.39: Comparison of security warnings based on the availability of 10 questions. 257

Glossary of Abbreviations

ANSI	American National Standard Institute
ASD	Adaptive Security Dialogs
BBC	British Broadcast Corporation
C	Total of Column
C-HIP	Communication –Human Information Processing
CA	Certificate Authority
CDD	Community Decision Data
CRA	Computing Research Association
CSCAN	Centre for Security, Communication and Network Research
DF	Degree of Freedom
DLL	Dynamic Link Library
DRD	Decision Risk Data
E	Enhance Warning frequency
FHSA	Federal Hazardous Substances Act
FIFRA	Federal Insecticide, Fungicide and Rodenticide Act
GCSE	General Certificate Secondary Education
GUI	Graphical User Interface
HO	Null Hypothesis
HCI	Human Computer Interface
HITL	Human in the Loop
HSI	Human Systems Interaction
HTTPS	Hypertext Transfer Protocol Secure
ICT	Information, Communications and Technology
ISAS	International Student Advisory Service
O	Standard Warning Frequency
PGP	Pretty Good Privacy
PI	Principal Investigator
R	Total of Row
SRAs	Security Reinforcing Applications
SSL	Secure Socket Layers
USD	User Support Data
WWW	World Wide Web
X ²	Chi-Square

Acknowledgement

I am praise to the Almighty god for giving me the strength and courage throughout completing my studies at Plymouth University. I would like to thank all of the people who have continuously supported me in pursuing this journey of a PhD.

First and foremost, my sincere appreciation and gratitude to my supervisors, Prof. Steven M. Furnell and Assoc. Prof. Paul Dowland for their support, commitment and guidance throughout the completion of this thesis. They provided direction for the work and ensured the best opportunities were always available.

A special acknowledgement to the Ministry of Higher Education (MOHE) Malaysia in collaboration with the University Sains Malaysia for the scholarship that has been awarded to me to make this thesis possible.

To all of my colleagues and staff members in Centre for Security, Communication and Network Research (CSCAN) Plymouth University, friends and others, thank you so much for your helpful advice and continuous support. You all have been a great family to me during my time here.

This thesis is especially dedicated to my family members, Rokiah bt Akop, Zaaba bin Shamsudin, Zalifatul Akmal bt Zaaba and Nurshazwani bt Zaaba. Their love and full support always make me to believe in myself and to become a better person and therefore able to complete this thesis.

Author's Declaration

At no time during the registration for the degree of Doctor of Philosophy has the author been registered for any other University award without prior agreement of the Graduate Committee. Work submitted for this research degree at the Plymouth University has not formed part of any other degree either at Plymouth University or at another establishment. This study was financed by the Ministry of Higher Education (MOHE) Malaysia in collaboration with University Sains Malaysia (USM). Relevant scientific seminars and conferences were regularly attended at which work was often presented; external institutions were visited for consultation purposes and several papers prepared for publication.

Word count of main body of thesis: 70 261 words

Signed: _____

Date: _____

CHAPTER 1

Introduction and Overview

1 Introduction and Overview

1.1 Motivation

Computer technology is continually evolving. Simultaneously, threats continue to propagate, targeting end users at home or within organizations. People realise on these technologies to make their life easier by any possible means. They are now creating a dependency chain in day to day life with computer system and network. In the era of 80's and 90's, people went directly to stores or banks to get things such as kitchen appliances, paying utilities bill, banking transaction and shopping. Today, these activities may be undertaken using computer technologies. However, while the invention is highly beneficial, the use of the computer may potentially cause harm to users if they do not know how to use it in a secure manner (Dourish & Anderson 2006). For instance, during online transactions, to purchase something from the website, users enter their personal details like credit card number and security codes. The issue raised here is that information may be hacked by attackers during transmission on the Internet, users might log in to another website via e-mail or link which leading them to phishing attacks, malware attacks and others. In this context, end users are the main subjects who use the computer. They might not know the consequences of this event unless they realize them, and appreciate the risks that they are facing now (Besnard & Arief 2004). Whilst security in computer systems in organization is managed by the organization's policies, protection for other general users such as at home is left to their own initiative. Users with knowledge and capabilities might know how to conceive of security matter to achieve better protection whereas for the laymen, they might know nothing if any impediments occurs on their current system. Users always say that they understand the security features with regards to information security; however, in real life they still failed to demonstrate their understanding. End users in general are not experts and they have a very general understanding of computers, but are unlikely to be familiar with most facets of security features and security technologies. Therefore, it is essential to understand the interaction between usability and information security in order to make users know how to make a security decision, to differentiate between possible menaces towards and to minimize the risk of possibly becoming a victim of such attacks.

In order for users to use security features correctly, to understand the computer interface and to manage their computer properly, all of the features represented must be usable

and users' friendly. Thus, in order to achieve that level is a challenging task (Folmer& Bosch 2004, Dickinson et al. 2003 and Bødker 2006). Using the established principles of Human Computer Interaction (HCI) helps to make the computer system easy to use by finding some methods and processes to design interfaces (Carrol 2003). This issue is raised as many users are still unable to demonstrate the effectiveness of computer security as a whole process. Computer security is not just a technical issue. The success of security is also dependent on the effective behaviour of users (Stanton et al. 2003). Understanding their actions is thus both needed and necessary. The impetus of this study is the fact that there are still some users who are not heeding on these issues and decide to opt out from doing anything (Furnell 2005 and Furnell 2005b). Various types of computer threat (e.g. virus, worms, spyware and rootkits) may cause catastrophic results for users' assets. A well devised action is essential in understanding how to deal with the issues. Nevertheless, the challenging part here lies in the fact that users are responsible for their own system. This means they simply cannot place the burden of responsibility on others. One key factor in effective containment is based on the actions, attitudes and perception of people. Therefore understanding the interaction between users and security tools and technologies is essential. These tools (e.g. antivirus and firewall) are used to provide security and protection for users. Since most of the applications, operating systems and web browsers use these tools; this indicates an attention to understanding the medium of interaction being used to deliver the message and information to end-users.

1.2 Objectives of the Research

This study aims to understand and improve upon the usability aspects of security warnings. It focuses in particular on issues relating to the security warning interface, and specifically focuses on initial investigation of issues of security and usability of security warning, assessing users' experience of encountering warnings, and proposing architecture to improve security warnings. Thus, the web security warnings dialogues will be used as a focal point to evaluate and validates the proposed architecture. The full objectives of the research programme may be more formally listed as follows:

- i. To establish the key usability issues relating to end-user interaction with security tools and technologies.

- ii. To investigate the specific context of security warnings and experimentally assess the associated challenges of user perceptions and understanding.
- iii. To design a means of improving and enhancing the usability of security warnings based upon user feedback.
- iv. To evaluate the proposed approach by means of a prototype implementation.

These objectives correspond to the general sequence of the material presented in the subsequent chapters of the thesis, as will be discussed in the next section.

1.3 Structure of thesis

This thesis describes the research that leads to a better way to understand and to improve usability of security warnings. The investigation begins at the general level, encompassing all aspects of information security considerations that are applicable to security warnings, before proceeding to identify a more specific technical approach and describing the conduct of practical evaluation. This thesis comprises nine chapters, the details of which are as follows:

Chapter 2 discusses users' interactions with security tools and technologies. The security, usability, trust, relationship between HCI and GUI are discussed in further detail. Then it reviews the warning research background and approaches from other scholars. It presents the warning contexts and processes, as well as the problems and issues of warnings implementation, approaches to warning studies and finally, the direction of this thesis.

Chapter 3 provides an examination of comprehensibility of issues in information security, using a survey study. Moreover, it provides general insights into the solid foundation to assess end-users' views about information security aspects in general. It also comprises 2 main warning scenarios to better understand users' perception and decision upon receiving these warnings.

Chapter 4 proceeds with wider evaluation of perceive security warnings, where users have the opportunity to capture what they believe a security warning to be (i.e.

capturing manually using installed application). A questionnaire is embedded together in the application to gather useful information from users.

Chapter 5 builds from the previous chapter to further appraise computer warnings in real-time contexts. It gathers the need to provide more information on each warning presented. Moreover, it supports the previous evidences and later leads to the creation of proposed architecture in the next chapter.

Chapter 6 proposes Automated Security Warning Interface (ASIA) architecture, a novel framework in improving security warnings. It describes the components and databases involved and describes in detail each of the functions. This chapter reveals how adaptation takes place in user's computers and the detailed interaction between the entities involved.

Chapter 7 evaluates and validates the proposed ASIA architecture, using a prototype system. It makes use of interview and questionnaire techniques to probe end-users' understanding and preferences in terms of the warnings presented. Details analysis is conducted in this chapter. A detailed comparison will be made to focus on the usability aspects of warnings, based upon users' experiences of the warnings presented to them. In addition, the results highlight the detailed interview process on user's decision process, with the warnings that they encounter (i.e. reasons for their actions, their understanding, difficulty levels).

Finally, Chapter 8 summarises findings from the earlier chapters, highlighting the future development of this research.

This thesis also includes a number of appendices, containing a variety of additional information in supporting the main discussions. This includes the research publications used throughout the completion of this research study.

CHAPTER 2

Users Interaction with Security Tools and Technologies

2 Users Interaction with Security Tools and Technologies

2.1 An overview of security tools and technologies

Security tools and technologies are used to provide significant protection to end-users whilst using computer. In order to cope with technological change, there is a need for people to strengthen their related knowledge and skills so that they are able to manage technology accordingly. Computers have now become the medium of communication in the cyber world. Applications that are installed in computers provide many functions to cater specifically for user needs in terms of the tasks they need to resolve. For instance, antivirus software is one of the most popular tools that end-users dealing with on day to day basis. In order to use this tool, users need to understand how it works, so that it can be used in a secure manner. Antivirus software is generally a piece of software that is installed to protect end-users, and functions as a shield from any computer menace (i.e. potential malicious attacks). Normally, in their workplace, this software will be installed by default by organisations, whilst at home, users need to do this by themselves (i.e. unless if the computer is pre-installed with antivirus on the first hand). Therefore understanding the security features of this tool are essential so that users know when and how to use it (Ben-Asher et al. 2009).

In different scenarios, web browsers for instance became a platform for end-users to use the Internet. In using this platform, users are able to search for information, communicate within distances, make banking transactions and download or upload information at their convenience. In these contexts, security features and functions must be available for users to use so that the communication or transactions become fully safe. Therefore, understanding the functionality provided within the current technologies is both crucial and challenging.

Nowadays, having security software on one's computer is deemed to be a necessity. A key reason for this is the volume and range of threats. For example, according to Symantec (2012), there were 42 billion computer spams (i.e. estimated global spam per day). In addition, it has been reported that 5.5 billion malicious attacked were blocked in 2011, as compared to 3 billion in 2010. On the other hand, Potter & Waterfall (2012) reported that users infected by malicious software were considered high as compared to

similar reports in 2010 (i.e. two-fifths in small businesses and three-fifths on larger organisations). This indicates the need for the use of security tools to protect users from any threats. In order to understand users' interaction with security tools and technology in further detail the next two sub sections consider security and usability, and end-user perception and trust.

2.2 Security and usability

Security and usability are two different domains, but can be linked in some way. Such concepts are also known as usable security. Smetters & Grinter (2002) claimed that designing usable security technologies, led to the design of useful secure applications from the end-users perspective. They discussed the three types of traditional "users" of security technologies; the developer – that integrates security in system, the administrator – who maintain the security policy and finally the end-users – who follow the policy. As more software can be used freely from the Internet, end-users must understand how to use it correctly so that they are able to protect their own device. Therefore, it is a challenge for the developer to create and implement a usable and secure system which end users can interact with accordingly. For instance, most users will need to interact with antivirus or Internet security packages that often present security decisions for users to make (Smetters & Grinter 2002 and Furnell et al. 2006b). Even though some products offer functionality to automate these responses (i.e. choose default settings) there is still a need for user intervention to use it in secure manner. In other words, end-users are likely to be their own systems administrator (Edwards & Grinter 2001). Balfanz et al. (2004) examined the traditional PKI deployment and found out that the setup for wireless network and PKI by Microsoft XP involved thirty eight steps when it only needs eight steps to take when they produced the manual in their study. This revealed that providing security and usability at the same time is a challenging task for developers. Thus, aligning both elements is necessary to avoid conflict especially in the early stages of the design cycle (Yee 2004 and Dewitt & Kuljis 2006). Later, end-users would be able to use the products correct and securely and the goal of computer security can be achieved.

The goal of computer security involves three main aspects of any computer related system that comprised of confidentiality, integrity and availability. According to Pfleeger & Pfleeger (2003) and Bishop (2003) confidentiality can be defined as the concealment of computer-related assets or resources from unauthorised parties (i.e. secrecy or privacy), whilst integrity refers to trustworthiness where only authorised parties are able to undertake any changes or modification in authorised ways. On the other hand, availability refers to the ability to use computer-related assets or resources when needed. Bishop (2003) stated that to implement computer security controls was a complex task and cumbersome. Security practitioners and developers should find a solution to ensure that the goals of computer security can be achieved. In order to achieve this, Yee (2004) suggested that security and usability should be aligned. He believed that security and usability shared common goals in accomplishing end-users expectations. He further claimed that when security and usability were not addressed as add-ons, conflict between it can be suppressed.

On the other hand, people involved in software engineering begin to realize tardily that information security is important for software development, even where the primary function is not related to security (Tondel et al. 2008). Many aspects have to be considered to create applications, software and systems, and one essential element is usability.

Wright (1991) defined usability as a measured by how easy and effective for the computer to be used by set of users. Brinck et al. (2002) defined usability as the degree to which people manage to perform a set of required tasks. Nielsen (2003) referred to usability as a quality attribute which evaluates how user interfaces are used. He stated in his study that usability needs to be defined by five quality components, namely learnability, efficiency, memorability, errors and satisfaction. A further definition by ISO (1998) is as follows:

“...the extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use.”

It may be noted here that usability covers various elements such as functionality, efficiency of usage and even error tolerance. Usability should, indeed, be regarded as an essential element for products, especially when it is related to end-users. Having fulfilled all of aforementioned components by these authors, the ease of use of the products may be achieved. Having experiences in multiple usages of applications and browsers in computer, it may be noted that usability and security play an essential role. If usability of such aspects were disregarded, the function and presentation of security warning would be unusable. Thus, security and usability must be able to complement each other. The ideal trade-off is to ensure that the design of one product (i.e. security warnings) have enough security functions without disregarding elements of usability. For instance, the concept of using *design principles* has been introduced to improve the security of computer systems (Saltzer & Schroeder 1975). They introduced eight examples of design principles that can be applied particularly to the protection mechanism. One essential finding of their research was the term of *psychological acceptability*, which stated that human interface was designed for ease of use, and users should apply the protection mechanism correctly.

Therefore, it is obvious that security and usability serve a vital purpose. By addressing the importance of security and usability, an indication is given as to how both elements may be aligned so that end-users can use the application in a secure manner, without having problems with implementation.

2.2.1 Usability problems

According to Furnell et al. (2006), many applications in computer contained security features for end-users to choose from and configure. Simultaneously, there is a potential for them to make a security-related decisions. However, with regard to features that were implemented to guide or help end-users, it was actually disregard them to use it accordingly. In addition, end-users have different knowledge and capabilities when using such technologies, especially those who are not sufficiently experienced with computers (i.e. customizing features, updates patches, run antivirus and handling security warnings). Figure 2.1 shows an example of security features available to users of the built-in Windows firewall. Not all users were able to

understand the options presented in this dialogue, as the information presented was not written in an accessible/understandable form. A similar scenario is illustrated in Figure 2.2 where the use of the technical terms “Script” and “Active X” might be confusing to some users and may cause them to make incorrect security decisions. This section thus describes some problems that occur with regards to the usability of security tools and technologies.

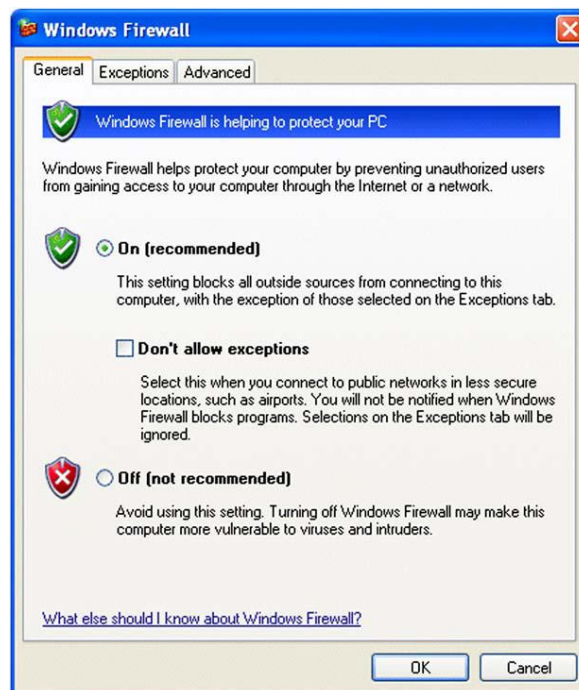


Figure 2.1: Windows Firewall settings (Furnell et al. 2006)

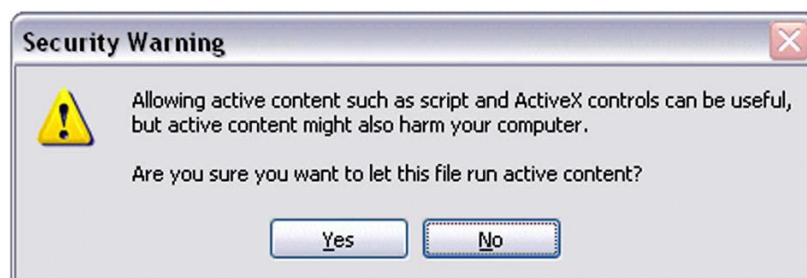


Figure 2.2: Security warning in Internet Explorer that used a complex language (Furnell et al. 2006)

Problems occurring in Pretty Good Privacy (PGP) 5.0 (see Figure 2.3) constituted one of the earliest studies on usability issues, as this tool was not sufficiently usable to be effective in the context of security (Whitten & Tygar 1999). They revealed that the design of the PGP application was not appropriate for end-users without a security

background. One third of them (out of twelve) were unable to correctly sign and encrypt an e-mail and one quarter even exposed the secret key. Another line of research by Proctor et al. (2000) found usability problems existed in third party authentication methods, whilst Wool (2004) found usability problems in configuring firewalls to selectively filter traffic. Lacking usability thus causes users to change from a secure system to an insecure system. In terms of ease of use, users will not be able to use the products accordingly, or to satisfy their needs.

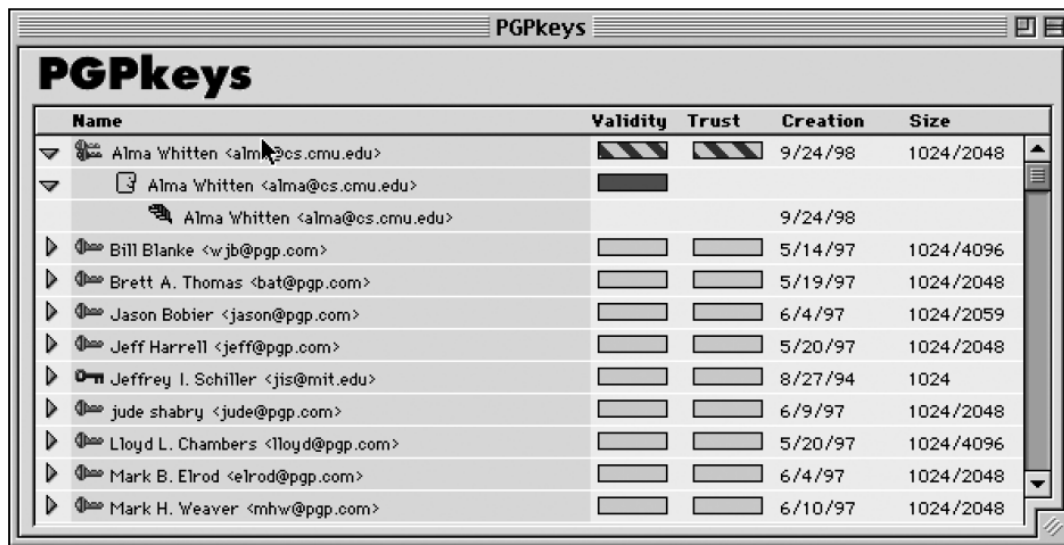


Figure 2.3: PGP keys display where users unable to correctly sign and encrypt e-mail in a specified task (Whitten & Tygar 1999)

On the other hand, Good & Krekelberg (2005) conducted a laboratory study with regards to KazaA file sharing user interface. They found out that their respondents were unable to tell what files they were actually sharing, and sometime they assumed that they were not sharing anything, although in reality, they shared all files in their hard drive. They revealed that KazaA sharing interface had usability problems which led to privacy issues. Most software developers were not primarily interested in security and usability issues (Coffee 2006 and Mouratidis et al. 2004). Their main intention was to implement as much functionality as possible, rather than making it easy to use (Meier 2006). This led to the weak implementation of usable interface on applications to deter end-users from unsafe behaviour.

Issues of usability were also highlighted as one of the major research challenge (CRA, 2003). In this report, “human error” is often cited as the main cause of configuration

errors. In assessing their fundamental research problems with regard to understandable, deployable, and usable security, they highlight one example as mentioned below:

“Encryption is one specific instance that deserves special mention. Well-encrypted messages can move safely through dreadfully weak systems. Encryption is well understood, but not widely employed. There is a ‘usability gap’ that translates directly into a ‘usage gap’” (CRA 2003).

Based on the examples given in this section, it is important to view usability and security beyond these contexts. Even if a particular application provides the required functionality, the overall achievement may be considered unsuccessful if users are still unable to understand and to use it correctly. For instance, most applications, operating systems and web browsers use security warning as a tool to let end-users know something is going on or that actions need to be taken. Indeed, some of the most crucial decisions may occur when such warnings are issued (i.e. security updates, antivirus protection and downloading application) and solely on end-users to respond appropriately. In this context, users’ decision making are really crucial because it could lead to good or bad consequences. Therefore, the usability aspects should be fully considered so that they can support users to make effective decisions. The importance of understanding security is to ensure that users are able to use the tools and technologies (i.e. from the perspective of security) in secure manner which later will promote a safe behaviour.

From one perspective, usability made the WWW (World Wide Web) successful (Berners-Lee et al. 1994). Usability helped developers to make better decision and made their task became more efficient and effective (Radle & Young 2001).). It was proposed that by identifying the users and their requirements, usability can be incorporated in the early product life cycle and therefore organisations can increase productivity, user satisfaction and accomplish usability goals without having problems using security tools. The failure to consult with end users will have annihilating effects on the products (Faulkner, 2000). This is why every feature that developers would like to implement should meet users’ requirement on the first hand.

In addition, Nielsen (2003) identified usability as a requisite aspect in websites, e-commerce transactions and Intranet. If it failed to address proper information and clearly stated the products, people would get rid of it. Since then, there has been increasing interest in security and usability studies, as demonstrated by the vast number of researchers (Cranor & Garfinkel 2005, Yee 2004, Hoegh 2006, DeWitt & Kuljis 2006 and Macaulay et al. 2009).

As the growing research and developments in this area encourage developers to pay more attention on usable security, security should be embedded as part of the product cycle, instead of implementing it after that. By integrating security during the life cycle able to improve overall web application security (Meier 2006). Usability should be viewed as one of the fundamental concepts in products creation, so that it can work as expected (i.e. comprehend end-users). On the other hand, there are some challenges to integrating both elements because of the difficulty of finding a subset of security and usability. However, Yee (2004) proposed a method regarding how to align these elements, so that usable security can be achieved.

2.2.2 End-users Perception and trust

End users often claim that they understand the usage of one particular application or tool, but in reality, they actually do not. Therefore, understanding end-users perception and trust with regards to the usage of security tools and technologies is essential (Morris 1997). Confidence and a trustful relationship are essential to reduce possible threats in the electronic commerce perspective (Ratnasingham 1998). When users experience a particular website or application, they develop their trust value in that process (Phippen & Furnell 2007). According to Lacohee et al. (2006) users decided to choose trusted company or website which they have used before. The branding process is able to generate trust by using logos and company names which their integrity is well respected (Shneiderman 2000). Similar results are portrayed in Furnell et al. (2008), as users claimed they only used trusted websites, but they still failed to demonstrate their knowledge to learn more about security features in the trusted websites. Users regularly tend to accept any security features in website (such as the lock symbol, trusted

company logos and verified by a certain established company) without taking further action to investigate (Schechter et al. 2007 and Whalen & Inkpen 2005).

When no factual basis or detailed information can be referred to, users' perception will be based on the emotions (Havana & Roning 2004). Decisions based on the emotions will then lead users to take risky actions, with potentially catastrophic end results. This was the reason Murayama et al. (2009) justified the importance of the "Anshin" concept as an emotional trust that incorporated a sense of safety, reliability, privacy and availability. This concept may be applied to end-users decision making processes so that they are able to act in secure manner.

In order to examine the level of severity, users need to strengthen their knowledge at first hand. The level of knowledge became an indicator to ensure people had the ability to evaluate the risks, and at the same time users gained trust that based on the amount of knowledge that they have had (Havana & Roning 2004). The laypersons often take vigilant action with regard to information security when problem starts to occur (Furnell 2004). When nothing much can be done, they will rely on other people to help mitigate the problems. The more steps involved in a specific task, the more difficult the task to perform and the more error user pruned to produce (Schultz 2007). The development of software and application must be parallel with user's requirements. Armed with appropriate knowledge, the developer can create a better design and people get used to using it.

On the other hand, to obtain trust will involve users in understanding the risks. Risk and uncertainty are essential concepts for people to evaluate and to understand, even though it may be difficult to do so (West 2008). Understanding the risk provides the basis for end-users to evaluate their decision making actions. Hence, users will be able to gather some evidence based on their experiences, perception and trust towards decisions related to security and usability.

2.3 Human Computer Interaction (HCI) and the Graphical User Interface (GUI)

This section emphasizes the need to understand human computer interaction and graphical user interface contexts. Both of these contexts need to be discussed because they collaborate in the sense of providing interface and information to end-users (i.e. with respect to end-users and developers). Every interface in computer systems (i.e. security tools and technologies) involves both of these contexts. To be more precise, from the developers' perspective, they create programs or software that are able to present features that would be able to help users to comprehend any possible actions that users have to take, or to provide useful information with regard to the problems they face. Hence, when they design such programs, the principle of human computer interaction (HCI) will generally be adapted, and the final products will be presented in user-friendly graphical user interface (GUI). It is anticipated that such final products would be able to be used in secure manner by the end-users. In general, and on balance, Shackel & Richardson (1991) viewed human computer interaction (HCI) as Human-Systems Interaction (HSI). They define it as:

“HSI is concerned with methods, media and mechanism for enhancing cooperation between people and systems in an interactive organisational environment”.

On the other hand, Hewett et al. (1996) defined human computer interaction as:

“a discipline concerned with the design, evaluation and implementation of interactive computing systems for human use and with study of major phenomena surrounding them”.

Therefore, it may be argued that human computer interaction (HCI) is a discipline comprising requirements with regard to the mechanism, evaluation and implementation, based on the interaction between human and systems. In order to improve the design of computer system interface, HCI can be used as a basis or reference point, as it integrates all fundamental elements that are needed in one particular interactive system.

According to Faulkner (1998), there are two main methods in which the users communicate with computer (i.e. linguistic manipulation and direct manipulation).

Linguistic manipulation also known as command line interface where users need to type some command line to interact with computer systems. Direct manipulation is also known as iconic interface or Graphical User Interface (GUI), where users interact directly with computer via tools such as keyboard, touch screen and mouse. Therefore, the direct manipulation method (i.e. GUI) seems to be more relevant within the current contexts of computer usage. It is clear that nowadays, every application or software is presented in such a way that it is easy to use and user friendly (i.e. appropriate with all level of users). As users' interactions are directly with the computer, it is important to understand the GUI concept in a bit detail. The concept of GUI had been introduced by Douglas Englebart when he demonstrated his system called oN-Line System (NLS) based on his work on "augmentation of man's intellect" (Baecker et al. 1995b). Since then, the GUI has been widely used by many computer developers for applications or products. GUI may be defined as graphical interface of one particular computer that allows users to do some actions (i.e. click and drag objects) via mouse instead of command line (Pc.net 2012). Linfo (2004) has claimed that GUI is human computer interface that used windows, icons and menus that can be manipulated using mouse and keyboard. In addition, Bétrancourt & Bisseret (1998) claimed that interface which integrated text and picture were able to improve learning. Therefore, this indicates that GUI can be seen as an intermediary between end-users and computer so that input and output can be delivered between them.

Having understood the relationship between these concepts, a basis has been provided to further understand how end-users interact and reflect with the security tools and technologies they have. Therefore, the next sections will explain the needs and potential direction of this thesis.

2.4 The needs for understanding usability for security and protection contexts

Usability aspects can be viewed as one of the most significant elements, especially when users want to make a decision. Before the decision process, users are normally presented with an interface which explains the current circumstances and possible options (e.g. security warning, notification, banners, and balloons). Therefore, it is clear that the ease of the decision making process can be aided through the usability or the

clarity of the interface (i.e. sufficient information and useful features). The following examples support how decision making is linked to the essential nature of usability of such features.

For instance, Tognazzini (2005) has described an example of a security device called “Tresor” (i.e. file encryption application). In order to make it usable for end-users in terms of the decision to key in their password, the application was able to offer users whether to veil or unveil the password based on their preference (e.g. base on users’ location or users’ privacy) which made them to use the Palm’s Graffiti System in a much easier way. Hardee et al. (2006) conducted experiment with regard to computer security decision making, and found that in order to achieve successful decisions, the warning presentation must be improved to be more usable and effective by altering the wordings or the decision frames (i.e. explicit wordings and highlighted the risks and potential losses).

West (2008) explained the difficulty of making a decision with security warning dialogues, as it looked similar and none too outstanding in relation to any other. He suggested that the design of the warning message should be enhanced and made it usable (i.e. looked and sound differently), so that users were able to differentiate, were likely to read and later to consider the options provided to them in secure manner. Stoll et al. (2008) proposed “Sesame” as a tool to help users make security decisions by showing details of the background process step by step until the user was able to make a decision. They made use of the concept of direct manipulation of the graphical interface to help non-experts make informed decision as shown in Figure 2.4. It helped users by revealing the system’s hidden security state using a graphical illustration that facilitates users’ understanding in making decisions.

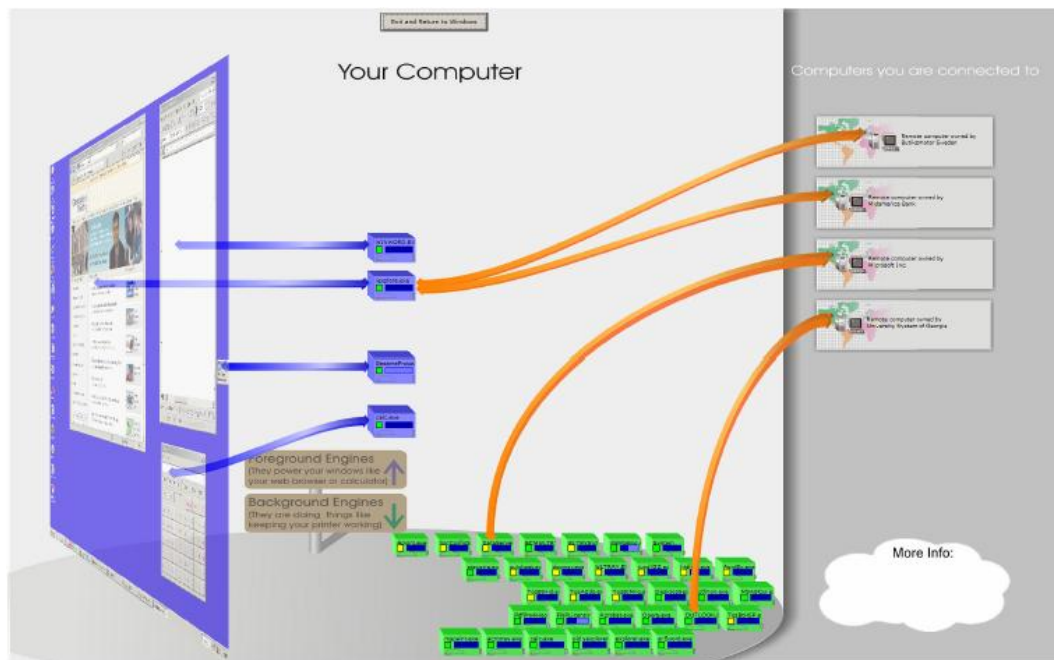


Figure 2.4: Behind the scene of Sesame where user able to view the process before making a security decision (Stoll et al. 2008)

All of this evidence illustrates the importance of usability from the context of the decision making process. Usability significantly helps users to make a better choice, and most importantly, navigate them from making a wrong choice that could impair or compromise their computers to computer menaces. With the rapid expansion of computing technologies day to day, the needs of usability become more dominant and as every products would need to be easy to use (i.e. usable) and works effectively. From the contexts of computer security, the decision making processes that carry the most risks are often associated with security warning messages. These indicate that security-related events have occurred or have been detected. Therefore if the wrong decision is made by users, this has a number of negative implications for security and protection of the user's computer. In addition, the goal of computer security (i.e. "secure level": confidentiality, integrity and availability) will be difficult to achieve.

One of the classic cases with regard to the implications of making wrong decisions was the assessment of PGP 5.0 (i.e. encrypted email) where two thirds of participants incorrectly thought they had encrypted data (Whitten & Tygar 1999). This resulted in serious consequences as the information had been breached within computer security contexts. Stool et al. (2008) also claimed that when wrong decisions was made, users were exposed to many attacks such as phishing, bot infestations and other forms of

malware. Egelman et al. (2008) revealed that 97% of the 60 respondents in their study became victims of phishing attacks, based on the decision they made, because they were unable to differentiate between authentic and bogus website. They mentioned that 79% of their participants heeded the active warning as shown in Figure 2.5. In contrast, only one user obeyed the passive warning (i.e. as passive warnings were often ignored) as shown in Figure 2.6. Jagatic et al. (2007) on the other hand found out that 72% of 487 participants revealed their personal credentials to the phishing websites. The impact of the wrong decisions significantly affected users in monetary terms, and even psychologically speaking. For instance, a similar situation occurred when users decided not to update his or her antivirus program in computer with the latest patches and decided to download software from peer to peer file sharing (e.g. Torrent). Simultaneously, he/she did not realise that a new computer malware was propagated within the computer network. Without realising the consequences of the implication, the user's computer was attacked or compromised as a results of wrong decision that the user had made earlier in time. This resulted in the computer virus being spread in the user's computer and likely to the entire system (Bellissimo et al. 2006).

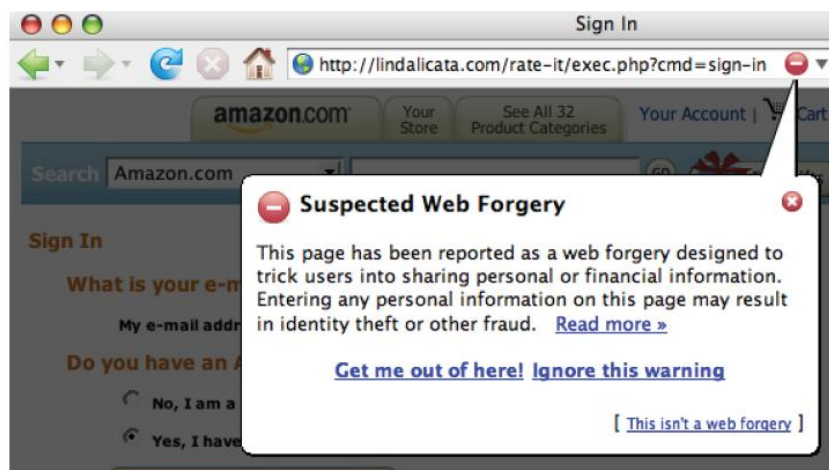


Figure 2.5: The active Firefox 2 phishing warning (Egelman et al. 2008)



Figure 2.6: The passive Internet Explorer 7 phishing warning (Egelman et al. 2008)

The most serious implication has been highlighted by Potter & Waterfall (2012), who indicate that individuals and organisations have suffered from direct and indirect financial loss and even damage to reputation especially for major organisations. They claimed that it can be estimated the total cost of incidents roughly around £15,000 - £30,000 for small business and £110,000 to £250,000 for large organisations. It had been reported by Symantec (2012) where 232.4 million identities were exposed and it was sum-up altogether to 5.5 billion attacked in 2011. This striking information indicates the potential danger if the wrong decisions are made that impair end-users as a whole.

Based on all of the evidence with regards to general users' interactions with security tools and technologies, one of the most significant areas that end-users are still facing difficulties is around the issue of specific interaction with computer tools or application, and more particularly, when the tools try to warn them about something is going on. Therefore, users' experiences the significance of security warnings as a medium to warn them before decisions can be made. Security warnings may be seen as the main medium by which to give warnings or even information about potential problems or risks at a specific time. Before any action can take place on the part of users, the security warning is presented as a reminder for them. The most crucial part, when users are offered more than one option and at the same time there were no specific functions or features to help or guide them to make a secure decision currently available. In these circumstances, any false decision making may lead to catastrophic results. This could

jeopardise the fundamental issues of computer security to ensure the goal of computer security can be achieved. At any stage, warning messages became prominent to users whilst using their security tools and technologies. Before the wrong decision is made, it is better to counter the problems in the initial phase and find possible methods to improve it. Therefore, based on the assessment with regards to the interaction with security tools and technologies, this thesis will take a particular look and covers the issues of security warnings from the computer context.

2.7 Guidelines

According to W3schools (2012), Microsoft products were used by the majority of users, especially the operating system and web browser. As their guidelines provided more details about the usage of features as mentioned in the earlier section, the author use Microsoft guidelines as the main reference to further explore how every feature on security warning can be improved and utilised. This provided the author useful input by understanding how every feature are implemented in different contexts that will be able to suit it purposes. Hence, the author is able to investigate and to evaluate current implementation of security warning based on this guideline. Later, it is anticipated that any potential gap or common ground would be found in the recent implementation. Having clarified the gaps or common ground, an effective approach will be introduced to implement more usable security warnings.

In the aforementioned Chapter 2, this thesis has explained the relationship between HCI, GUI and usability. The rationale behind this was that the Graphical User Interface (GUI) was introduced to accommodate the interaction between users and computers in a simpler and appropriate way, specifically in the fourth generation of the computer. Prior to this, presenting a security warning during that time was very limited because the interaction between users and computer was based on linguistic interaction style. If this occurred, warnings were usually presented through the wordings on the computer's interface, which was obviously not a user friendly type of interaction (e.g. MS-DOS prompt). HCI was used as standard principle so that inter-communication between human and computer could be achieved in a secure manner. Since graphical user interface (GUI) was introduced as part of HCI implementation, the author believed that

it was the era when security warnings started to evolve. Simultaneously, issues regarding usability of computers started to be highlighted as one of the major issues.

2.7.1 Purpose of warnings

According to Wogalter (2006), warnings may be defined as safety communications that are used to inform people about hazards and protect them from any harm. Rogers et al. (2000) and Tuchscheerer et al. (2010) defined warnings as anything that is able to alert an individual's attention towards potentially dangerous circumstances. Thus, a warning is a means to inform users about potential risks or problems that might occur in the future, and may protect the user from any possible harm. A similar definition can be applied in warnings in computing contexts. Applications or operating systems present warnings as the medium to inform and to warn about the possible consequences of an action by the end-user. This explains that risks that might occur and possible precautions should be considered before users proceed with a potentially risk action.

Fundamentally, Wogalter (2006) pointed out four main functions of warnings in general context (i.e. consumer products, equipment and services):

- i. To communicate important safety information
- ii. To influence people's behaviour in a way that will improve safety
- iii. To reduce or to prevent health problem, workplace accidents and property damage
- iv. To act as a reminder of something that people already know but may have forgotten about.

Based on these main purposes, the essentiality of warnings may be indicated so that users can be informed about the potential risks and provide safety information to avoid on such incidents. In addition, warnings are able to influence users to act accordingly when facing difficulties. Based on the information provided in the warning, users learn how to differentiate how and what to avoid, so that later it will prevent them from such hazards (i.e. malware, phishing). Warning was used widely regardless of any locations that suited its purposes (i.e. road - to warn pedestrian or the drivers and product labels -

to warn about the contents of products). Viewing warnings from a computing perspective, they can be posed as a reminder when users are potentially facing any type of risks. For instance, an antivirus program pops up a warning upon detection of malicious activity in users' computers. Warnings thus become the first point of contact to remind users that attention is needed. In this scenario, some of the users might already know what is happening and the next steps to take. Regardless of this, warnings have still been presented as a reminder, so that any possible actions can be taken. Wogalter (2006) also introduced the warning hierarchy as part of the hazard control hierarchy, as shown in Figure 2.7.

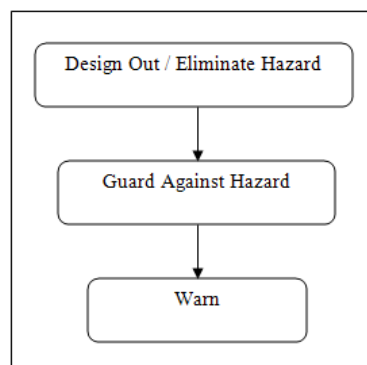


Figure 2.7: Hazard Control hierarchy

The first step in the hierarchy is to get rid of the hazards (i.e. try to eliminate or to minimize it). He claimed that alternative design was generally the best method to eliminate hazards. After trying to eliminate the hazard via the design, the next step is to guard against all possible hazards. This to ensure that people or property had limited contact with the hazard. The third line of defence was to warn where warning can be viewed as the third priority, and not always reliable to prevent contacts with the hazard. Wogalter (2006) also clarified that where all of these three steps are still not effective, the additional last step is to remove the product or the environment from use.

From the author's point of views, one particular product (i.e. software or application) cannot be removed from the end-users as the last resort of action, but an appropriate warning should be put in place so that it will be able to navigate users to make a secure decision. The author believes that the implementation of products should be reviewed (i.e. in computing context it can be reviewing the implementation of security in system development cycle). Mouratidis et al. (2004) & Tryfonas et al. (2001) claimed that

security is often considered after the completion of the system, instead of integrating it in the earlier stage. This has often led to problems when the system cycles had to be repeated again to integrate the changes.

Consider Google Chrome as one example. It is a browser or a platform for the user to seek more information, to upload and download software and medium of communication. If any problem occurs at any stage whilst using this browser, the warning is still used as a medium to inform users about what is currently happening. In this context, a warning can be viewed as the first source of information that keeps users aware about current problems which they encounter. If the problem persistently occurs, one particular product should be reviewed back in the product cycle (e.g. system, analysis and development).

On the other hand, Bravo-Lillo et al. (2011b) have argued that in certain situations, designing or eliminating the hazard and guarding against the hazard might not be feasible. He gave the example of the sharp edge of the knife. To make a knife safe, none of the edges should be sharp to stop the user from cutting their fingers and hands. Designing a knife with blunt edges is not practical, as the main purpose of a knife is to cut objects. Moreover, placing a guard on the knife (like a metal shield) would be not being practical as it would restrict the use and capabilities of the knife. A similar scenario in computer security incidents that risk of being attack by malware cannot be completely removed as to design particular software that is fully secured is also impossible.

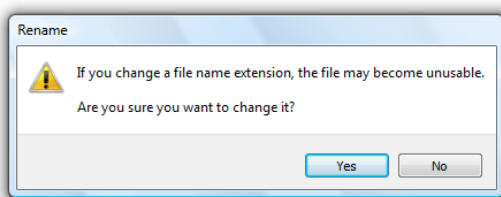
2.8 Warnings in computer contexts

By understanding warnings in general contexts based on the aforementioned sections, it may be seen that there is a need to further understand how previous warning implementation can be applied in the contexts of computing. Most of the features based on the descriptions on warning history such as using signal words influenced directly to the current implementation of computer security warning. In order to suit the context or circumstances, the regulators and industry adapted the best approach to warning, to change community standard and guidelines, citizen pressure, technological innovations or even new scientific knowledge (Egilman & Böhme 2006). Based on the guidelines

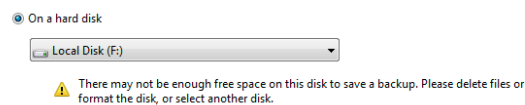
by Microsoft (2010), warnings alert users within five different user interface contexts, as shown in Table 2.1.

User Interface Contexts	Suitable Usage
Dialogue Box	Used for critical warnings that includes confirmation. Users must respond to the warning instantly (Modal dialogue box)
In-Place	Used to provide information that possibly prevents a problem. It is useful when users are making choices
Notifications	Used with significant circumstances or status that can be safely ignored by users (at least temporary)
Balloons	Used as a control in a situation that affects the input. This state is likely to be unintended and users may not realize that the input is affected.
Banners	Used to provide information that may prevent a problem. It is useful upon users completing a task

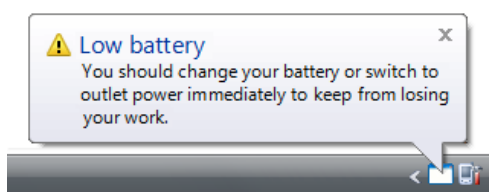
Table 2.1: Five different user interface warning contexts



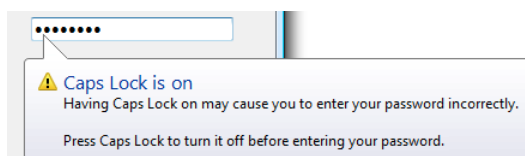
Dialogue Box



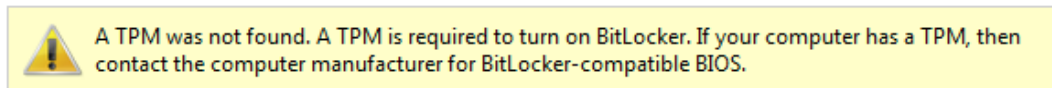
In-Place



Notifications



Balloons



Banners

Figure 2.8: Examples of warnings in various contexts of user interface

It can be noted from Figure 2.8 presented the examples of security warning implementations based on the contexts of the warnings. In Microsoft (2010) guidelines, there is a detailed explanation, especially with regard to the design concept and how one particular element should be used (e.g. icons, colours, fonts and texts). This provides a clear context to explain the different usage and with the help of image. The differences in presentation of one particular warning might have a different impact in terms of how the user perceives it.

2.9 Problems and issues with security warnings

Having looked at the general context, this section highlights useful evidence with regards to warning studies relating to security tools and technologies. Security features on warning messages help users to mitigate the risk by providing protection from potential threats. This provides information and options that would encourage users to take or to be more cautious. For instance, the usage of signal cues such as colours, help function and useful links. These features are generally notable because they have been used in most of the operating system and applications in web browsers. Molich and Nielsen (1990) claimed that a good warning dialogue provided carefully phrased information on messages in various situations especially when the user needed helped. Johnston et al. (2003) suggest that user interfaces were designed to help end-users to understand the usage of computer technology and later they were able to increase the efficiency to complete the task. Nowadays, the challenges for the end-users are not only in terms of understanding the complexity of interfaces on one particular application, but the external factor is far more challenging which comes inconspicuous and cause harm to people.

Infection by viruses or malicious software were among the highest incidents recorded (Potter & Waterfall 2012, GoCSI 2010 and Potter & Beard 2010). In one recent study by Symantec (2012), variant of malware were 286 million in 2010 and increased to 403

million the following year. They also claimed that the “website malware” was among the most popular cyberspace issues where 61% of malicious sites were actually regular websites that had been compromised. In addition, Symantec (2012) also categorized the five most infected websites (i.e. blogs and web communications, hosting/personal hosted sites, business/economy, shopping and education). The results from these findings indicate that end-users were exposed with many cyber-threats whilst they dealt with computer on daily basis. These also provided the essentiality to further probe and clarify on what users’ understand about warning and how to better support users’ to make better decisions. This is supported by Bravo-Lillo et al. (2011b) who clarify that to understand what users think and believe about warnings in order for them to make safer choices needs an attention to further clarify and solve the problems.

As warning communicates to inform people about hazards, it has been used widely in the software and applications context (Microsoft 2010). It had been implemented in web browsers, operating system and applications. Users were notified with regards to warning in various mechanisms such as dialogue box, balloons and notification. Some of these notifications might directly interrupt the user’s current task and some might just pop up for a while (i.e. active and passive warning). Böhme & Köpsell (2011) pointed out that the average users made several dozens of decision per day to respond with the pop-up dialogues that interrupted their primary tasks. The author believed that for general or laymen users, this task would be a daunting one especially when it involves with security elements and usage of technical terminology. This is supported by Norman (2009), who similarly discovered users were afraid to make a decision especially with regards to security as it was very difficult to distinguish the legitimate or illegitimate source.

As a medium of communication to warn users, warning presentations should be able to give users with enough information and guidance. In this particular section, the author highlighted literature reviews on the problems that users’ usually encountered with computer security warning studies. This would clarify the problems that users encounter whilst dealing with warnings. For the past ten years, computer security warnings have been investigated in many domains such as virus alerts and active browser warnings (Dhamija et al. 2006, Egelman et al. 2008 and Sunshine et al. 2009), online banking context (Mannan & Oorschot 2008 and Weir et al. 2009), privacy and

policy (Reeder et al. 2007 & Lampson 2009) and fake security warning (Sharek et al. 2008 and Stone-Gross et al. 2013). On the other hand, Symantec (2012) also claimed that web browsers were a popular target for the criminals to exploit the vulnerabilities of browsers (i.e. Opera, Mozilla Firefox, Internet Explorer, Google Chrome and Safari). With respect to the mentioned evidences, it is obvious that there are needs to investigate and to gather evidence on how people views security warning in general contexts. It is useful to gather some evidence to understand the problems that users encounter whilst assessing security warning. The following sub sections highlight the underlying evidences on the reality of what end-users had experienced with security warning in general contexts. It is useful to gather this evidence to show the need for further research in this field of study.

2.9.1 Attention towards warnings

A study by Whalen et al. (2005) investigated insights from visual security cues using eye tracker and found out that participants did not pay attention to web security cues warning. Users have demonstrated that smaller icon warnings can be easily misidentified, certificates are seldom used and understood and people tend to stop searching for security information once they log in to the websites.

Wu et al. (2006) conducted user studies with 30 participants to prevent phishing attacks, and revealed that participant were fooled 34% of the time. These participants ignored the warning especially when the web content looked legitimate.

Seifert et al. (2006) conducted a web based survey with 114 users to evaluate the effectiveness of security warnings in a web browser setting. They revealed that some users still ignored the warning as it did not encourage them to take secure action. They argued that the warning displayed did not have enough information regarding the implications of such action by users. Their findings also suggested that users' decision as to whether to install or not the "ActiveX components" were driven by the display of security warning they had.

Schechter et al. (2007) conducted a study with 67 bank customers to evaluate security indicator warnings and how they affected participant behaviours. They found that users

ignored the HTTPs indicators and site-authentication images were found to be ineffective as 92% of participants still entered their credentials (i.e. username/password) to access their online bank service even though the warning image had been removed.

2.9.2 Understanding of warnings

Egelman et al. (2008) conducted an empirical study related to the effectiveness of phishing warnings and found that 20 out of 47 users did not understand the meaning of the warning that been presented. 97% of overall participants fell into at least one of the spear phishing messages they received. They provided some recommendations to improve the warnings, and stated that indicators needed to be distinct, from less serious warning to more danger and warnings indicators, so they could only proceed to the phishing website after reading the warning message.

In a different scenario, 72 individuals were unable to identify a secure browser connection via extensive two hours semi-structured interview that included drawing task about web security warning evidences (Friedman et al. 2002). They also point out the surprising finding that technology savvy participants did not always have an accurate understanding of these warnings, as compared to other users.

On the other hand, Sharek et al. (2008) conducted a study to evaluate end-users behaviour upon receiving fake Internet pop up warning. Their study revealed that 73 % of respondent (out of 42) incorrectly responded to fake warning pop up. The results indicate that end-users did not even realise the potential of the negative consequences of their actions. 42% of total responses claimed they prefer to get rid of the warning as it was annoyed them. This finding reveals that end-users were lacking of knowledge to differentiate the characteristics of real and fake warning. It also suggests that warning presentation should be made clear by using unique features that able to comprehend them.

Sunshine et al. (2009) conducted a survey of 400 Internet users to examine their understanding of SSL warning effectiveness in two versions of Mozilla Firefox and Internet Explorer browsers. They pointed out that 62% of the respondents did not understand the warning contexts that had been displayed (i.e. expired certificate,

unknown certificate authority (CA) and domain mismatch warnings). In terms of users' comprehension and risk perception, they revealed that some of the respondents claimed they were not at risk because they used operating systems liked Macintosh, Linux and FreeBSD.

2.9.3 Use of technical wording

Bravo-Lillo et al. (2011b) conducted an open interview with 30 respondents related to computer security warnings and reported that novice users often did not understand the technical terminology. They claimed that these participants had heard about it, but they struggled to comprehend the meaning of the terminology been used.

Furnell et al. (2006b) conducted a survey with 340 end-users with regards to the usability of end-users security software. They found out that understanding technical terminologies became common problems in end-users security features where only 35% of overall respondent knew the meaning of the ActiveX control in Internet Explorer browser.

2.9.4 Evaluation of risks from warnings

Downs et al. (2006) claimed that users were unaware of cues and information provided to warn them. Therefore, they were unable to identify phishing threat and unlikely installed program albeit it cause harm to their computer. On the other hand, Nodder (2005) studied on users' behaviour in trust situations and revealed that users' did not think about the consequences of their actions. As a result, they made one-off decision making and might fall in bigger consequences such as became victim of malware.

Raja et al. (2010) also revealed that most of their respondents (i.e. 30 participants) specifically with low level of security knowledge unable to make informed decision based on the context of firewall warnings. They claimed that these users were unable to use the protection accordingly, unable to understand the factors that affects their decision making and how it may affect them in the future.

2.9.5 User's motivation towards heeding warnings

West (2008) suggested principles to improve security behaviour, and pointed out that users' generally unmotivated with regards to security-related decisions. He highlighted that users did not read all information that relevant to them and did not consider all possible consequences of their actions.

On the other hand, Herley (2009) claimed that users ignored security warnings and security advice because it offered a poor cost-benefit trade off and was a burden to them. This made users become demotivated, with too little benefits or incentives for too much cost they needed to manage. He suggested a better understanding of actual harm to users and prioritized the advice given to influence good security decisions and motivate them.

2.9.6 Users' assessments of the implication of warnings

Zurko et al. (2002) conducted a study with 500 people in an organization with regard to the security of the Lotus Notes client against unsigned active content. They found that users often did not understand the impact of their security decision enough to be able to make an informed choice albeit the warning was presented. Their study revealed that 44% of respondents executed the unsigned content regardless of warnings. They concluded that the more frequent security warning been presented in daily use, the more users learned to click "OK" without initially thinking about their action.

2.10 Gathering Evidence on the need for research into security warnings

From the highlighted works, it may be seen that end-users are still facing difficulties in assessing security warnings. Even though Wolgater viewed warnings as a third line of defence, from the author's viewpoint, it can be considered to be more important than this. This similar views agreed by Johnston et al. (2003) and Stoll et al. (2008) when they considered warning as the "first line of defense" especially to non-experts. To be precise, non-experts generally view warnings slightly differently, as they do not have much experience and knowledge of warnings. Therefore, most of the time, their decision will be based on their belief or their previous experienced. The necessity to understand further details about warning is when the decision of warning that users have

to make might impact the security and protection directly. Providing this evidence indicates that end-users still face problems with security warning specifically in computer applications. A security warning must be able to present sufficient information to warn users about risky circumstances and be able to promote safe behaviours with regards to decision making process.

On the other hand, the problems of security warning were not entirely because of end-users and consideration should be given by developers as well. Software designers are still leaving some decision for end-users to make that included important security tasks (Bravo-Lillo et al. 2011b). In addition, many options were provided on security warnings for users to rely on but unfortunately the information provided was still not sufficient to comprehend users with safe actions. On the other hand, Amer & Maris (2007) claimed that very limited standards exist in computing and computing professional literature related to the parameters that should be included in warning messages. In order to get deeper understanding whilst searching for the solutions, further investigation would be needed to examine end-users perception and attitudes towards security warning. In addition, further evidence should be gathered from users to assess security warning specifically with regard to the elements that they understand and elements that made them baffled. The following section presents useful frameworks and approaches that have been used to improve security warnings.

2.11 Overview of warnings process and other frameworks

There are many different conceptualizations and division of warning process. Overviews of warning process are discussed from the warning science literature to the specific method with regards to security warning in computers. Lehto (1991) developed hierarchy of operator performance that consisted judgment, knowledge, rule and skill-based behaviours that based from human information-processing steps. Simultaneously, different forms of information such as signs, symbols and values were used at every level performance that allowed the effectiveness of different warning message to be inferred. Rogers et al. (2000) introduced an integrative perspective warning process as shown in Figure 2.9. In order for the warning to be effective, four steps with interactions of person and warning variables are involved, as follows:

- i. Notice the warning – users’ attention is given towards the warning
- ii. Encode the warning – users used external information to internal representation
- iii. Comprehend the warning – users understood the meaning of the warning
- iv. Comply with warning – users’ behaviour worked in accordance with the warning

They defined person variables as individuals that interacted with the warning, whilst warning variables can refer to the characteristics of the warning or the context in which the warning appeared. From the context of computer security warning, to ensure its effectiveness, the security warning should be noticed on the first hand. Then users will use any information (i.e. experience or knowledge) to encode the warning. This can be done by understanding the meaning of the features on the security warning itself such as icons, words and colours (i.e. comprehend). Once users are able to understand everything and gathered enough information, they will be able to comply with the warning. Therefore, it would be useful for the developers to understand this warning process and the variables involved in the overall interaction so that a warning can be implemented accordingly. The following sub sections introduce the frameworks and the approaches to improve security warnings.

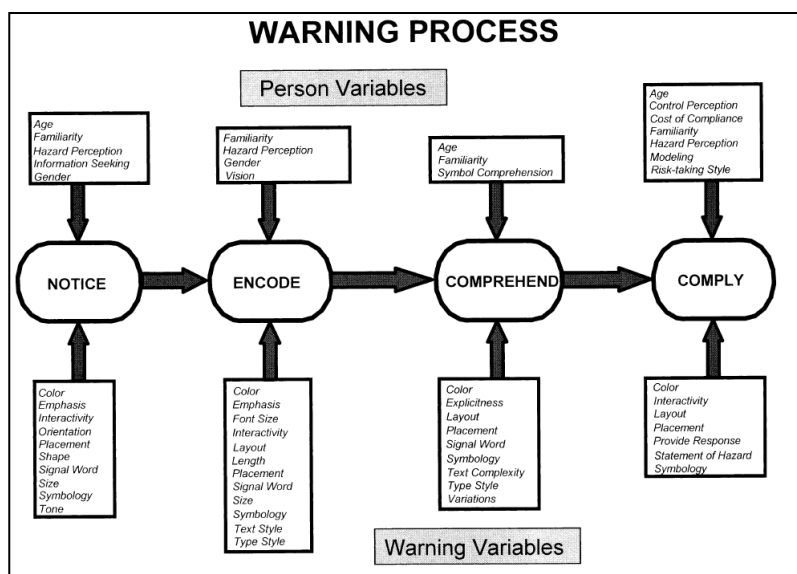


Figure 2.9: Four main components of warning process via repetition variables (Originally derived from Rogers et al. 1999)

2.11.1 Communication-Human Information Processing (C-HIP)

After understanding the overview of warning process, this section explains the related framework to security warning process in more detail. Wogalter et al. (1999), Wogalter et al. (2002) and Wogalter (2006) introduced the Communication-Human Information Processing (later will be used as C-HIP in this thesis) framework that involved steps in warning processing and as diagnostic tools to identify reasons for the failure of warnings as depicted in Figure 2.10. By using this framework as a tool, a specific area of the warning implementation may be identified, and a correction can be made accordingly.

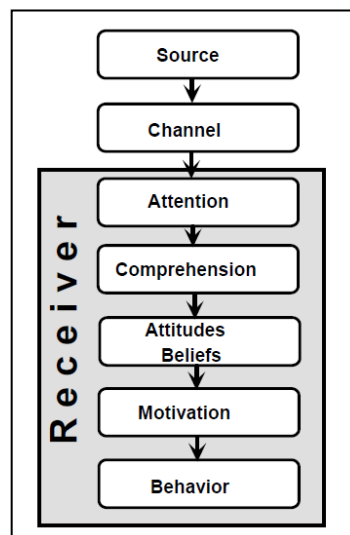


Figure 2.10: Communication-Human Information Processing Framework (C-HIP) based on Wogalter et al. (1999).

Wogalter et al. (1999) explained the framework in further details beginning with the source as the originator of the risk or hazard. It will then be channelled to the receiver using sensory modalities such as visual, auditory and kinaesthetic. In the receiver group, attention would be the first point of contact. The risk or hazard should be able to have a context or background, so that it will enable the warning to be more prominent. The next stage is comprehension that facilitates the understanding of the risk or hazard (e.g. the usage of symbols and words). It will then affect users' attitudes and beliefs. Later, it goes on to consider the motivation elements that relate to users' compliance with the risk involved. Lastly, is the essential part namely behaviour. It is expected that safe and correct behaviour will be achieved based on one particular warning that user

receives. From this framework, the author has learnt that the security warning problem can be identified in the early stage. This is useful, as early assessment on how security warning can be improved later on.

2.11.2 Human in the Loop (HITL)

Cranor (2008) was among the first researchers to use C-HIP model to develop the Human in the Loop (HITL) security framework. She used a similar approach but constructed her framework to be more specific based on security tasks. It provides a systematic method to design out security problems and help to understand end-user behaviours when they perform security-critical functions as depicted in Figure 2.11. Both of the C-HIP and HITL models explained the sequential steps that users will deal with but HITL is different in the sense of it focusing on security-related actions. Security related actions normally actuate through security-related communication (e.g. warning, notices, status indicator, training and policy). The stages that have been presented in the model were improved with some additional information, as listed in Table 2.2. By using this framework, she claimed that it is likely to act as a checklist to analyse and to understand human role in secure systems. There are four main features (i.e. communication, communication impediments, human receiver and behaviour). She classifies communication impediments with environmental stimuli and interference and grouping elements in human receiver accordingly (i.e. personal variables, intentions, capabilities, communication delivery, communication processing and application). The final stage of this model will lead to the aim of security communication, which is to ensure a safe behaviour.

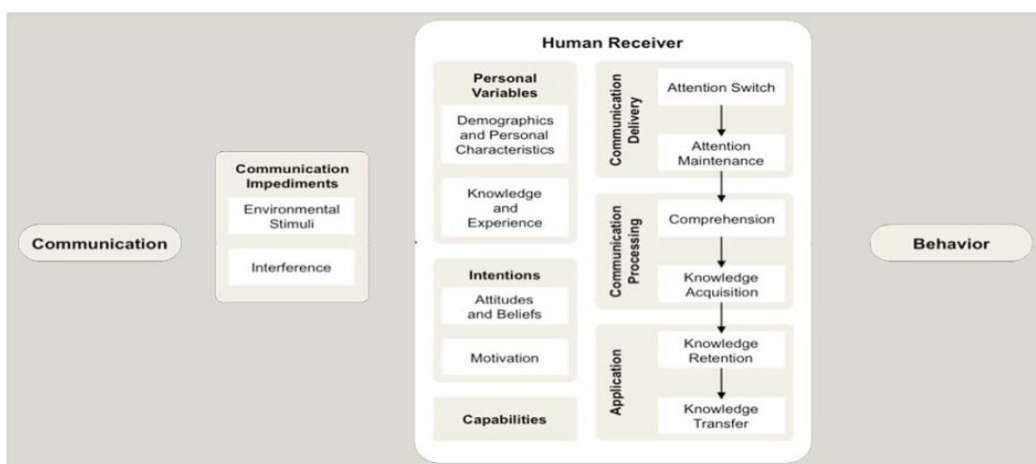


Figure 2.11: Human in the Loop security framework (HITL) by (Cranor, 2008)

Component		Questions to ask	Factors to consider
Communication		What type of communication is it (warning, notice, status indicator, policy, training)? Is communication active or passive? Is this the best type of communication for this situation?	Severity of hazard, frequency with which hazard is encountered, extent to which appropriate user action is necessary to avoid hazard
Communication impediments	Environmental Stimuli	What other environmental stimuli are likely to be present?	Other related and unrelated communications, user's primary task, ambient light, noise
	Interference	Will anything interfere with the communication being delivered as intended?	Malicious attackers, technology failures, environmental stimuli that obscure the communication
Personal Variables	Demographics and personal characteristics	Who are the users? What do their personal characteristics suggest about how they are likely to behave?	Age, gender, culture, education, occupation, disabilities
	Knowledge and experience	What relevant knowledge or experience do the users or recipients have?	Education, occupation, prior experience
Intentions	Attitudes and beliefs	Do users believe the communication is accurate? Do they believe they should pay attention to it? Do they have a positive attitude about it?	Reliability, conflicting goals, distraction from primary task, risk perception, self-efficacy, response efficacy
	Motivation	Are users motivated to take the appropriate action? Are they motivated to do it carefully or properly?	Conflicting goals, distraction from primary task, convenience, risk perception, consequences, incentives/disincentives
Capabilities		Are users capable of taking the appropriate action?	Knowledge, cognitive or physical skills, memorability, required software or devices
Communication delivery	Attention switch	Do users notice the communication? Are they aware of rules, procedures, or training messages?	Environmental stimuli, interference, format, font size, length, delivery channel, habituation
	Attention maintenance	Do users pay attention to the communication long enough to process it? Do they read, watch, or listen to it fully?	Environmental stimuli, format, font size, length, delivery channel, habituation
Communication processing	Comprehension	Do users understand what the communication means?	Symbols, vocabulary and sentence structure, conceptual complexity, personal variables
	Knowledge acquisition	Have users learned how to apply it in practice? Do they know what they are supposed to do?	Exposure or training time, involvement during training, personal characteristics
Application	Knowledge retention	Do users remember the communication when a situation arises in which they need to apply it? Do they recognize and recall the meaning of symbols or instructions?	Frequency, familiarity, long term memory, involvement during training, personal characteristics
	Knowledge transfer	Can users recognize situations where the communication is applicable and figure out how to apply it?	Involvement during training, similarity of training, personal characteristics
Behavior		Does behavior result in successful completion of desired action?	See <i>Norman's Stages of Action, GEMS</i>
		Does behavior follow predictable patterns that an attacker might exploit?	Type of behavior, ability of people to act randomly in this context, usefulness of prediction to attacker

Table 2.2: The main components based on Human in the loop security framework (HITL) by Cranor (2008).

Simultaneously, Cranor also proposed a four-step iterative process, whereby human threats to system security are identified and mitigated, as shown in Figure 2.12. She claims that HITL framework to be used as part of this iterative process. Based on Figure 2.12, task identification step would involve system designer to identify whether the systems rely on human in order to perform security functions and task automation step deal whether security functions would be able to partially or fully automate. On the other hand, the failure identification step focuses on identifying the failure of security functions (i.e. by using HITL and user study) whilst failure mitigation step

finding method to prevent failures by determining how users can be supported to perform these task. In order to assess this framework from security warning views, Cranor (2008) gave an example by using anti-phishing tools to apply to this framework (i.e. passive warning indicators in web browsers were not effective to prevent users from phishing sites). She concluded from her findings that one failure identification step revealed the need to find ways to correct users' imprecise mental model about phishing, and she proposed to focus on the links to educational materials to improve anti-phishing warnings.

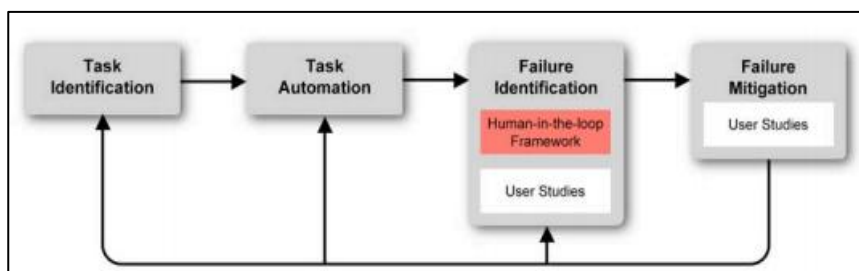


Figure 2.12: Human threat identification and mitigation process originally by (Cranor 2008)

Having understood the human threat identification and mitigation process, Cranor (2008) has recommended three high-level strategies to build a secure system for human beings to use, as follows:

- i. To find ways to ensure human out of the loop and build systems without involve human in security critical functions;
- ii. To build systems that are intuitive and find method to make it easy to use;
- iii. To teach human on how to perform the security critical task.

She argues that to ensure the effectiveness of the proposed strategies, we cannot rely only to one strategy but a combination approach must be adopted. For the purpose of this thesis, the author has decided to use the combination approach. This thesis seeks to combine strategy two and three. Strategy one is not chosen, because the author believes that to build a system security without human intervention is cumbersome and cause many problems especially when the mechanism failed. This is agreed by Bellotti & Edwards (2001) and Isbell & Pierce (2005) who revealed usability issues occurred and users were exposed to incorrect threat assessment. On the other hand, combination of strategy two and three seems to be more practical and reasonable. Therefore, the next sections are expected to provide evidence of these combined strategies.

2.11.3 Security automation for security warnings

According to Edwards et al. (2007), security automation can be defined as a system or technology that effectively removes the end users decision process. Therefore the decision making is made by others such as the system administrator or a suitable expert. This is supported by Nielsen (2004) when he mentioned that users should not be burdened to defend themselves. From the perspective of information security management, security automation would reduce the human intervention and thus it increases the cost and complexity of security (Montesino R and Fenz S, 2011). With this approach users should not need to make security critical decisions and should not encounter disruption whilst completing their regular tasks.

Edwards et al. (2007) introduced “the Spectrum of automation approaches” that explained the range of strategies on how security automation for end-users can be implemented as shown in Figure 2.13. The fixed policy indicates where security decision policies are comprised in tool and application (e.g. Karberos server – security kernel implementation). The customise policy allows the policy to be customised (e.g. control by the system administrator) whilst the dynamic policy works in a flexible manner with dynamic policy adaptation (e.g. Bayesian spam filters).

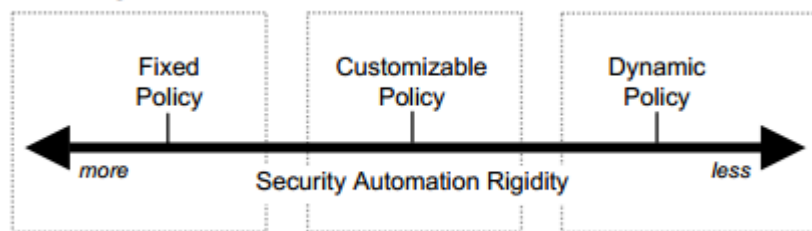


Figure 2.13: The Spectrum of automation approaches

From the scope of security warnings, it can suit the spectrum when the security warnings are identified. In one particular system, end users do not have to make any decision with regards to the security warnings when the system itself is able to do it for them. However, there are many challenges that limit automation such as the social and environmental contexts of security and the effects of security automation on users. It can be argued that at the end of the day, users are the ones who use the system and they

should be able to understand the current context of event they are dealing with. Thus, a users' intervention is still compulsory in most of the scenarios.

2.11.4 System visualisation for security warnings

System visualisation is used as a tool to provide more information to end users to bridge the gap of understanding of how each process works in the computer system. However, not much focus has been given to system visualisation in a security warning perspective. Stoll et al. (2008) introduced "Sesame" an interactive visualisation concept in order to help non-expert users make informed security decisions. It provides a clear picture by utilising the desktop metaphor in order to show the background process when users wants to make security decision. The result of system visualisation is pretty convincing as system activity, configuration and action can be seen in an understandable form (De Paula et al. 2005).

Generally this system works to cater for two groups of users, namely expert and non-experts. For experts, visualisation tools and text-based tools are used whilst for non-experts, tools for specific activities and for specific threats are used. This suggested that the system visualisation caters for the needs based of end-users in a way that suits their understanding and technical capabilities. "Sesame" implemented a direct manipulation model that helped users comprehend scenarios (i.e. leveraging end-users knowledge). From a security warnings context, users will be able to understand the process from the beginning of receiving security warning, the process when the decision is going to be made up until the informed decision is made. All visual elements with step by step flows will be revealed so that users realise what is happening (i.e. foreground and background process). System visualisation presented encouraging results but it is more useful for non-experts. To implement this in a computer system is a challenge as there are various types of warnings derived from the operating system, browsers and other applications. It will also involve security and privacy issues. Thus, these challenging scenarios suggest that more research is needed to reveal the suitability of system visualisation within this context.

2.12 Evolution of security warnings studies

Computer security warnings become part of the development process as they provide a method to warn users of possible threats in the system. Thus, the security warning also shared similar impacts in the sense of having changes to suit its current purposes and context. Normally changes will reflect the design or layout, the colour schemes and additional functions to fix the previous problems (e.g. fixing bugs and usability issues). The previous section introduced frameworks and approaches that have been used to improve security warnings. However, the trend to improve security warnings varies as there is no standard method that has been used. Thus, it opens opportunities to explore how security warnings can be designed to accommodate the needs of end-users. This section highlighted the previous and current developments of how to improve security warnings mainly on the usability aspects and also other related approaches in warnings design.

2.12.1 Improving the usability aspects of security warnings design

Nodder (2005) highlighted a Microsoft case study on types of dialogues in security warning contexts (i.e. consent dialogues, ActiveX dialogues, file download dialogues and pop up blocking). He proposed a design solution based on users' behaviour based on usability studies that he had conducted. He argued that the previous version of Windows XP and XP SP1 as depicted in Figure 2.14 did not help user to make decision as the question presented mislead the users. He further explained the text "You are downloading the file:" took over the main content of the dialogue which was the question "Would you like to open the file or save it to your computer?"

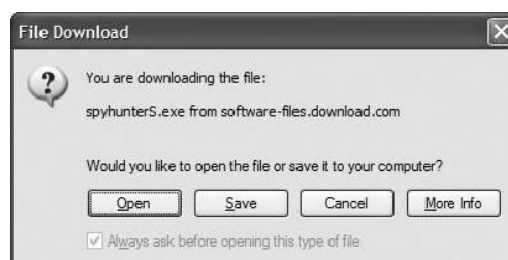


Figure 2.14: The original File Download dialogue (Nodder, 2005).

He then pointed out that Microsoft adopted the positive approach of improving previous warnings by enhancing the warning dialogue (i.e. button defaults, button labels, primary text, evidence and assistance text) as depicted in Figure 2.15. It may be noted that the question and information were available straight away, as compared to the previous security warning. This version of security warning is able to comprehend users more easily especially when it related to trust decision process.



Figure 2.15: Redesigned File Download dialogue (Nodder, 2005).

Raja et al. (2009) introduced a new version of the Windows Vista firewall by revealing the hidden context to end-users. The prototype was designed to provide contextual information so that they realised the security state of the current network connection in their computer system to make them better understanding. Their study utilised 30 participants from the university and general public. The results suggested that a correct design interface in respect of usability (firewall) helped users to develop a correct mental model and it also increased users' understanding of the firewall configuration.

Bravo-Lillo et al. (2011b) used examples from 29 security warnings from operating system and application software and conducted open-ended interviews with advanced and novice users in relation to usability of security. Their results produced a clear mental model of novice and advanced users perceptions of warning dialogues. Their study revealed that warnings design should also deal with the wrong diagnosis (i.e. novice users always tend to over diagnose the computer virus problems).

Hardee et al. (2006) conducted a survey with 56 respondents to understand the differences of how they made decision with regards to computer and non-computer security domains (i.e. an examination of computer security decision making).. Their study revealed that users' perceive gain-ratio consistently and not in loss-ratio in both

domain (i.e. time/convenience, protecting information, protecting property, social/emotional, protecting self and others). They suggested utilising attributes or features in security warnings (i.e. explain the potential loss explicitly and usage of explicit text).

2.12.2 Related approaches to improve security warnings design

This section describes useful methods that have been implemented by other research communities in security warnings implementations. Thus, understanding how end-users perceive and understanding the warnings is fundamental in order to design and to develop features that end-users use. It can be noted that various techniques had been used. However, based on the author observation, none had used one specific approach.

Keukelaere et al. (2009) conducted a study with 32 non-technical participants (i.e. any person that had no significant with computer security expertise, engineering or computer background) by implementing an e-mail client simulation known as Adaptive Security Dialogues (ASD). ASD worked by matching the complexity of one particular dialogue with the risk associated, as shown in Figure 2.16. The study revealed that with ASD, fewer people immediately open the attachment file and the majority of people spend more time considering their decision.

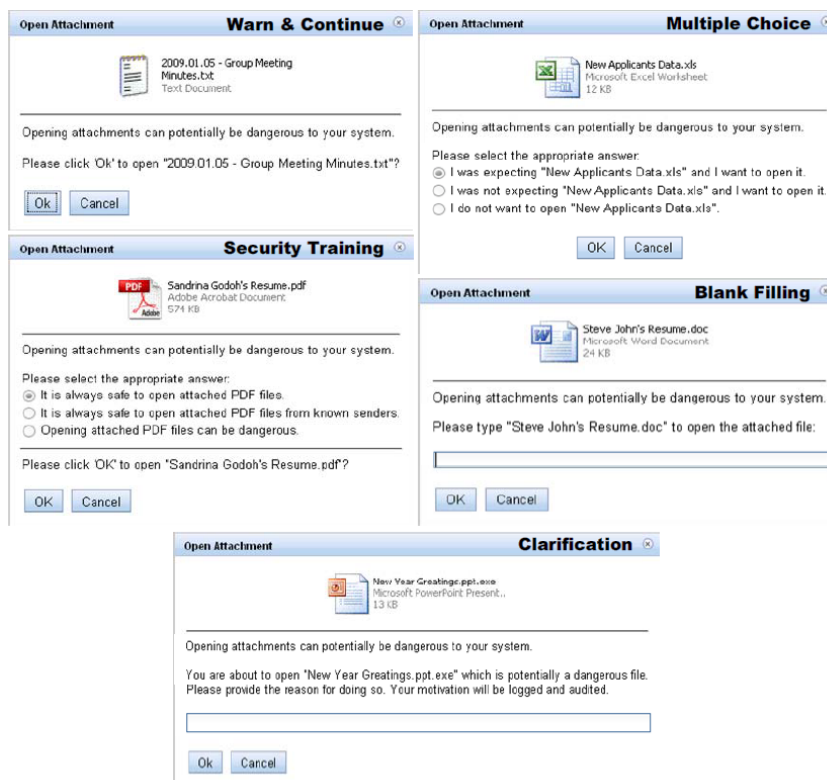


Figure 2.16: Five types of dialogues boxes namely warn and continue, multiple choices, security training, blank filling and clarification (Keukelaere et al. 2009).

Edwards et al. (2007), meanwhile, introduced the concept of security automation where user security decision process is removed from one particular system. Using empirical evidence from social and technology perspective, they suggested guidelines for automating appropriately albeit there are some obstacles that developers need to cater on the first hand. They realised that this technique is worthwhile in theory, but in practice there are many limitations.

Bravo-Lillo et al. (2011) conducted an online survey study that involved 733 participants using four contexts of warning (i.e. encryption warning, attachment warning, address book warning and certificate warning) based on low and high risk scenarios. Then they created two groups of redesigned warning (i.e. warning based on mental model and warning based on guidelines) and improved the four contexts of warning that had been presented. Their study revealed that the design changes were able to improve understanding, motivation and the tendency for end-users to choose better option, but further work need to be done so that users are able to differentiate between low and risk conditions.

Kauer et al. (2012) conducted a laboratory study and a survey with different certificates browsers security warnings (i.e. Firefox 2, Firefox 4, Internet Explorer 6 and Internet Explorer 9) whilst accessing websites which involved 30 participants. They revealed that in order to improve the warning, the risk should be communicated clearly to the end-users. The communication of risk (i.e. wordings) is very important to deliver the message. Therefore, they suggest that it should be formulated in terms of technical risks, and also personal risks, to make it more convince.

On the other hand, Raja et al. (2011) made use of the comparison between the Comodo's original warnings and their improved version of warnings with 60 participants using computer user study and questionnaires. The design of their improved version warning was based on the physical security metaphor and humans in the loop framework (HITL) as discussed in aforementioned section. Their study revealed that the majority of their respondents preferred to have the improved version of warnings, because it were more understandable, and that it was better to communicate the risks and promote users to make safe decisions.

Brustoloni & Villamarín-Salomón (2007) introduced polymorphic and audited dialogues to improve security warning decisions. Twenty participants who had previous work experienced participated in this role-played laboratory session. All conversations and processes were recorded. Their study revealed that these techniques helped users to make better security decision, as these dialogues were easy to understand and provided good guidance). Polymorphic dialogue changed the order of the layout and delayed options provided every time the user encountered warnings, whilst audited dialogue warned or penalised users' based on the decision provided by referring it to auditor.

Villamarín-Salomón and Brustoloni (2010) proposed security reinforcing applications (SRAs) that rewarded users based on their secured behaviours using 24 participants in role-played laboratory studies. They demonstrated that SRAs are able to improve users' secure behaviours by accepting justified risks and rejecting the unjustified risks.

Maurer et al. (2011) introduced a new concept of warnings, which appeared at the same time as user wanted to enter data in online forms. To be more precise, the warning only

appeared if the data type was critical (e.g. credit card and password) in order to prevent phishing websites. 24 respondents were involved in this computer role-based lab study, in two groups (i.e. experimental and control), in which a special plugin was installed. The results indicate that this concept was promising especially to non-expert participants. They claimed that this was the first step to reducing the frequency of the warnings and minimizing habituation.

Stoll et al. (2008) conducted a user study and interview with twenty non-expert participants with regard to the security decision making process and introduced Sesame. Sesame used system visualisation to show to end-users the background process of one particular incident until users able to make decision. Their study revealed that majority of respondents able to make better informed security choices.

Based on all of these findings it may be suggested that there are many methods to improve the presentation of security warnings in order to comprehend end-users. It may be noted that various techniques have been used to assess end-users' understanding about computer warnings in various contexts (i.e. web browsers and dialogue box). Having understood these useful techniques, this thesis now highlights the classification of improving security warnings based on the identified findings.

2.13 The classification of security warnings approaches

Previous sections provided evidence of how security warnings design can be improved in relation to usability and other suitable approaches. It is useful to get a clear picture of how each approach can be grouped or classified based on the techniques that had been used. It can be concluded that the similarities among all of the findings to improve security warnings were based on these four classifications:

- i. Redesign the warnings by utilising the features and available information in the warnings
- ii. Redesign the warnings by behaviour modification.
- iii. Redesign the warnings by changing the presentation or layout
- iv. Redesign the warnings by the adaptation of warnings

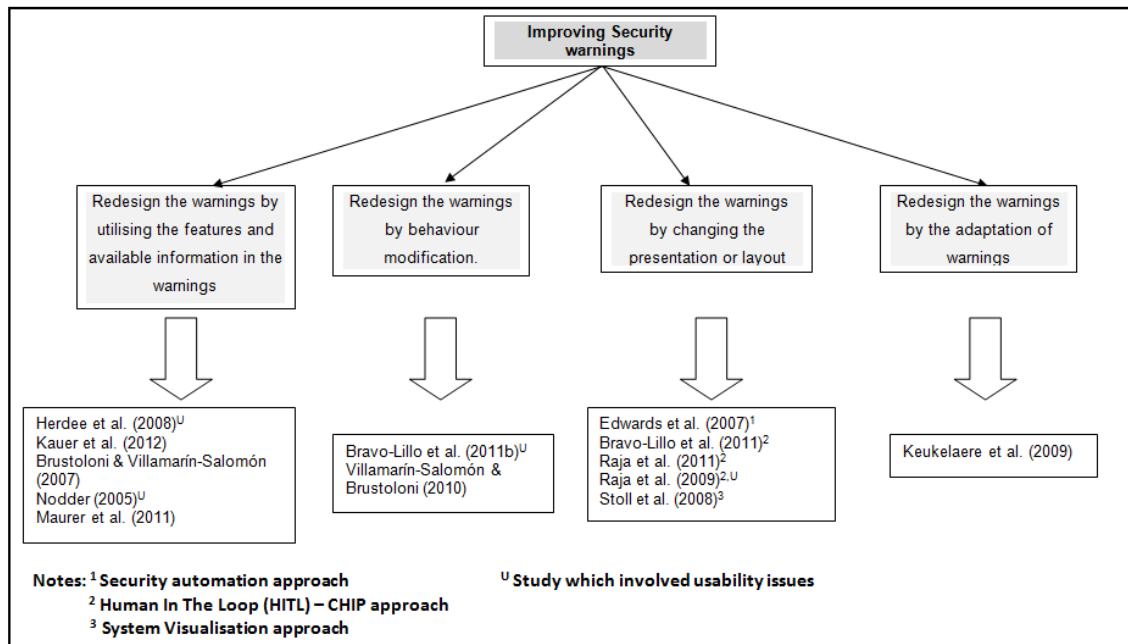


Figure 2.17: Classifications approaches to improve the security warnings

Based on Figure 2.17, four classification approaches were used to improve security warnings. These classifications were based on the observations and understanding of how each study had been conducted. It can be noted that most of these findings were focusing on redesign warnings to ensure that the interface of the warnings was more understandable by utilising the features, available information and changing the layout or presentation. However, focus was given to “redesign the warnings by changing the presentation or layout”. It can be noted that findings within this classification had used the same methodology which had been explained in the earlier sections. On the other hand, four findings determined to focus on usability aspects of security warnings as depicted. With regards to “redesign the warnings by the adaptation of warnings” only one study had been found. Keukelaere et al. (2009) focussed on improving security warnings dialogs by producing a new architecture in order to promote a new type of interaction called “Adaptive Security Dialogs” (ASD). As the underlying cause of the security warnings problem had been addressed, it indicates a necessity to design security warnings in a way that can work within all of these classifications. The next section explains the opportunities which need further research and focus.

2.14 Warnings potential directions

In reality, end-users are confronted with many challenges in using the computer and applications. As the technology evolve rapidly, not every user able to cope with its fast momentum. This poses difficulties to end-users to use computer and its application in secure manner. For instance, most organisations kept their applications and software updated with the latest version. This impacts end-users, especially to laymen groups, as they might only familiar with the previous version they used instead of the most recent. As a result, end-users are still baffled when faced with the new changes. They must therefore learn about new features or functionality which will impact their decision especially when it related to security decisions. On the other hand, developers still left the decision making specifically security decision to the end-users. This also posed potential threats of becoming the victim of malicious attack if users choose inappropriate decision. Hence, to design one particular security warning is not an easy task. The warning should be able to explain the possible risk and able to convey users so that they behave in secure manner.

Evidence in Chapter 2 highlighted the need for further research in this field of study by emphasizing six issues or problems in security warnings implementation (i.e. attention towards warnings, understanding of warnings, use of technical wording on warnings, evaluation of risks from warnings, user's motivation towards heeding warnings and user's assessment of the implication of warnings faced by end-users. Research communities highlighted these as common problems when users interacting with security warnings. It gave early indications on the importance to investigate and further probe how security warnings can be improved to meet end-users needs. Therefore, it is useful and essential to understand the methods or suitable approaches to improve the security warning implementation. In order to understand and to compare on the approaches, Table 2.3 describes summary of studies that focus on how security warnings can be improved as described in the aforementioned section.

Authors	Methods/Techniques
Nodder (2005)	Proposed a new design of warning based on users' behaviour
Raja et al. (2009)	Proposed a new design of firewall interface that helped users to develop a correct mental model and increased users' understanding on firewall configuration.
Bravo-Lillo et al. (2011b)	Introduced the concept of mental model on how novice and advanced users assessed security warnings.
Keukelaere et al. (2009)	Introduced Adaptive security dialogues (ASD) by matching the complexity of warning dialogues and the risk associated
Edwards et al. (2007)	Introduced security automation concept where decision is made by the system
Bravo-Lillo et al. (2011)	Proposed that design changes able to help end-users to make better decision in relation to warning interaction.
Kauer et al. (2012)	Proposed that the risk should be communicated clearly in warning in order to deliver the message in secure manner,
Raja et al. (2011)	Proposed a design solution based on the physical security metaphor and Human In the Loop (HITL),
Brustoloni & Villamarín-Salomón (2007)	Introduced Polymorphic and audited dialogue to improve security warning decisions.
Villamarín-Salomón & Brustoloni	Introduced security reinforcing

Authors	Methods/Techniques
(2010)	applications (SRAs) which rewarded end-user based on their behaviours.
Maurer et al. (2011)	Proposed new concept of warning design where it appeared together when user wanted to key in the data online.
Hardee et al. (2006)	Suggested that attributed or features should be utilised in security warnings
Stoll et al. (2008)	Introduced Sesame – visualisation system which showed to end-users the background process which always hidden from them.

Table 2.3: Summary of studies on how to improve security warnings

Whilst the preceding sections within this chapter highlighted useful techniques to improve security warnings, apparently, there is no complete version of security warnings which are able to solve every single problem experienced by the end users. Table 2.4 summarises the previous research mapped to the common problems.

Common problems with security warnings	Proposed solutions
Attention towards warnings	Bravo Lillo et al. (2011b), Raja et al. (2009), Nodder (2005), Keukelaere et al. (2009), Raja et al. (2011), Maurer et al. (2011) and Hardee et al. (2006).
Understanding of warnings	Bravo Lillo et al. (2011b), Raja et al. (2009), Nodder (2005), Keukelaere et al. (2009), Kauer et al. (2012), Edwards et al. (2007), Bravo Lillo et al. (2011), Raja et al. (2011), Brustoloni & Villamarín-Salomón (2007), Hardee et al. (2006) and stoll et al. (2008).
Use of technical	Bravo Lillo et al. (2011b), Raja et al. (2009), Nodder

Common problems with security warnings	Proposed solutions
wordings	(2005), Keukelaere et al. (2009), Raja et al (2011) and Hardee et al (2006).
Evaluation of risks from warnings	Bravo Lillo et al. (2011b), Raja et al. (2009), Nodder (2005), Keukelaere et al. (2009), Kauer et al. (2012), Maurer et al. (2011), Raja et al. (2011) and Stoll et al. (2008).
User's motivation towards heeding warnings	Bravo Lillo et al. (2011b), Bravo Lillo et al. (2011), Raja et al. (2011) and Stoll et al. (2008).
User's assessment of the implication of warnings	Bravo Lillo et al. (2011b), Raja et al. (2011), Brustoloni & Villamarín-Salomón (2007), Villamarín-Salomón & Brustoloni (2010) and Stoll et al. 2008).

Table 2.4: Common problems with security warnings and proposed solutions

In general, there are four classification approaches of how security warnings can be improved. The first classification is “redesign the warnings by utilising the features and available information in the warnings” in which security warnings are enhanced with suitable used of icons, words, colours, technical jargon and useful information to comprehend the meaning of the warning. Most of the researchers realised that the available features on security warnings should be utilised and used accordingly (McDougald & Wogalter 2011, Hardee et al. 2006, Whalen & Inkpen 2005 and Kauer et al. 2012). However, this approach is unlikely to succeed by itself due to the issue of habituation where users have been exposed to similar warnings. The second classification is “redesign the warnings by behaviour modification” aimed at engaging users to make more appropriate secure decisions. Bravo-Lillo et al. (2011b) claimed his mental model warning response behaviour is useful to differentiate between how advanced and novice users think about security warnings. Camp (2009) also agreed that it is important to understand the mental model so behaviour could be modified to improve communication about computer security risks. Although it is essential to

modify the behaviour, it is better if it can be done with other approach to support one and another.

The third classification is “redesign the warnings by changing the presentation or layout”. Raja et al. 2009 improved firewall warnings by revealing the hidden context with their interface design. Later, they produce a novel approach to designing firewall warnings using a physical security metaphor in which it conveyed the risks and encouraged safe behaviour when compared to standard warnings (Raja et al. 2011). Stoll et al. (2008) introduced a new dimension of security user interface called Sesame where the background system is visualised to end-users so that they can see the background process for better understanding. However, the layout or interface changes can only work in best condition providing that the attributes involved are understood so that users will be able to comprehend the risk involved (Hardee et al. 2006 and Sharek et al. 2008).

The final classification is “redesign the warnings by the adaptation of warnings”. Instead of changing the layout or presentation, the warnings can be adapted to match the end-users requirements. Keukelaere et al. 2009 introduced a new approach which combined a new architecture and a new method to communicate using security dialogues called Adaptive Security Dialogs (ASD). To the best of their knowledge, no previous study had addressed the various level of user risk and correspondingly adapted to their dialogues implementation. In Adaptive Security Dialogs (ASD), the adaptation of warning dialogs was based on the level of user risk. Security warning dialogs layout were presented differently based on the type of the file. For instance files with an .exe extension will be treated differently to those with a .pdf extension (i.e. where in this case the adaptation involve was based on the risk of file type).

Although most of these proposed solutions were proved to work effectively, none of them were perfect. They either required a combination approach from others to support or it can only solve the problems at that particular time (i.e. only during their experiments or users study). Given the problems and proposed solutions regarding common security warning issues as shown in Table 2.4, suitable approach from Figure 2.17 should be determined to further this research. The state of the art in security

warnings study is to ensure that warnings play a vital role in order to warn users about possible dangers and to promote safe actions. In addition, it should be able to advise the users on the current contexts of the warnings which users are facing. It can be seen that as a possible solution to further this research is the combination of approaches in the preceding sections.

The absence of a focus on the design of a meaningful approach as a mean of a new way interaction (framework/architecture) to provide an effective security warnings design to suit end-users need is clear. Only one previous study has highlighted this and focused on security dialogs. Given the facts that the author shared similar underlying intention to improve security warnings in the security dialogues context, the author will produce his own architecture based on the previous implementation of ASD as the basis of study. As the security warnings in dialogue boxes continue to be used as the medium of interaction to deliver warnings and information, this context is adopted as the main focus of this study. McGrath et al. (2006) argues that dialogue boxes tend to be ineffective in informing the user about threat and practicing safe behaviour. Krol et al. (2012) conclude that security warnings in this form are largely ineffective. Whilst the continuous problems still exists, to date, warning dialogue box are still used as a vital form of context (Microsoft 2010). In addition, end-users encounter many versions of dialogues boxes via web browsers that became a popular target for criminal to exploits the vulnerabilities (Symantec 2012). The impact of users' decisions and choices in response to such dialogues may significantly impact the security and the protection of computer systems. If a wrong decision is made, then it could jeopardise the security of the computer as a whole (i.e. confidentiality, integrity and availability). From the author's experiences and observations, most security warnings presented whilst using computer are in dialogue box contexts, regardless of any software or applications used. Users are likely to be more familiar with dialogue box contexts, as they appear more frequently than other types of context. As the dialogues boxes are particularly prevalent for computer users, this are will be further investigated as the focal point of study.

To be precise, in Adaptive Security Dialogs (ASD), the adaptations of warnings dialogues were based on the level of user risks. However, in the new proposed architecture more information is given to users by utilising the help function on security

warnings. Thus, warnings will be presented to users based on their preferences rather than having a standard version unless it has been chosen by users in the first place. This work opens a new dimension of how security warnings can be improved by addressing their own design principle and creating warning interface based on end-users needs. The issues that need further research and focus can be listed under the following areas:

- i. Understanding the current trend of security warnings
- ii. Usability aspects of security warnings
- iii. Utilising the available features and available information
- iv. Usable help technique

Although many problems faced by the end-users in relation to security warnings have been highlighted in the preceding section, it is useful to gather some more evidence to see the latest trend from the end-users and to determine if the problems still persist. This also gives more opportunity to ask alternative questions and to aim for different types of participants (i.e. can be based by gender, age, location, nationalities and security experiences). Then, an exploration on usability aspects will be given to the more specific types of warnings (i.e. security warnings dialogues) to assess users' understanding, effectiveness and efficiency of warnings and finally users' satisfaction. This should provide solid evidence of how end-users perceive warnings in daily routine activities in relation to usability.

One of the possible classification approaches is to utilise the available features and available information. At this stage, all features in the security warning must clearly communicate to the end-users especially in relation to the risk they they encounter. Probing end-users' thoughts about what features or information are easily understood or cause confusion will help to find a possible way of improving security warnings. Finally, to provide a proper help which will be better than the available conventional help function in current security warnings (e.g. via link or button). It can be seen that little effort has been invested or given to the usage of help function in one particular warning. Normally, upon clicking this function, users will be guided with some useful information about current state of the applications. According to Herzog & Shahmehri

(2007) online help is among the prominent user help techniques in many applications. When pressing the help button, users will be presented with a dialogue box window with useful information. As this states, the only guidance that users can rely on is the help function. Help functions become the only source available to help users in decision making process or comprehend them with current problems they encounters (i.e. in the dialogue box contexts). Herzog & Shahmehri (2007) made a table comparison on usable help technique, as presented in Table 2.5. They claim that these were the important criteria that arose in applications and from the context when one particular security system can be called usable. The series of ten questions originally derived from Baecker et al. (1991) were used to answers questions that always pondering end-users mind upon receiving warnings. These questions were normally asked by the users as generally were the sets of questions that always pondering in users’ mind when using one particular application.

	Online Help	Context sensitive help	Light-weight help	Sophisticated tutorial	Wizard	Safe staging	Social Navigation	Built in security	Combined approach
Informational What can I do with this application?	Yes	Maybe, upon start-up	No	Yes	No	Maybe	No	No	Maybe
Descriptive What is this? What does this do?	Yes, after searching	Yes immediately	Yes, on a simple level	No	No	Yes	No		Maybe
Procedural How do I do this?		Chances are good	No	Yes	Yes, the wizards shows/guide how to do it	Yes	No		Maybe
Interpretive What is happening? Why did this happen? What does it mean?		Maybe	No	Maybe	No	Maybe	No		Maybe
Navigational Where am I? Where have I come from and gone to?		Maybe	No	Maybe	Yes by numbering the stages of the	Chances are good	Maybe		Maybe
Choice What can I do now?		Chances are good	No	Yes	Yes by showing the next step		Maybe		Maybe
Guidance What can I do now?			Yes if shown how previous user have progressed and where the current user came from	Maybe					
History What have I done?		No	No	No	Maybe		Yes by making previous steps accessible	No	Maybe
Motivational Why should I use this program?	Yes	Maybe, upon start-up	No	Maybe	No	No	Maybe		
Investigative What else should I know?	Yes, after searching	Maybe	No	Maybe	Maybe	Yes show other available stages	Yes shows other possible path	Maybe	

Table 2.5: Which user questions can be answered by which user help technique originally by Herzog & Shahmehri (2007).

Table 2.5 was amended with the additional field of “combined approach”. The grey box indicated as unable to answer the question whilst the white colour box indicated as “Yes” or “Maybe”. On the right hand side (i.e. in a blue colour box) is the additional information noted as “maybe” which is one of the focus of this thesis. This thesis made use of all possible approaches to answer the listed questions, based on the new security

warning presented in the evaluation and validation process later on. The possible approach here can be referred to method to improve warning layout in order to provide all answers based on the depicted questions. It is not necessarily rely on the questions and answers type of interaction. However, some other useful techniques are considered (e.g. expressing the warnings using signal words and icons, usage of colours to get attention, explained technical jargons to avoid confusion, tooltips information to provide quick information and explaining resources using a simple expression).

By using the new approach, it is expected that it can covers all questions features as presented, and even be able to improve the quality of warning presentation and usability of security warnings. As presented on Table 2.5, the “combined approach” field was highlighted with blue colour background with “Maybe” wording to indicate the possibility of the proposed technique is workable (i.e. which will be conducted at the final stage of user studies).

Evidences suggested that changes on warning design significantly able to improve warnings implementation. The design changes can be a novel solution to provide users with information and secure decision making process. Therefore, enhancing usability in the context of security warnings is needed. This is because problems with usability will identify the difficulty to interact with computer system from the end-users perspective in relation to the cause, location and the explanation that derived from the interface (Cockton et al. 1999). Therefore, this thesis seeks to investigate further all four elements mentioned earlier. A series of user studies is presented in the next few chapters to further clarify, answers and improve the current implementation of security warning (i.e. thus answer the “combined approach” as mentioned).

2.15 Study approach

This thesis seeks to focus on security warning dialogues in web browsers. Having assessed all evidences in the preceding sections, the author made use the ‘Human threat identification and mitigation process’ (Cranor, 2008) as initial guidance, as depicted in Figure 2.12. In this process, Human in the Loop (HITL) framework was introduced in the Failure Identification process. As HITL was developed to focus on security

communications (i.e. warning dialogue, notices, status indicators, training and policies), it similarly suit with author focus on security warning dialogues. Thus, this thesis will use a similar approach as the basis to identify problems that users encountered whilst dealing with system security and then mitigate the risks using a propose technique. Based on Cranor’s approach in the aforementioned section, some amendments have been made in order to suit the aims of this study, as presented in Figure 2.18. The amendments were based on the rationale that on every task involves it should be at least user study been conducted (i.e. except in task automation). This is to ensure that there are sequence and consistency in conducting the research study. In addition, usable help technique and Microsoft Guideline also had been used as the basis and to support the user studies. The author believes that these two additional elements are essential in order to provide some guidance on elements that should be considered in improving security warnings.

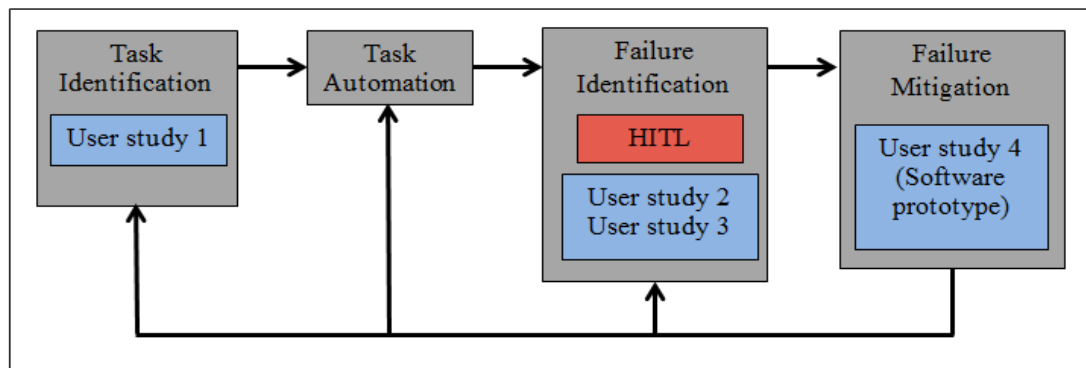


Figure 2.18: Amendments of human threat identification and mitigation process

Table 2.6 further explains the approach that has been taken based on four conducted user studies:

Phases	Descriptions
Task Identification	This stage identifies systems that rely on humans to perform security-related function. User study 1 was conducted to understand in more detail the problems that end-users can face related to usability and perception of information security issues. Further details are discussed in Chapter 3.
Task Automation	This stage tried to find methods to partially or fully automate the security-related function. As this research

Phases	Descriptions
	focuses on security warning dialogues where user intervention is necessary to make a secure decision, this stage will not form part of the focus.
Failure Identification	This stage tried to find ways on how end-users can be better supported in terms of handling security warnings. HITL here is basically the framework that been proposed by Cranor (2008). This thesis determines to use this framework by asking users' series of questions (i.e. as shown in Table 2.2) in user study two and three. Based on the compilation of evidence presented from user studies one to three, the author is able to identify the problems of computer warnings and proposed possible solution in Chapter 6.
Failure Mitigation	This stage tries to find method to prevent problems occurring. One useful approached was presented in Table 2.5. Using this approach and the proposed new method (i.e. automated adaptation of security warnings), this thesis seeks to improve the presentation of security warnings (as discussed in Chapters 6 and 7).

Table 2.6: Human threat identification and mitigation with the propose study

2.16 Conclusions

This chapter has highlighted users' interactions with security tools and technologies and approaches related to security warnings studies. It covers the overall background studies of security, usability, perception, trust, HCI and GUI. Security and usability becomes the focal point when assessing the users' interactions with security tools and technologies. With many new threats, it indicates the need to ensure that end-users are able to interact with such tools in a secure manner. It can be concluded that most of the researchers have used various method to improve security warning and even some relatively propose a new concept (i.e. matching complexity of risks, security automation,

rewarded security behaviour, mental model). Thus, there is no specific single method that has become mandatory for developers to use.

Problems with regard to usability remain one of the concerns that affect users' understanding upon dealing with security tools and technologies. The fast pace of technological growth has forced users to keep up to date, which is generally cumbersome for laymen or non-technical savvy groups. Therefore, Human Computer Interaction with the usage of Graphical User Interface (HCI) is readily available as a mediator between user and machine (i.e. present instruction and information in acquit manner). A significant aspect of usability is when users have to make a decision. A significant type of decision that they have to make is when the system issues them with computer warnings, because their impact on the decision may be significantly greater where security and protection of the system and information are concerned.

Motivated by the results from other researchers to improve security warnings, this thesis makes use of the approach in the aforementioned section, and conducted series of user studies to further explore security warnings in details. User study 1 is presented to examine general understanding in terms of usability and perception as a basis of study (i.e. explained in Chapter 3). Even though in the earlier section, the problems with security warnings had been highlighted, the author would like to conduct again a survey (user study 1) with the aims to gather the latest evidences from end-users experiences. In addition, the survey will be able to cater different demographic and scenarios facing by them. On the other hand, user study 2 and 3 focus on assessing users' understanding about security warning in practical and wider contexts (i.e. explained in Chapter 4 and 5). To be precise, user study 2 is focused on the experiences that the users had with the software to capture the security warning (i.e. dialogue box context) manually and gathered evidence on what they understand about the features of particular security warnings. It can be confirm that based on the author knowledge, this approach has not been conducted before by researchers in security warnings. The author uses this approach with the rationale to gather real exposure on what end-users belief on security warnings. This would be useful to strengthen the findings on the problem that end-users encountered with security warnings. User study 3 confirms whether information presented on the warnings are enough for them to make a decision in real-time context.

It gives end-users real-time experience to express their satisfaction whilst dealing with security warnings. Finally, based on the outcomes of the series of user studies, the new architecture namely Automated Security Interface Adaptation (ASIA) was developed to enhance current security warning implementation with the similar underlying as in the ASD implementation (i.e. explained in further detail in Chapter 6) and later, the evaluation with regards to the usability will be conducted as a final stage (i.e. further discussion in Chapter 7).

CHAPTER 3

Examination of Comprehensibility of Issues in Information Security

3 Examination of Comprehensibility of Issues in Information Security

3.1 Introduction

It is useful to gather information from an end-user's perspective when dealing with computer tools and technologies so that a clear understanding of their perception and knowledge on issues of information security in general can be gathered as the foundation of this research. In general, people tend to think that they are not at risk from any particular hazard and they choose what to fear and how much to fear with it (Oltedal et al. 2004). A survey study has been the preferred research tool of many scholars for initial research to establish the basis or foundation in most user studies (Stanton et al. 2005, Furnell et al. 2006, Jones et al. 2007 and Mannan & Van Oorschot 2008). To determine the nature of the difficulties encountered by users, this chapter presents a survey study aimed at examining the perception and usability of information security, with security warning contexts being the focus of scenarios (i.e. phishing warning and dialogue box warning). This survey then became the basis for conducting practical trials in the later stages of the research.

This chapter describes a general investigation on the general and specific issues of computer security issues. The issues raised include the general usage of the computer, operating systems, usability, computer protection and case studies using a security warning dialogue interface from different web browsers. These identify insights regarding the problems that end-users usually face, and some potential solutions. Some users demonstrated that they knew how to make a decision, whilst others did not. Users are the people who use security technologies and a standard should be implemented that are usable and works efficiently. Having said this, many issues were raised in terms of how users reflect on the usage of such features, for instance security notification for users to make decisions. Security notifications are used to inform users about any possible computer problems that users need to address. In order to avoid incorrect or dangerous decisions, end-users need to understand the context of the problem before they make a decision as a wrong decision could jeopardise the security and protection of the computer. Furnell et al. (2006b) listed a series of common problems with regards to the usage of security features such as usage of technical terminology, unclear

functionality, lack of visible status, forcing uninformed decision and lack of integration. This highlighted that end-users face real difficulties caused by the design and implementation of security warnings.

Every web browser has a different method to present warnings. Thus, people who use different web browsers have to deal with different types of security warnings. Laymen will often face a dilemma when they are forced to make a decision that they do not understand. They use Internet security packages to protect their computer from malicious attacks, but managing the application by themselves is not an easy task. Whilst they may be aware that security updates/patches are available for them to download manually or automatically, they may refuse this, as they do not know how to do this or they do not realise the importance of doing it. By explaining such incidents, this study seeks to clarify potential problems that users face, based on the scenario study presented in the survey, in terms of how they perceive the security features, the decision making process, and the usability of such technologies. It is seen as essential from the author point of views to understand end-users' preliminary insights, so as to identify potential issues that can be raised for further investigation.

3.2 Methodology

This study emphasizes issues regarding perception and usability in information security. For the purposes of current research, an online survey using a questionnaire has been used to analyse and to understand usability and people's perceptions with regard to information security issues. This method was easy to implement and it was easy to gauge people's attention on such issues. Indeed, the Internet was regarded as a suitable platform, as the survey could be conducted online. The target population of this method was based on people who used the computer and Internet anonymously, given the facts that people use the Internet everywhere, and at any time. Once the survey was promoted to the intended recipients in general, individuals were able to respond to the survey by accessing the website. From another perspective, the survey method research aimed to gauge the subjective feelings of people with respect to specific studies (Fowler 1993). In addition, the survey was seen as useful where information could not be observed directly (Balnaves & Caputi 2001). Thomas (2003) claimed that the survey

was a method to gather information from the target variables within a particular collectivity and then reporting a findings summary. According to Oppenheim (1996), a questionnaire may be considered to be an important instrument of a research where it became a tool for data collection. Many previous studies have used the questionnaire as a method to gather information, using self-administered, postal questionnaires and even an online version. Having said this, it may be noted that a questionnaire using the Internet was not expensive, leading to quicker feedback and less missing data (Nowack 1997, Stanton 1998 and Weible & Wallace 1998). This method may be seen to measure data quantitatively, and respondents were directed to answer section by section. With respect to the previous study conducted, it is fair to consider the survey as a practical method for this study purpose.

The survey in this chapter was designed for adult participation, targeting participants 18 years old and above only. The survey was approved by the Ethics Committee of Plymouth University to ensure the confidentiality and respondents were treated anonymously during collection, storage and publication of material. The ethical principle governing data collection was that no harm should come to the respondents as the outcomes of their participation in the study. The subjects were recruited via an e-mail, predominantly targeting students in Plymouth University as well as friends and relative. The Centre for Security, Communications and Network Research (CSCAN) and International Student Advisory Service (ISAS) website had advertised the survey. In addition, a news entry for the staff and student portal had been used to inform general users to participate in this study. The target population of this study was based on people that used Internet. The survey was conducted using online questionnaire with open and closed-ended questions with multiple choices of answers. However, in order to analyse certain issues in depth, the study will also be conducted using open-ended style of questions to address some issues, especially users' ideas in taking certain actions. (Please note that all details of this particular survey are provided in Appendix A).

3.3 Study design

In order to determine users' perceptions relating to issues of information security usability issues in information security, a survey was conducted to investigate preliminary insights from users regarding their level of understanding of particular issues in relation to the security of their computer systems. The survey was conducted online between February-March 2010, and promoted to the end user community via e-mail, word of mouth and news entry information on the university's intranet website. This survey consisted of 41 questions, offering both open and closed responses. Respondents were not obliged to answer all the questions, as some of them were conditional. The survey was divided into 4 sections:

i. Section 1

Background/demographic - Overview of users' background (i.e. gender, education background, occupation, computing skills and perceptions of computer security).

ii. Section 2

General usage of computer and operating systems - Analysis of users' experiences in using the Internet and operating system, as well as more general computer security concerns

iii. Section 3

Usability and protection - Analysis of users' understanding of issues of usability and protection in relation to malware, security applications, security updates and trust. This section required respondents to identify features from a diagram in order to determine what they understood about those features.

iv. Section 4

Computer scenario study – Analysis of users' understanding of computer security issues was based on their past experience and their knowledge of how to deal with information security by using a security warning dialogue box.

(Note: All figures and tables within this chapter had been analysed using a descriptive statistical analysis)

3.3.1 Study participants

Overall, 784 responses were submitted to the website; however, only 564 were fully completed, representing a 72% completion rate. This provided a good basis for the subsequent analysis, although it should be noted that due to rounding, the values presented in the study and some of the later discussion do not total 100%. All of the figures and percentages reported were based upon the proportions of respondents in this study. Participants in this study were required to fill in the consent form and agree to participate in this study. The responses were treated as confidential at all times, and data was presented in such a way that users' identity could not be connected with specific published data. Participants were free to withdraw from the survey at any time.

3.3.2 Section 1: Background and demographic

This section consisted of 7 questions. The survey resulted in almost an equal split between male and female, with a range of ages as depicted in Figure 3.1. In terms of age, 67% of the respondents were below 30 years old, which indicated they were likely to have grown up in the information, communication and technology era, 26% aged 31-40 and only 7% aged above 50. The education profiles of the group are shown in Figure 3.2. It should be noted that more than 90% of overall respondents demonstrated a high level of achievement in their education. This suggests that a large proportion of studies have been conducted within academia pathways.

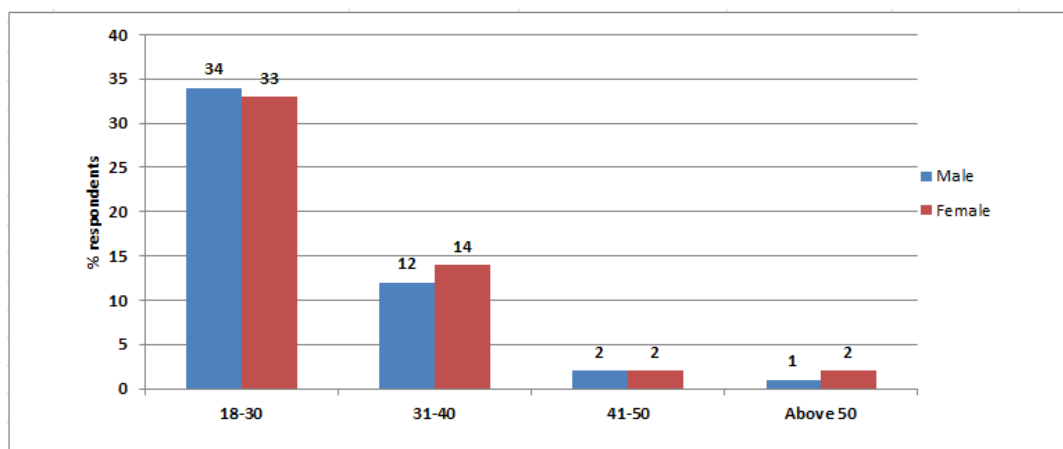


Figure 3.1: Age profile of the respondent group

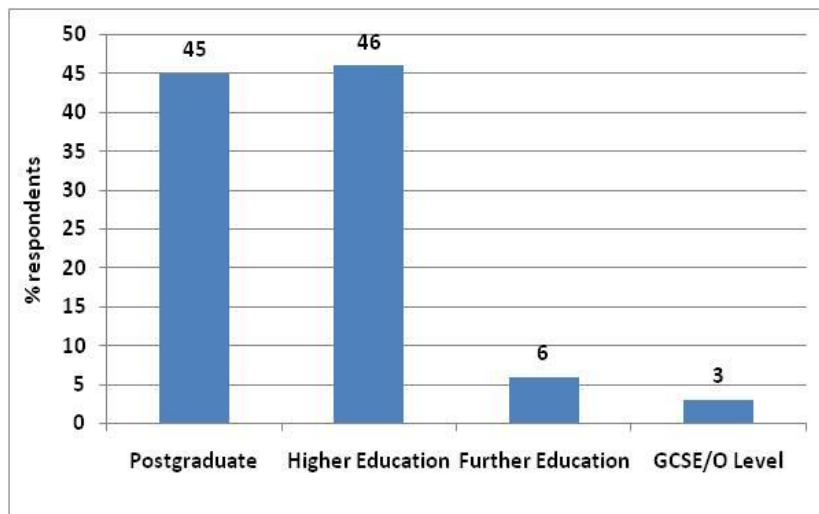


Figure 3.2: Respondents by educational background

With regard to their computing skills, the respondents rated themselves as advanced (47%), intermediate (39%), expert (12%) and the remainder as beginner (2%). Users demonstrated their awareness of the usage of computing in general and this correlated with their educational background. As pictured in Figure 3.3, the vast majority of respondents were very familiar with computing technology, with over 95% of the respondents claiming to have been using their computer for more than five years. This was not a surprising finding, as users are now using the computer and Internet in their daily live for working purposes and online transaction, amongst others.

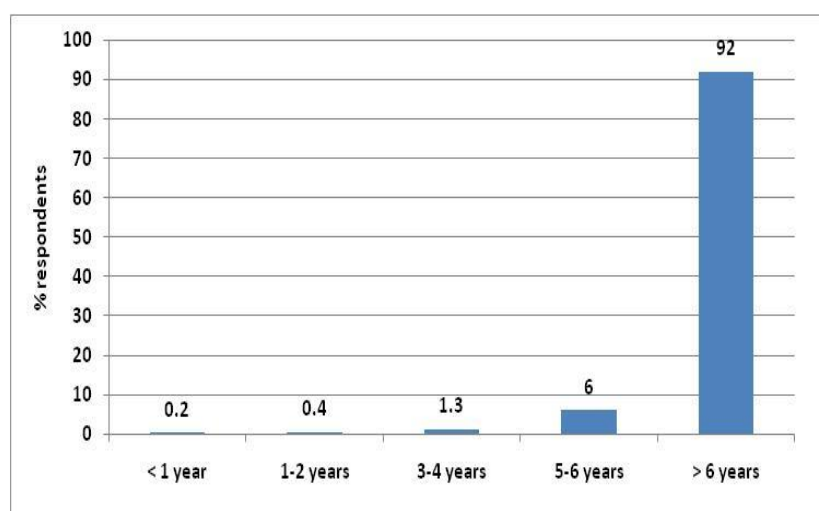


Figure 3.3: Computing experience

Before focusing upon the specific issues in information security, the questionnaire attempted to gauge the respondents' level of concern with respect to computer security.

Based on Figure 3.4, the majority of respondents were seen to be very concerned about the issue of computer security. 23% claimed to be mildly concerned and 1% showing ‘uncertain states’. It would perhaps have been more useful if this study had been able to probe what made them choose this option. On the other hand, 5% of respondents were not concerned with the issues, with the majority of them claiming to be intermediate and advanced level respectively.

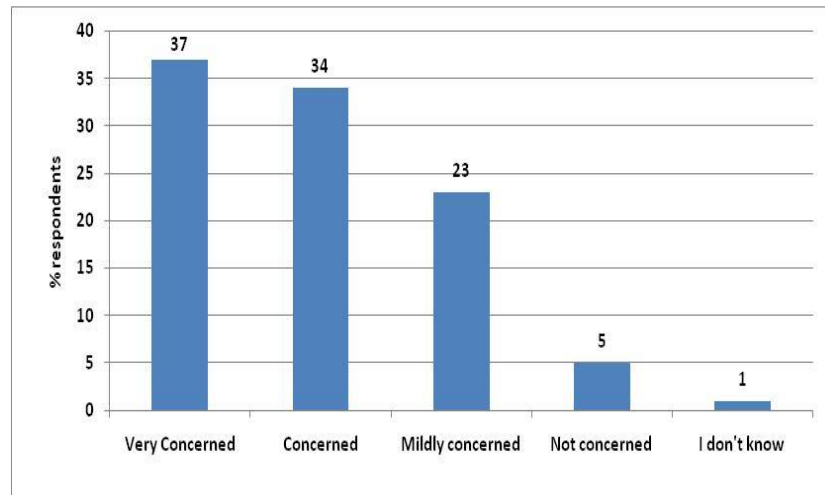


Figure 3.4: Level of concern on computer security

3.3.3 Section 2: General usage of computer and operating systems

The Internet has become a new form of communication, source of information and tool of entertainment. Having understood that, this survey examined end-users patterns in terms of usage of the Internet. This revealed that 84% of respondents demonstrated a high level of experience in using Internet for more than six years, 5-6 years (11%), 1-4 years (5.3%) and less than a year (0.1%). When considering the respondents’ primary operating system, the majority claimed to use Windows XP (44%), Windows Vista (30%), Windows 7 (17%) and others as depicted respectively in Figure 3.5. It may be noted here that Microsoft products were still among the most popular operating system among end- users (representing over 90%). Surprisingly, some users still used a “previous windows version” such as Windows 95, 97, 98 and 2000. To this extent, users demonstrated their ability to identify their operating system, as this was a vital component for any computer. Indeed, it became an interface between computer and supporting hardware and software. Without it, the computer would malfunction and users would be unable to use it accordingly.

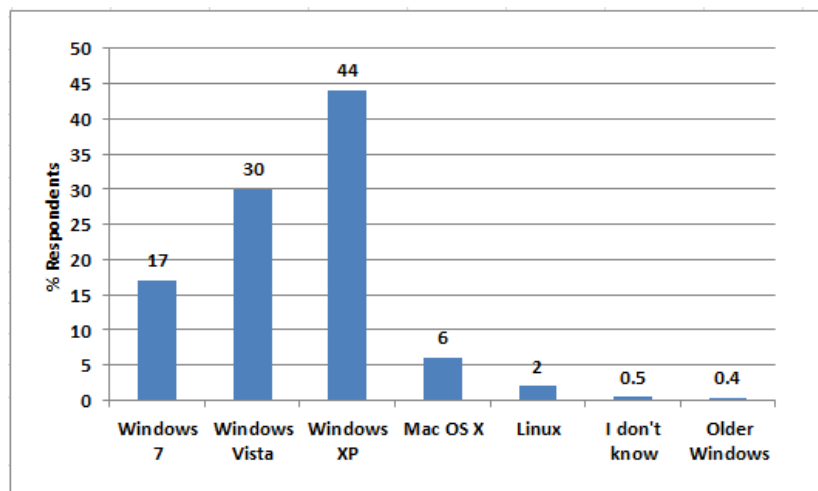


Figure 3.5: Primary operating system.

Users were likely to be exposed to many potential threats if they did not update their security patches. As Figure 3.6 shows, 68% of overall respondents ranked this as “it is important” and “it is very important” whilst 25% considered that “it is mildly important”. It should be noted that whilst the majority of respondents showed their concern about this issue, 7% of respondents’ claimed it was “not important at all” and “I don’t know”. This finding also suggests that most of these respondents were from the intermediate and advanced group. Even though users claimed that they were at a high level of expertise on computing skills, they were likely not to be concerned about taking action to update their operating system. It is essential for users to update their security patches in order to fix bugs or any security issues before problems start to occur.

On the other hand, users demonstrated that they were more aware of any issues relating to computer security in general as portrayed in Figure 3.4, compared to specific issues like operating a system update. This may be viewed in Figure 3.6 where the percentage of “important” and “very important” was slightly lesser. 7% of respondents chose “not important at all” and “I don’t know”. It may be assumed that end-users might assume that operating system did not have direct impact on security issues, as it is something that operates in the background. However in reality, the operating system serves a core function in order for the computer to operate.

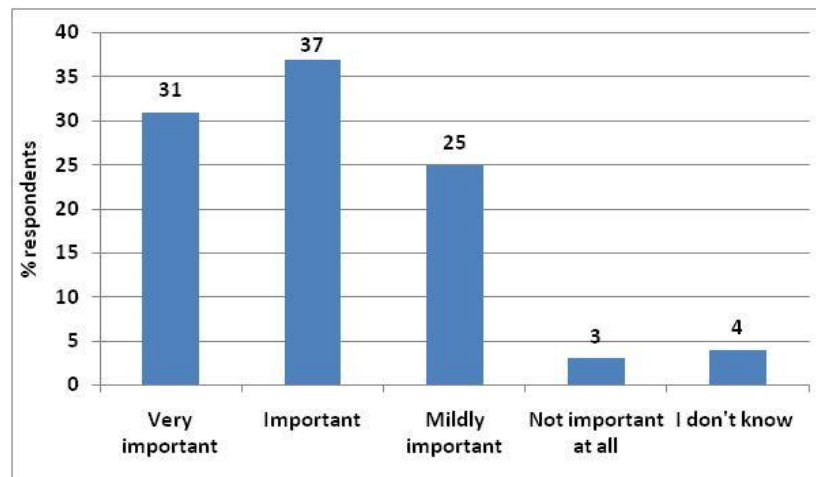


Figure 3.6: Concern on updating operating system

After understanding their concern regarding updating the operating system, the following question determined how users updated them. This updates helped users in dealing with bugs, security vulnerabilities and secure critical infrastructure (Bellissimo et al. 2006). As depicted in Figure 3.7, the results revealed that 89% of respondents' updated automatically and manually, 9% did not update at all and 2% did not know. The minority of 9% who did not update at all were from intermediate and advanced users. Surprisingly, there was a user that claimed to be an expert, but still did not know his/her method of updating the operating system.

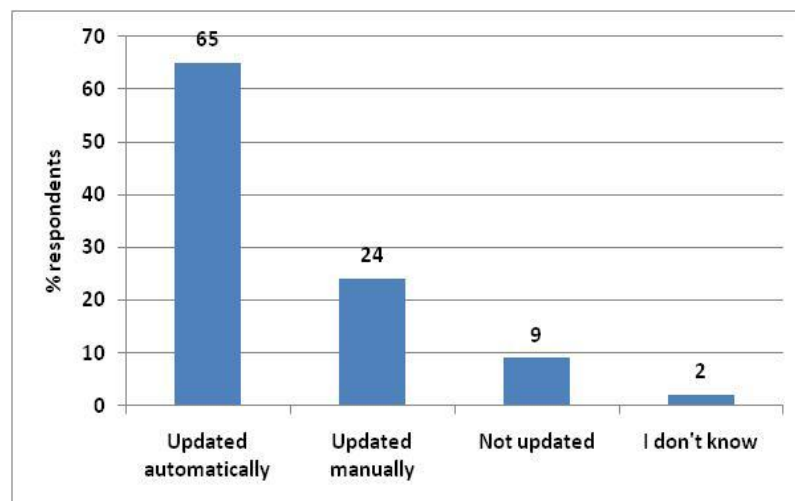


Figure 3.7: Method to update their operating system

Using security software is vital for users, whether at home or within an organisation. According to Richardson (2008), more than 95% of organisations use security technologies (i.e. anti-virus and Internet security package) to scan for malware, filter

incoming e-mail, and protect their website from any possible threats. A similar line of research by PWC (2008) also presented similar results based on organisations in United Kingdom. Therefore, it was important to ask respondents for their acceptance and usage of security software products. The majority 86% of respondents used security software in their computer, while 14% of respondents claimed that they were not using security software, or did not know about it. A vast majority of the 14% of respondents were intermediate, advanced and even expert users. Some users argued that they did not use security software, as they were not using a Microsoft operating system such as Linux and Mac OS X. They claimed that by using this version of the operating system, they would not have to be afraid of becoming victims of malware attacks. Their behaviour might lead them to catastrophic results (i.e. by becoming a victim of malware attack). This was a somewhat interesting finding in terms of how users perceived the acceptance of the importance of security.

The next question asked users about their security vendor. Based on the current trend, it can be noted that Kaspersky, AVG, McAfee, Norton, Avast and Avira were amongst the most commonly used security software. With regard to the survey findings, Kaspersky became the most popular vendor, with 30% of respondents choosing it. One reason that led to these results was that this survey was well promoted within the university environment. More specifically, Kaspersky was used as the main security software for the university, which might reflect positively in the outcome of the survey. One noteworthy findings based on Table 3.1, was that 7 respondents in which represented 1% claimed they were unsure of their security software vendors, with 5 of respondents claiming to be advanced and expert users. Based on this scenario, the majority of respondents were able to identify their security vendor, which indicated their knowledge of knowing one particular security vendor in the market. However, it did not guarantee them to use the security tool effectively. It may be noted that users were allowed to choose more than one security vendors. Therefore, the overall total of participants and percentages did not represent 564 respondents and 100% respectively.

CHAPTER 3: EXAMINATION OF COMPREHENSIBILITY OF ISSUES IN
INFORMATION SECURITY

Vendors	Male	Female	% overall	Vendors	Male	Female	% overall
Avast	38	39	14	Comodo	4	0	0.7
AVG	68	78	26	Panda	1	3	0.7
AVIRA	39	42	39	ZoneAlarm	1	0	0.1
BitDefender	11	3	3	Secunia	1	0	0.1
eScan	2	5	1	Mailbytes	0	1	0.1
ESET NOD32	14	15	4	Autorun Eater	0	1	0.1
F-Secure	4	5	2	Microsoft Security Essential	6	3	2
G DATA	0	0	0	Advanced SytemCare 3	0	1	0.1
Kaspersky	86	85	30	Intego	1	0	0.1
Kingsoft	2	0	0.4	NOD32	1	1	0.2
McAfee	51	58	19	Lavasoft	0	1	0.1
Microsoft Live OneCare	3	6	2	Internet banking security	1	0	0.1
Norman	1	1	0.2	Trusteer	0	1	0.1
Norton	32	38	13	Checkpoint	1	0	0.1
Sophos	7	11	3	Bullguard	0	1	0.1
Symantec	22	32	10	ClamAV	1	0	0.1
Trend Micro	10	8	4	Smadav	1	0	0.1
Trustport	0	0	0	Not sure	4	3	1
Windows Defender	0	1	0.1				

Table 3.1: Preferred security vendor

For the following question, users responded in regards to the type of security products they used (i.e. they were allowed to choose more than one option). Overall, 70% of respondents used antivirus software, 51% used Internet security packages and 38% used anti-spyware software, 9% used zone alarm firewall, 4% used mobile security, with the remainder as depicted in Figure 3.8. As users were able to choose more than one option with this particular question, they might not realise that choosing an Internet security package meant that they were obliged to choose antivirus and antispyware. Most security software vendors embedded many other security tools in a bundle or package so that it would be easier to use, rather than purchasing separately. Further assessment with regards to the usage of Internet security will be discussed in section 3, based on Figure 3.15.

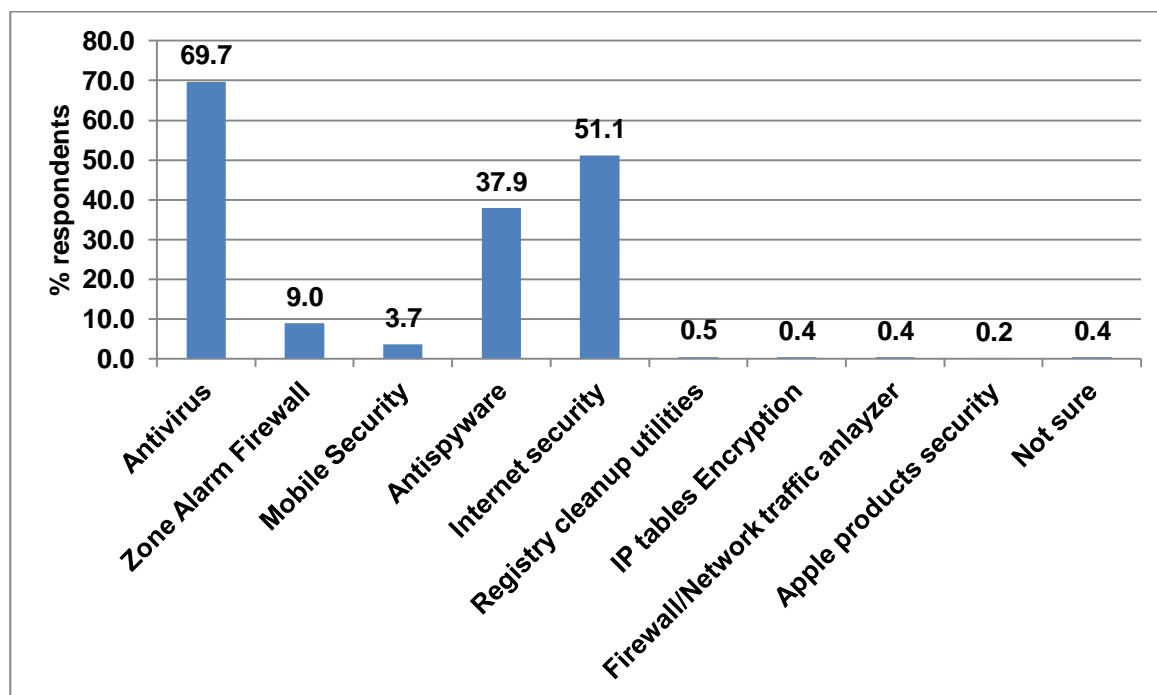


Figure 3.8: Usage on types of security software products

Having established the idea of security protection for users' computers, the survey asked the respondents about their usage of their preferred web browser. Various web browsers are on the market, and each of the browsers has a different method of security implementation. The survey used six main web browsers as sample case studies (i.e. Mozilla Firefox, Internet Explorer 8, Internet Explorer 7, Opera, Safari and Google Chrome). The study revealed that 47% of respondents used Mozilla Firefox as their preferred web browser, compared to 12% of Internet Explorer 7 and 17% of Internet Explorer 8 respectively, as depicted in Figure 3.9. Interestingly, 1% of users suggested Flock as his/her preferred web browser (i.e. a new web browser which specializing for social networking).

From these results, it may be noted that 2% of respondent still did not know their preferred web browser. It may be speculated that these respondents did not prefer to use one specific browser, and might indeed use different browsers at any time. According to W3schools (2010), Mozilla Firefox and Internet Explorer remain among the most popular website chosen by the users. Interestingly, this study presented a similar pattern of results. It may be noted that the survey was well promoted in Plymouth University surrounding, so that the result might reflects the outcome of high percentage of users using Internet Explorer (i.e. 39% of respondents chose Internet Explorer 7 and 8).

In the previous section, the majority of participants also demonstrated that they preferred to use Windows operating system. This might reflect the 37% of Internet Explorer browsers chosen by the participants as well, because this browser was automatically embedded in the computer system.

From different viewpoints, it may be seen that even though this survey was well promoted in the university's environment, surprisingly majority of respondents did not choose it as their preferred one but Mozilla Firefox became more dominant. These results also indicate that end-users (i.e. which is not from university's environment) significantly contributed to the overall results, which covered other distinct overall population.

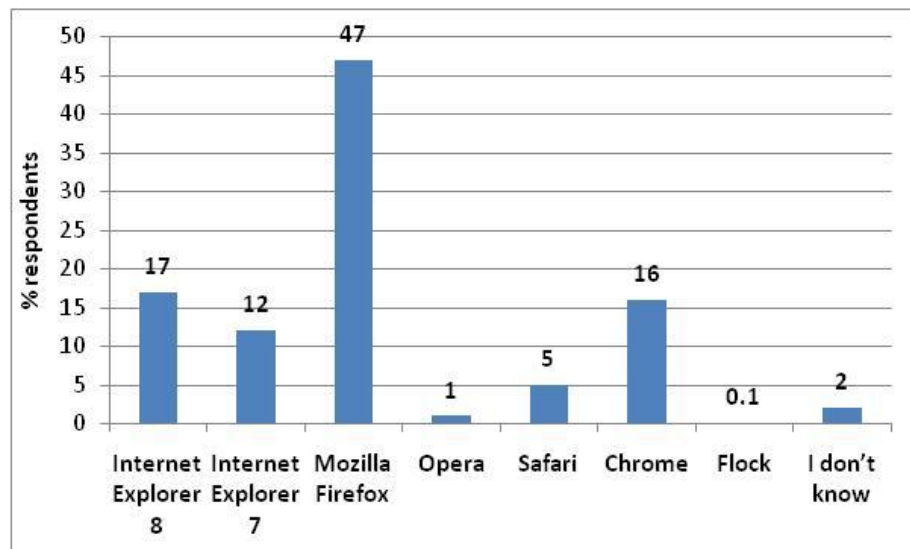


Figure 3.9: Preferred web browser

3.3.4 Section 3: Usability and protection

In this section, focus was accorded to the usability of security warning and issues on computer protection. Having established the idea of preferred web browser, the survey then asked respondents, based on a scenario study with regards to the e-mail, to activate a banking account (i.e. phishing warning). Every respondent received a different security warning based on their chosen web browser in the earlier questions. When they received this message, they had to make a decision by choosing their response to the e-mail message. (as shown in Appendix A). The majority of respondents (67% on average) decided to close the web browser. Generally, it was a good approach to deal

with this scenario. It was expected that users would be aware of what was going on and had their own rationale based on their decision (i.e. security awareness). Trying to find more information about the meaning of the message became the second most popular question answered by most of respondents. It may be noted that users had the capabilities to gather further information about the problems or risks that they encountered before decision was made, and this indicated that they would be able to behave in a secure manner.

A somewhat surprising finding here was that in every type of web browser, a small percentage of respondents claimed that they ignored the warning and proceed with the transaction. In real scenario, this warning was actually derived from a real phishing e-mail. The message might look as though it came from a legitimate source. Users became a victim once they responded to the e-mail link (i.e. provided they give their details to activate their online banking). The e-mail usually would inform the users that they are facing problems with their bank account, and would later direct users to take remedial action by entering personal information on the illegitimate website (Irani et al. 2008). On the other hand, some respondents stated that they did not click the link at all, and called the bank to get clarification, finding ways to report the problem and shut down their system/network. Even though the percentage of end-users' misbehaviour was not really high, it still indicated that they might become the victim of such attacks. These findings were also able to reveal that users demonstrated an ability to use other medium to ascertain the problem that they had encountered, so that possible precautions could be put in place.

After assessing users' responses towards phishing warnings, the next question attempted to assess users' general understanding on the security warning that appeared in previous section (i.e. phishing warning). Picking up from the findings, 75% of respondents understood the information provided in the security warning, whilst leaving a quarter of them with the dilemma of "No" and "I don't know". Having established the general understanding of information, the questionnaire attempted to reveal the reasons for not understanding the information provided on the security warning.

It is essential to gain a clear perspective from the end-users in order to improve the warning presentation in general. This study reveals that 62% of respondents who answered “No” claimed they were facing difficulties understanding the security warning information provided because of technical terminology, the nature of the event being described and the available choices, as illustrated in Figure 3.10. A further line of research highlighted similar finding regarding the obstacles to understanding security technologies that rely on language and terminology being used (Furnell et al. 2006).

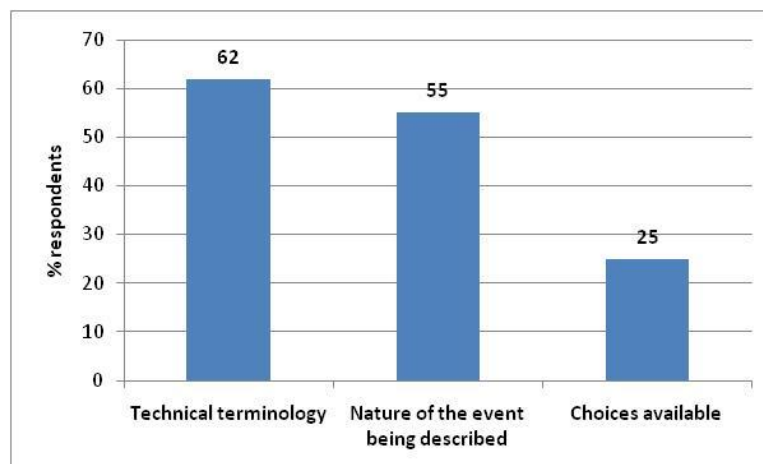


Figure 3.10: Reason on difficulty to understand the security warning

The questionnaire then revealed users’ belief as to the reasons why the security warning would have appeared. This question was based on previous security screenshot on phishing warning. People who answered on their preferred web browser were compulsory to answer this question. The finding revealed that 73% agreed that the website is linked to fraudulent activity, 30% said that the website contained viruses, 23% said the website contained inappropriate materials and the remainder as pictured accordingly in Figure 3.11. Even though only 4 % of total respondents said they did not know about the reason why the message appeared, this small percentage indicated end-users can simply be the potential victims of the threats. Furthermore, this fraudulent activity became more popular, as the e-mail message presented tended to look legitimate and end-users were baffled as to how to make a decision on such incidents.

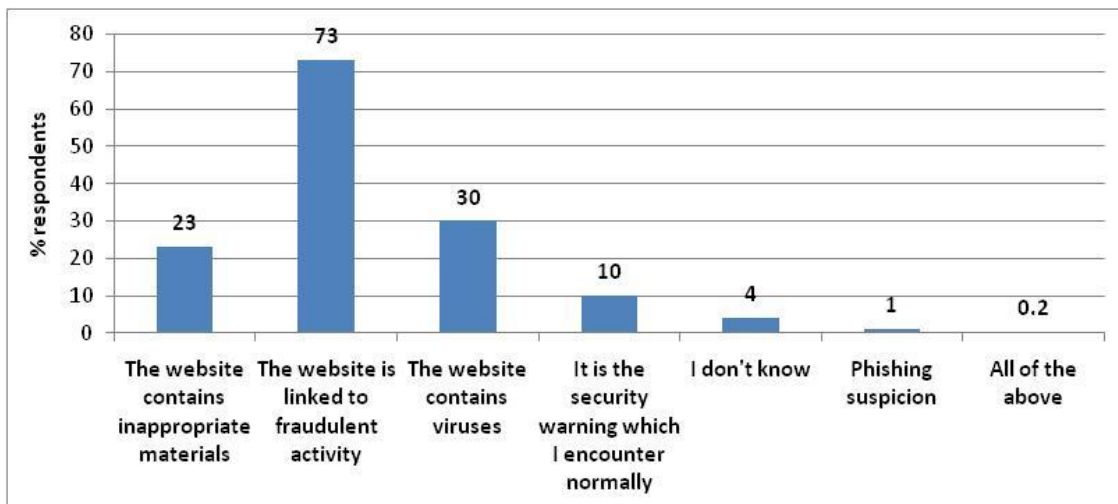


Figure 3.11: Belief regarding the security warning that appeared

The next question sought to gather evidence as to users' experiences of malware attacks. According to Noreen et al. (2009), computer malware became a major threat to computer network and systems since 1990s and malware sophistication had significantly improved to trick the end-users. Seven types of malware/threats were presented, as depicted in Figure 3.12. The majority of the respondents have had experience with spam (93%). Surprisingly, 4% of those who had used computers did not know about spam. A vast number of percentage (more than 70%) of respondents had also had experienced with viruses, worms, trojans and spyware. However, it was completely different for phishing, as indicated only 48% of respondents had experienced with it. In spite of the fact that phishing was a simple social engineering attack, it proved to be surprisingly effective, as a number of phishing scams continually grow and the costs of resulting damage was increasing (Raffetseder et al. 2007). A somewhat surprising findings on experienced with unauthorized access attempt as it was equal to 37% respectively for people who have experienced with and not experienced. Almost one third of respondents also claimed that they never heard of it. It may be seen that some of the malware terminology sounded technical and odd, which might contribute to uncertainty where a particular threat was encountered.

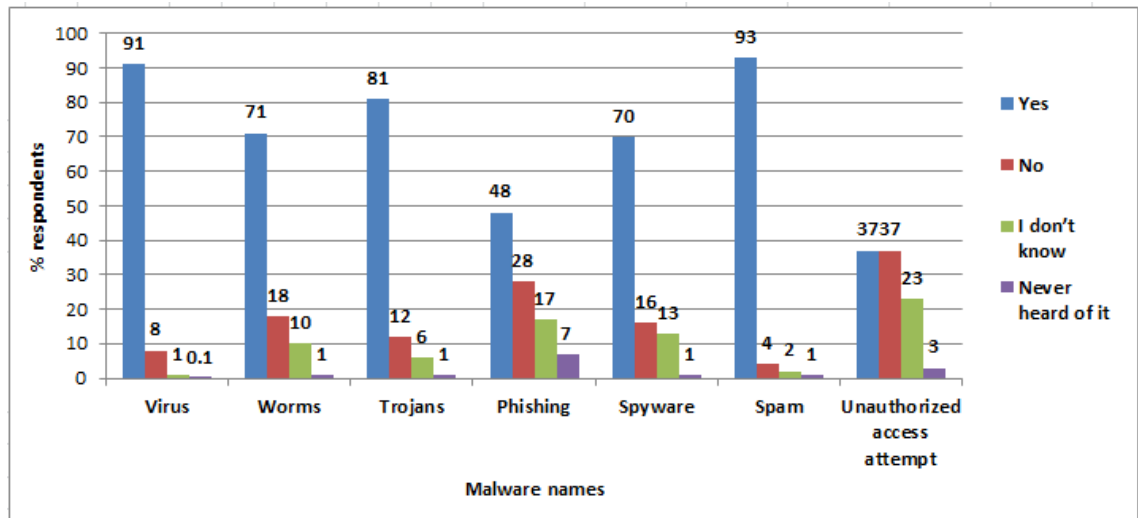


Figure 3.12: Experienced with malware/threats

The end user is the locus of threats. They are the people who are always baffled, face a dilemma and end up by becoming victims. After understanding respondents' experience on malware, the questionnaire attempted to reveal how users' response by possibility of becoming a victim of malicious attack or cybercrime. Overall, 50% of respondents agreed that they were only visited the website that they familiar with, 49% used Internet security package, 21% not changed their attitude, 3% went online less often and the remainder as depicted in Figure 3.13. It can be noted that even only 3% said that they went online less often, it did not solved the problem from possibility becoming a victim in cybercrime or malicious attack. Without knowledge and awareness to deal with the threats, they are likely to be the victims again in future. This survey had similar findings based on a study conducted by Symantec (2009).

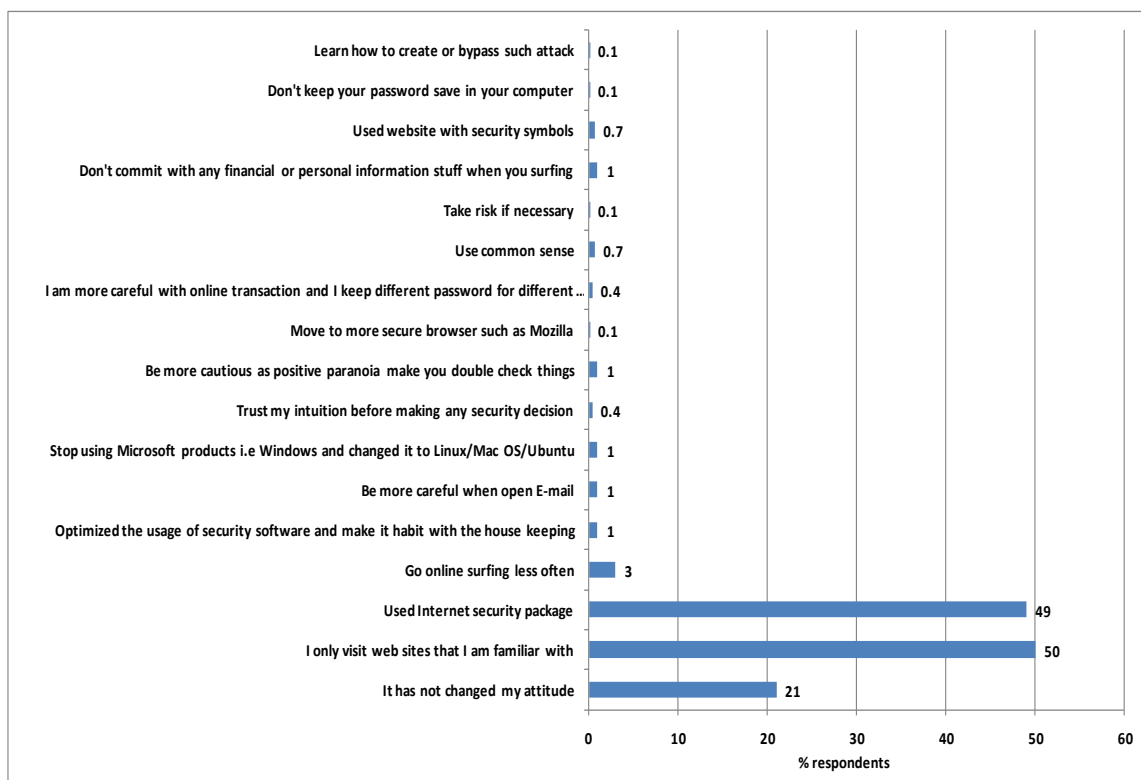


Figure 3.13: Behaviour towards the usage of computer security through the possibility of becoming a victim of malicious attack or cybercrime

In the aforementioned question, the survey asked respondents about their usage of security software. It was significant to ask them type of security software which they used to examine their understanding level of its usage. In aforementioned question section 1 on usage of security software, 86% of respondents were using security software. Having said this, most of respondents agreed they have installed with antivirus application compared to other security software as pictured in Figure 3.14. Interestingly, whether users realized it or not, most of mentioned security software had been embedded in the Internet security package and even some in Antivirus software. The mean value (average) of users who installed all of these security applications was 59%. This revealed that even though 86% of total respondents knew they had installed security software in their computer, only 59% of them really realised types of security application they have in their usage software. From the figure as well, it can be noted that 73% of respondents did not know about parental control features. From author observations, mostly parental controls had been embedded in the Internet security package instead of general Antivirus product. Among all of these security applications, intrusion detection system and anti-phishing were the most popular choice for the

respondents attributing “I don’t know” and “never heard of it”. The terminology for the intrusion detection system was somewhat difficult for non-technical savvy users so it was not a great surprise as the results showed that majority of respondents did not know about it. In general and on balances, intrusion detection system involved in all security applications processes. However, due to its major roles in a critical component in network architecture, it even became a foreign concept to many security practitioners and systems administrators (Koziol, 2003). Based on these findings, end-users generally demonstrated that they were able to behave accordingly, but some users were still unable to act in secure manner (i.e. learn to bypass attack, take risk if necessary, go online surfing less often and not committing to any financial or personal information related). To get a better understanding on usage of security software and its application, the study determine to ascertain whether users understand on the usage of their security software. Hence, this study made use of the tabulation between usage of security software and security applications as depicted in Figure 3.15.

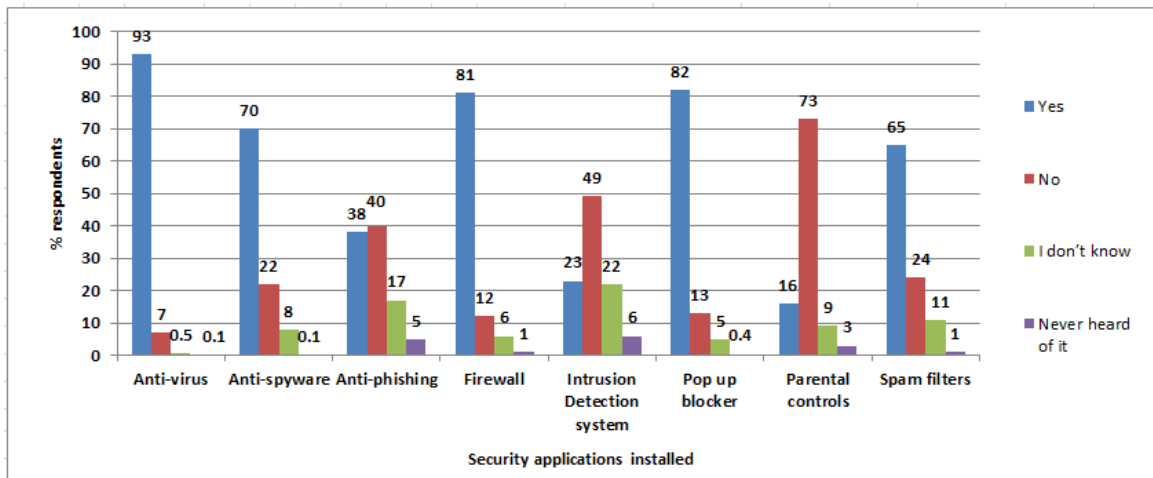


Figure 3.14: Usage of security applications in their computers

Prior to the findings on Figure 3.8, 60% of respondents used the Internet security package as their preferred security product. The three most popular security applications have been compared to the usage of Internet security package. If users had used the Internet security package, all of these three security applications were already embedded in the software. As expected, highly percentage with 99% of respondents claimed using Internet security package and had installed anti-virus albeit only 1% said no. For anti-spyware application, 86% had Internet security package and anti-spyware application installed in their computer, whilst 14% claimed otherwise and did not know

about it. On the other hand, the results on anti-phishing were not convincing, whilst only 54% who claimed to use Internet security package had installed anti-phishing leaving 46% with other available options.

Based on these findings, it indicated that some of users still did not understand their usage of security software and its functionality. They claimed they used the security software but were failed to demonstrate the usage and presence of specific tools. Then again, users might not aware the existence of this specific tool as the terminology being used was cumbersome for them. When it involved a rigorous process, users chose to opt out of learning or aware about it. As a result, even users claimed they had used security software, but in reality they were still in a dubious position about what specific tools they had as security software.

In percentage (%)	Had installed Anti-Virus				Had installed Anti-spyware				Had installed Anti-phishing			
	Yes	No	I don't know	Never heard of it	Yes	No	I don't know	Never heard of it	Yes	No	I don't know	Never heard of it
Using Internet security package	99	1	0	0	86	9	5	0	54	26	17	3

Figure 3.15: Users' claimed using Internet security package vs. claimed installed security applications

Having established the usage of security applications, the next question attempted to assess method of updating users' anti-malware tools. Most of the security applications were updated automatically as depicted in Figure 3.16. However, respondents demonstrated that they still wanted to update their anti-malware tools manually as depicted accordingly. It can be noted that most of these anti-malware tools were embedded in the Internet security package where once users updated their software; it updated every other component as well. On average, 15% of respondents chose not to update their anti-malware tools. This action was not advisable, because anti-malware tools needed to be updated regularly with the most recent security patches. Failing to comply with this might open possible menaces to users.

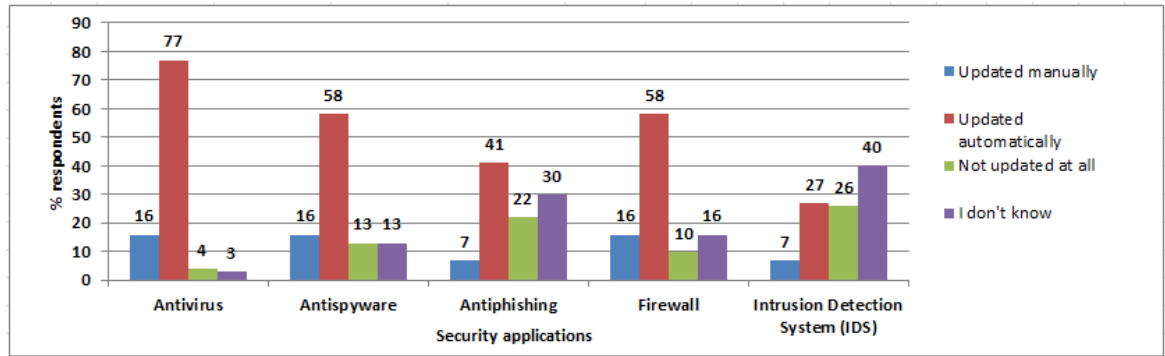


Figure 3.16: Method of updating their anti-malware tools

Finally, the survey assessed users’ awareness in regards to the importance of updating their anti-malware protection tools as illustrated in Figure 3.17. It may be noted here that 80% chose “it is very important” and “important”, 12% claimed “mildly important” and “not important” and “I don’t know” with 3% and 5% respectively. In the aforementioned question regarding concern on updating operating system, 68% users demonstrated that “it is very important” and “important” whilst with anti-malware tool the percentage proportion was slightly higher with 80%. In contrast, a surprisingly high proportion of respondents expressed different levels of importance in regards to two main security applications, namely the operating system and anti-malware tools. This indicated that many people still did not understand the importance on updating security patches on their security applications, regardless of the operating system or anti-malware tools. Securing a computer with updated patches did not guarantee users the best security. However, it promoted good security practice, which might help end-users reduce the risk of becoming victims of computer threats.

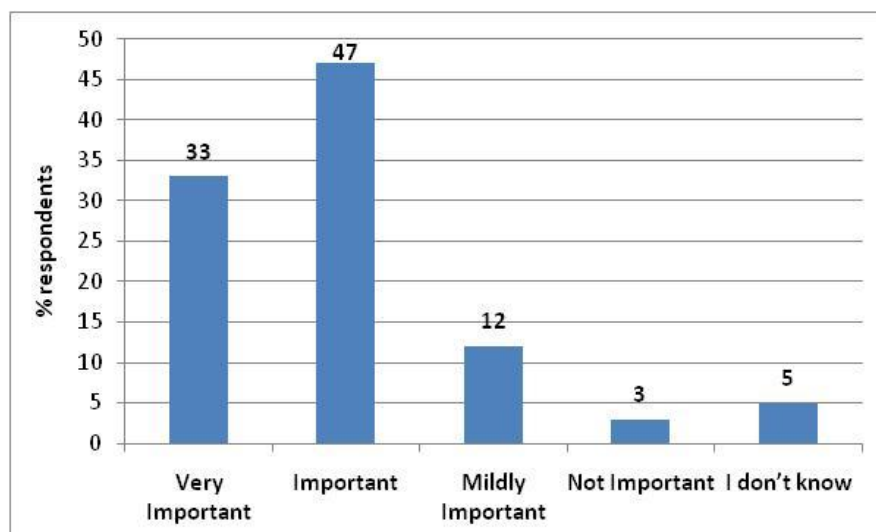
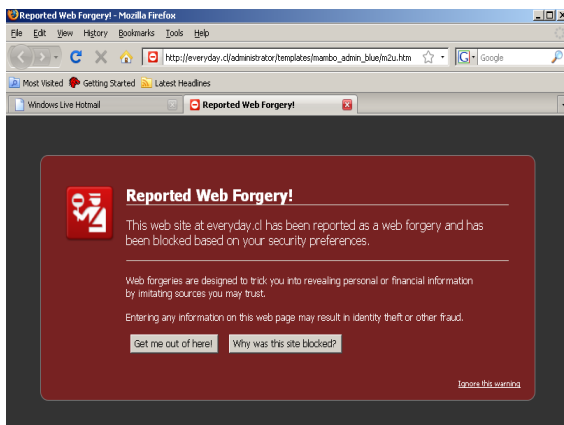


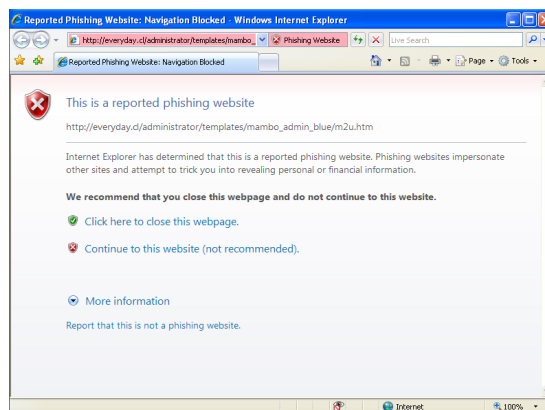
Figure 3.17: Level of concern on updating their anti-malware protection tools.

3.3.4.1 Further evaluation – Independent reviews

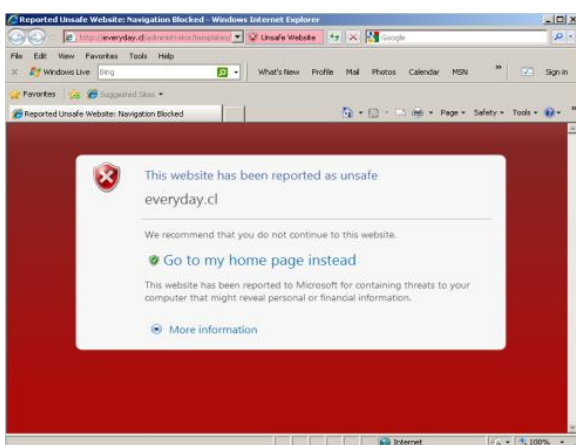
The author conducted independent reviews, comparing the layout presentation based on 6 web browsers contexts presented (i.e. Google Chrome, Mozilla Firefox, Safari, Internet Explorer 7, Opera and Internet Explorer 8), as shown in Figure 3.18. Generally, this survey presented two types of security warning study (i.e. phishing warning that was explained in section 3 and dialogue box warning that was explained in section 4). The basis of this review was to assess how security features been presented and used, elements that might attract or mislead users and any missing elements. This was to contemplate if current security warnings are able to perform its function, as discussed in Chapter 2.



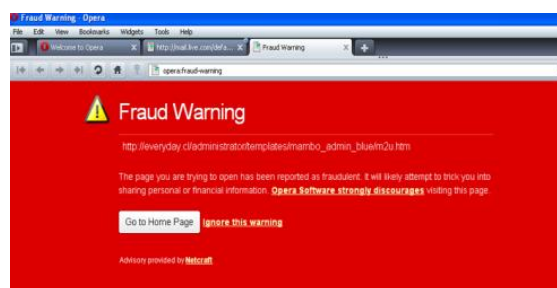
Mozilla Firefox



Internet Explorer 7



Internet Explorer 8



Opera

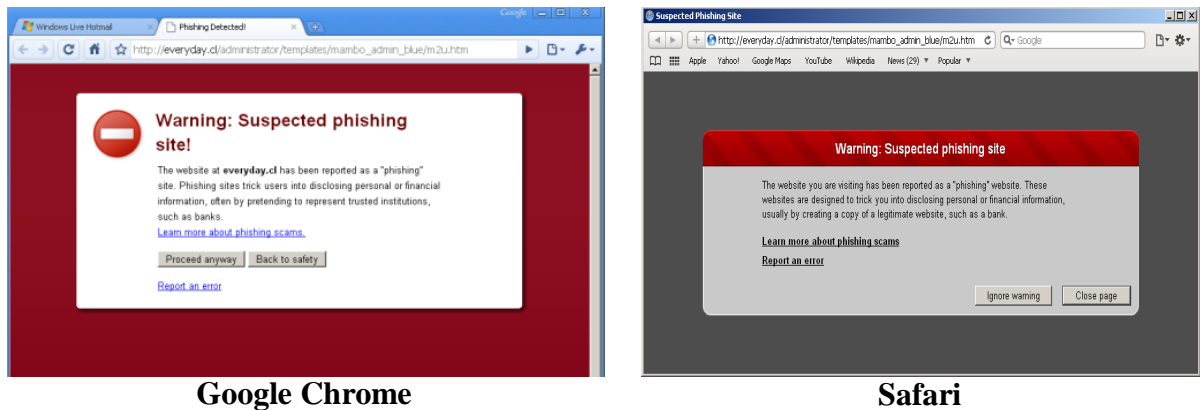


Figure 3.18: Screenshot from various web browsers showing a security warning having detected a possible phishing website.

It may be noted from Figure 3.18 that the ways in which warning information was delivered differed in terms of wordings, colour scheme, available options, technical jargon and the design of the warning. For example, Microsoft improved the phishing warning to ensure that end-users were able to comprehend the message accordingly (i.e. Internet Explorer 7 to Internet Explorer 8). Instead of using “This is a reported phishing website” terminology, Microsoft changed it to “This website has been reported as unsafe”. This piece of information was presented using simple, plain language without using any technical jargon. The background colour of the warning was also changed to red and the option “Continue to this website (not recommended)” was hidden from users. The colour was also able to convey the severity of the risk, whilst recommended action was highlighted as the main option. The author did not further assess the effectiveness or efficiency of the changes, but highlighted the different methods of presenting phishing warning from different web browsers, as depicted in Table 3.2. Based on the author’s knowledge and observations, no other such comparison table has been produced.

CHAPTER 3: EXAMINATION OF COMPREHENSIBILITY OF ISSUES IN
INFORMATION SECURITY

Browsers	Usage of Help Function	Usage of Colours	Usage of Icon	Available choices	Terminology used
Mozilla Firefox	<ul style="list-style-type: none"> • Providing information on why the website is blocked 	<ul style="list-style-type: none"> • Using a red background colour scheme to get attention 	<ul style="list-style-type: none"> • Using 2 types of warning icon 	<ul style="list-style-type: none"> • Ignore this warning • Get me out of here • Why was this site blocked 	<ul style="list-style-type: none"> • Reported as web forgery
Internet Explorer 7	<ul style="list-style-type: none"> • Providing more information about the incident 	<ul style="list-style-type: none"> • Address bar changing to red colour with Phishing website connotation 	<ul style="list-style-type: none"> • Error warning icon 	<ul style="list-style-type: none"> • Continue to website(not recommended) • Close the webpage • More information about phishing • Report that it is not phishing website 	<ul style="list-style-type: none"> • Reported as phishing website
Internet Explorer 8	<ul style="list-style-type: none"> • Providing more information about the incident 	<ul style="list-style-type: none"> • Address bar changing to red colour with Unsafe website connotation 	<ul style="list-style-type: none"> • Error warning icon 	<ul style="list-style-type: none"> • Go to my homepage instead • More information about phishing • Report this site does not contains threats • Disregard and continue (not recommended) 	<ul style="list-style-type: none"> • Reported as unsafe website
Google Chrome	<ul style="list-style-type: none"> • Providing more information about phishing scams 	<ul style="list-style-type: none"> • Using a red background colour scheme to get attention 	<ul style="list-style-type: none"> • No entry warning icon 	<ul style="list-style-type: none"> • Proceed anyway • Back to safety • Report an error • Learn more about phishing scams 	<ul style="list-style-type: none"> • Suspected as phishing site
Safari	<ul style="list-style-type: none"> • Providing more information about phishing scams 	<ul style="list-style-type: none"> • Using a red highlighted header colour 	<ul style="list-style-type: none"> • No icon 	<ul style="list-style-type: none"> • Learn more about phishing scams • Report an error • Ignore warning • Close page 	<ul style="list-style-type: none"> • Suspected as phishing site
Opera	<ul style="list-style-type: none"> • No details 	<ul style="list-style-type: none"> • Using a fully red background colour scheme 	<ul style="list-style-type: none"> • Warning icon 	<ul style="list-style-type: none"> • Go to homepage • Ignore this warning 	<ul style="list-style-type: none"> • Fraud warning

Table 3.2: Comparison of the security warnings from various web browsers (Zaaba et al. 2011)

This table comprised five features as the basis of comparison. These features were chosen based on the features commonly presented in security warnings, as referred to in Microsoft (2010) guidelines. It may also be noted that most of these warnings used technical terminology to explain the problem that users faced (i.e. phishing, fraud and web forgery). In addition, three common security warning icons were used (i.e. no entry, error and warning) and a red background colour predominantly conveyed the risks. Surprisingly 6.5% on average of respondents still decided to close the browser and proceed with the warning (i.e. possibility became the phishing attacks).

3.3.5 Section 4: computer scenario study

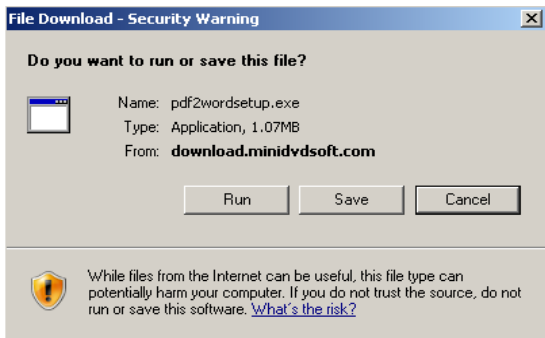
One scenario study related to the security dialogue box (i.e. common security dialogue that users' received.) In the aforementioned question on section 2, the survey asked respondents as to their preferred web browser. On that basis, the following question was asked in order to understand users' decisions as to the security warning dialogue issues (i.e. when downloading application from the website). According to Farago (2010), the BBC (2010), Schonfeld (2010) and the Daily Mail (2012) downloading applications, music or software is widely used by end-users whether using mobile phone or computer. Thus, it was relevant to use the security warning dialogue as a scenario for examining users' understanding of the current interface by assuming they would download any software from the websites. In this second scenario, as depicted in Figure 3.19, users were presented with a security warning dialogue, with this question:

“You would like to download a new free application from your web browser. When you click the link to download the file, the following pop up appears. What would you do next?”

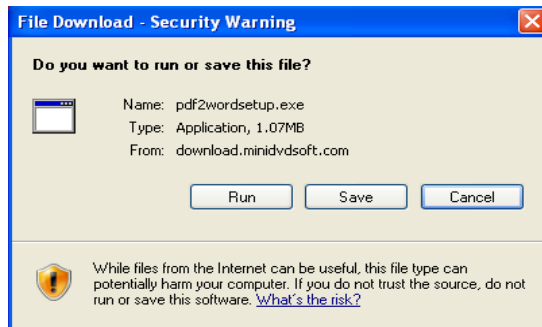
The majority of respondents commented that they saved and scanned the file for viruses as depicted in Appendix A. A somewhat surprisingly finding by Internet Explorer 7 respondents where the majority of 29% of respondents chose to cancel and quit from the process. Although this action hindered users from downloading the file, possibly with malicious contents, users might learn to get rid of this kind of security warning in the future (i.e. habituation effects).

On the other hand, a small group of respondents decided to run the application directly; 10% from Internet Explorer 8, 9% from Internet Explorer 7, 3% from Mozilla Firefox, 17% from Opera, 11% from Safari and 7% from Chrome. This revealed that users were not afraid to take the risk of downloading the application, even though they did not know about the authenticity of the provider or software. On the other hand, 19% on average of all respondents decided to cancel or quit the process upon receiving a security warning. It may be noted that this action might prevent them from the risks at that particular time, but in long term (i.e. if they encounter similar situation again), and they might fail to become a potential victim of malware. A small percentage of

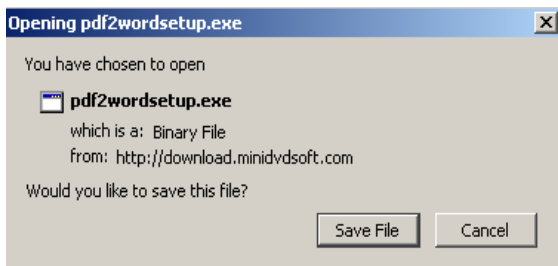
respondents suggested that their decision was based on their intuition, reviews about the application and only downloaded from a reputable source.



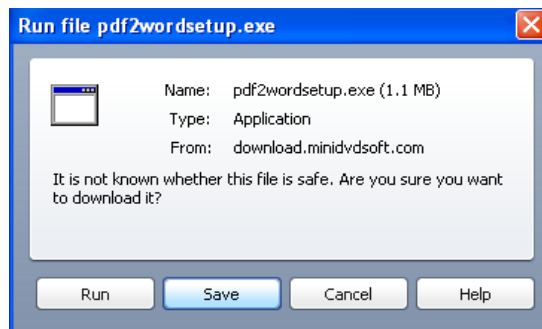
Internet Explorer 8 Security pop up



Internet Explorer 7 Security pop up



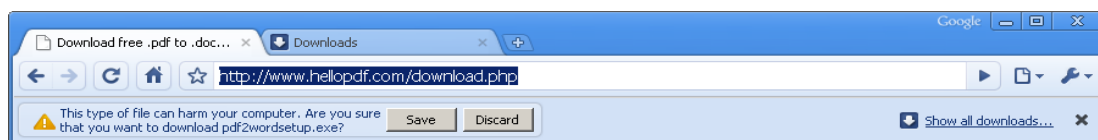
Mozilla Firefox Security pop up



Opera Security pop up



Mozilla Firefox Security pop up



Chrome Security pop up

Figure 3.19: Security pop up according to various of web browsers

Having assessed the respondents' decisions with regard to the security warning dialogue, as depicted in Figure 3.19, it was also relevant to consider whether respondents felt the information on the depicted warning was sufficient. Respondents only answered this question if they had answered the aforementioned question on preferred web browser. Overall, 43% felt satisfied with such information on the depicted warning, while more than 54% said the information was not enough (i.e. we may take into account that each web browsers had presented with different security features for end-users to use and to understand). A further 3% of respondents corresponded without any answer, representing seventeen respondents altogether (i.e. one beginner computing skill user, eight intermediate computing skill users, seven advanced computing skill users and one expert computing skill user). Having understood this, it may be seen that there is a need to further investigate the level of information provided in security warning dialogues (e.g. security features such as icons, words and colours) which can be gathered based on end-users' experiences. It is useful to assess and evaluate how end-users understand the implementation of such features, and later, to be able to make them act in a secure manner.

Prior to the previous question, where 54% respondents claimed that not enough information was provided, this survey asked respondents about their point of view of other information which they think should be there on the depicted warning. As depicted in Figure 3.20, 38% of respondents said that they wanted the details of the consequences if they were to proceed in running the application, a quarter of total respondents said they wished to have confirmation of legitimate download, 27% commented that they wanted the application they downloaded to be free from any malware attack, 17% claimed to have a proper help function, while others remain below 1% respectively. Some respondents demonstrated useful ideas that suggested computers should have strict defending process, understandable features, an automatic virus scan and details of the application provider. Users also suggested that the developer should cater for all issues of security before any system or application can be used by the end-users. From these findings, the proposed solution was generally implemented by various usable help techniques (i.e. explained in Chapter 2). However, none of these techniques were able to come up with one solution that comprised all

elements or features that users’ wanted. A considerable number of research studies are needed in this area so that a better solution can be imposed.

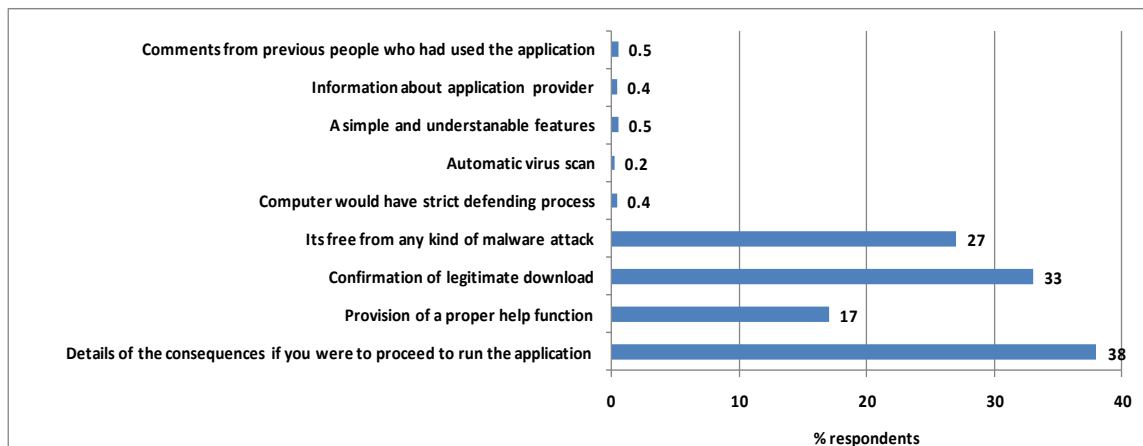


Figure 3.20: Point of view on other information that should be in the security warning.

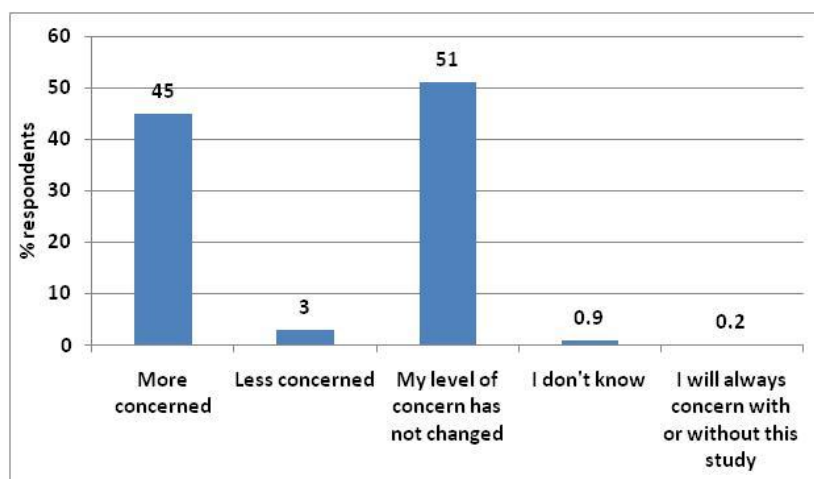


Figure 3.21: Level of concern after completing the questionnaire

The final set of questions in this section asked users whether completing this study would change their level of concern about computer security. In the early section, this survey asked users about their concern regarding computers (i.e. pre-question), with 37% of respondents being ‘very concerned’ about the security of their computer, as pictured in Figure 3.4. In contrast, it was notable that 45% of total respondents were ‘more concerned’ after completing the survey as portrayed in Figure 3.21. Users demonstrated a small increased level of concern, albeit 51% said their level of concern had not changed. A somewhat surprising finding was that 3% of total respondents said they were less concerned. Even though this represented a small percentage, it showed that

these groups of users had the potential to become a victim of malicious attacks. They did not see the unpredictability of the danger while dealing with computer. At least some knowledge, awareness and experience can ensure the best thing to do or act accordingly. One user also stated that he/she would always be concerned, with or without this study.

3.4 Feedback comments

In addition to answering the pre-set questions, respondents were also given the opportunity to leave free-text comments if they had any further thoughts or clarifications to share. It may be noted that this question was not compulsory. Although not fully representative, below are some selected responses:

- i. “Antivirus should be embedded together with the operating systems to provide security so that users do not need to install too many things in their computer” (User 102).
- ii. “Information presented to inform users about the current problems should use simple explanation and less technical terminology” (User 14).
- iii. “The problem of malware is on the people and not the technology. People are responsible with anything because they are the one who make a decision” (User 204).
- iv. “User interface should be more user-friendly so that it helps user to comprehend the possible actions to take” (User 291).
- v. “Although I use the computer on a daily basis, this is only when at work, I do not use a computer at home. Therefore, the IT department do any necessary upgrades and deal with any problems for me so I don't really worry about any of the problems that could occur” (User 355).

- vi. “Most of my answers stated "I don't know" because am not very familiar with all the computer terms as am not a computer expert and not a heavy user unless for work related purposes” (User 38).
- vii. “Security information in the past has not been very well explained to the average user, leaving them confused or unsure, and vulnerable to attack” (User 144).
- viii. “What could I conclude here is we can't control things on the internet, trust your feeling, directly ignore suspicious files or any and get yourself educate on the internet security on how to protect, defend and take action from the infection” (User 181).
- ix. “Again it is up to the operation system the user used. I am better off on Apple OSX. Others like Windows, users need all the security package available and need to understand them carefully. Finally better OS makes life easier” (User 486).

Based on these presented comments, users still experience significant problems whilst using their computer at home or organisations. From the contexts of phishing warnings and security warnings on web browsers, users' comprehension upon receiving such warnings was revealed. Even though, these comments did not represent all of the respondents, it gave some indication as to the clarity of the issues presented.

3.5 Discussion

This study has provided a general overview of how end-users understand issues relating to information security, especially with regard to perception and usability. Overall, it may be noted that end-users were concerned about issues of information security in general. The majority of respondents were derived from a higher institution background, which reflected familiarity in using computers for more than six years. From these findings, end-users demonstrated different kinds of experience and understanding when using their computer. This may be summarised as follows:

- i. Generally end-users demonstrated a good level of understanding in terms of the issues presented. The majority of respondents decided correctly upon receiving phishing warning, although some of them still decided to proceed albeit there was a potential for risk. In another scenario, upon receiving security dialogue to download application, the majority of end-users chose appropriate precautions instead of downloaded the software straight away. 10% of overall respondents still decided to download it straight away.
- ii. The majority of users had a good education background and the vast majority had used the Internet for more than six years.
- iii. From independent reviews and observation, it may be noted that the security warning presentations were presented differently based on the vendor's and browsers' version. Clearly, the usage of terminology was too technical, especially for general users. The level of information provided was sufficient, but might be improved (e.g. to explain the risk levels more clearly, give proper help functions).
- iv. Users still faced difficulties with regard to understand information available in phishing warning (i.e. 25% of overall respondents). They agreed with the three main reasons, namely technical terminology, the nature of the event being described and the available choices.
- v. Users demonstrated that insufficient information was presented on the security warning dialogue (i.e. 54% of overall respondents). They suggested some options to improve the current warning dialogue presentation which were able to help them to better understand the warning they received (i.e. confirmation it is free from malware, confirmation on legitimate download, provision of help function, details of consequences if they were to proceed).
- vi. A high percentage of respondents claimed to use security software (i.e. anti-virus, Internet security, zone alarm firewall, anti-spyware, mobile security and others). Surprisingly end-users were unable to demonstrate full understanding

of the usage of Internet security software. In using cross tabulation table presented in section 3, those who claimed to use Internet security in the first place and who claimed to have installed anti-spyware and/or anti-phishing surprisingly chose “no” and “I don’t know”. This indicated that they did not really understand the usage of security technologies they had (i.e. they might use it but not really sure how this particular software functions and able to help them).

3.6 Constraints

This study was conducted online, and hosted on the Plymouth University server. It may be noted that any individual was able to respond to this survey provided they knew the link. There was no specific target in terms of users’ technology capabilities or background. As the survey was well promoted within the university environment, this might be reflected in the results of the study in terms of percentage of users’ using Kaspersky, Internet Explorer web browser and educational background (i.e. as reported in this survey accordingly). Most of the questions presented in this survey were closed ended type of question. This limited the survey to probing more details from end-users. Therefore, some clarifications of findings were based on the author’s assumption (i.e. based on knowledge and experience).

3.7 Conclusions

From the overall results of the 564 respondents, it may be concluded that there is a need to take action to improve the perception and usability specifically with regard to the design of the current security warning interface based on the early stage examination. This also shows that there is a need to better understand the ways in which end-user utilise the security features provided (i.e. icons, wordings, technical terminology, help functions and others). This study provides some evidence to confirm some of the findings in the literature reviews in Chapter 2. The study now proceeds with the next investigation and assessment in Chapter 4, which focuses upon users’ wider encounters with security warnings and the level to which these are felt to be understood and usable.

CHAPTER 4

A Wider Evaluation of Perceived Security Warnings

4 A Wider Evaluation of Perceived Security Warnings

4.1 Introduction

The prior survey study in Chapter 3 was conducted to assess end-users' insights regarding information security issues with regard to the perception and usability and specifically of the security message/warning interface scenario study. This provided a basis to further probe end-users' understanding of the security features or security related events that they encountered on daily basis. In Chapter 2, computer warnings dialogue box contexts were seen as the focal point of this thesis. In this chapter, a more detailed investigation is given with regard to the practicality of security warnings, specifically considering dialogue boxes, in-place, banners, notifications and balloons.

According to Seifert et al. (2006), security warnings successfully discourage users from encountering computer threats. However, 16.92% participant in their studies proceeded to install an ActiveX component (i.e. ignoring the security warning). This study was in line with Wu et al. (2006), namely that the security was not the users' primary concern. Thus, the security warning was presented as distraction to end-users because it hindered the completion of their current task. As presented in Chapter 2, end-users were not really understood and paid attention towards the warning and they even did not understand the implication of ignoring the warnings. Based upon current literature and the author's knowledge, there was a lack of research into evaluating and accessing users' understanding of the features of the security warning specifically in dialogue box contexts. However within this chapter, security warnings contexts can be viewed in a broader context, so that a comparison can be made of which of these contexts is more dominant. Following this, a more focus study can be tailored to solve the problem later.

The aforementioned study was unable to examine the effectiveness of the features available in security warning from end-users experienced dealing with it. For instance signal icons, signal words, help function, technical terminology and available options (i.e. with the aim developing a meaningful feature to help users). Hence, this chapter (i.e. user study 2) describes further investigation of how end-users dealing with security warning features on daily basis during practical tasks. The core of the study involved participants identifying perceived security warnings that were encountered during

normal system use, and then recording feedback regarding the extent to which they understood them. It is anticipated that this finding will help to determine the features that are useful and important to make sure users comprehend the meaning of every security message that they receive, and are able to use the features accordingly.

4.2 Methodology

User study 2 made use of software prototype that had been developed as part of the practical assessment for participants (i.e. respondents were required to install and used the software for approximately fourteen days). Fourteen days was considered to be appropriate to give participants ample time to capture what they believed computer warnings to be all about. It is expected that users did not have to be rushed and they were able to undertake this user study at their convenient time. In addition, based on the author's knowledge and observation, most studies related to warnings research focused on trial experiment rather than gave them opportunity to use it at their own time (i.e. one-to-one session or user trial) (Sharek et al. 2008, Raja et al. 2009 and Kauer et al. 2012). Therefore, the author wished to explore this gap by using the proposed technique.

This study was approved by the Ethics Committee, as with the previous user study. The subjects were recruited predominantly from among Plymouth University's students and staff, as well as friends and relatives. Ten questions were provided in the questionnaire (i.e. based on human in the loop (HITL) framework which involved communication delivery, communication processing and application). By using some elements within this framework, this study started by focusing on security communication components (i.e. the type of communication involves – warnings dialogues contexts).

It may be noted that this experiment used a different approach to the methods presented in Chapter 2 in order to probe security warnings in further detail. As there is no one specific method to be used, the author believed that manually capturing the security warning would be more useful, because users have their own experience and beliefs of what a security warnings is. Therefore, this provides more realistic evidences and insights from end-users. Having used the software installed in users' computer without any interruption from investigator also provided a new dimension in order to produce

more reliable results. Users would no longer feel they were being watched and would possibly be able to show their true attitude (Oppenheim 1996).

Users were required to capture the security warnings on a daily basis, and answered the questionnaire for every warning that they had captured. These processes took approximately less than five minutes to complete (i.e. captured warning and answered questionnaire). User also had been advised to capture two to five images per day. Users were reminded by the principal investigator when fourteen days were approaching. Shortly after this, users were required to send the zip file within the installed software via e-mail.

4.3 Study Design

This study was promoted to the end user community via e-mail, news entry information on university's internal staff and student websites and word of mouth among colleagues in April 2011. The software prototype to support the experiment was developed using Microsoft Visual Studio Professional (2010), specifically using Visual Basic platform. This platform was chosen due to its suitability and the effectiveness on web and system development. This software was divided into three main sections. Personal details encompassed demographic details of respondents, capture utilized users' action to capture for every security warning they encountered (i.e. it had been simplified by using short cut key) and questionnaire covered list of questions that users' must answered based on every captured security message (See Appendix B in guidance sheet on user study 2).

4.4 Questionnaire

There were four main sections to the questionnaire, as depicted in Figure 4.1. The first section showed list of pending questionnaires which comprised of ID, date captured and image name. This was the location where users were able to view the security warning that they had captured before. By clicking any item on the lists, users were able to view the warning image on the image view section. On the other hand, section three asked about the event details of the security warning that user had captured that comprised the event name and source of the browser. Meanwhile, section four consisted of ten questions (i.e. questionnaire) that covered users' understanding of security features such

CHAPTER 4: A WIDER EVALUATION OF PERCEIVED SECURITY WARNINGS

as signal icons, signal words, technical terminology and available options (with the aim developing a meaningful feature to help users) as depicted in Figure 4.1. Some of the questions presented related to perceptions and attitudes that related to the decision making process and risk. These questions were created based on the Human in the Loop (HITL), which provides a systematic method to design security problems and help to understand end-user behaviour when they perform security-critical functions (Cranor 2008).

These questionnaires were used to further clarify from the aforementioned study in Chapter 3. Five likert-scales have been widely used as part of questionnaire types (Faulkner 2000). According to Oppenheim (1996), there were two main benefits on using the likert-scale. Firstly, it provided more precise information and users were preferred to a simple agree/disagree method of response. Secondly, it was able to explore and manifest content, with deeper ramifications of an attitude to be explored.

Questionnaire

ID	Date Captured	Image Name
26	02/03/2011	02032011130712_236875.jpg

Image View Please click the image to zoom in and out

Event Details
 Event Name:
 Source of Browser:

Questionnaire

	Strongly disagree	Disagree	Neither agree nor disagree	Agree	Strongly agree
1. The available options are enough for me to make a decision	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
2. The use of visual cues (e.g. words, icons, colors) helps to draw attention to the event	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
3. The message (and any associated help) provides sufficient detail to understand what to do next	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
4. It is clear from the message why it's been displayed	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
5. The use of visual cues (e.g. words, icons, colors) helps me to understand the nature of event	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
6. I am likely to ignore this security message	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
7. I am aware of the risk if I ignore this message	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
8. This security message is confusing as it appears similar to others	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
9. There are enough information in this security message	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
10. I understand the urgency of this security warning	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

Skip Save

Figure 4.1: Questionnaire section

The questionnaire made use of the components available in Human in the Loop security framework (i.e. personal variables, intentions, communication delivery and

communication processing). In Figure 4.2, the questions were more specific to the usage of security features and level of information (i.e. elements that normally help users to comprehend warnings). By assessing these ten questions, empirical evidence was provided as to the initial problems with security warnings and some potential suggestions as to how to improve it can be gathered.

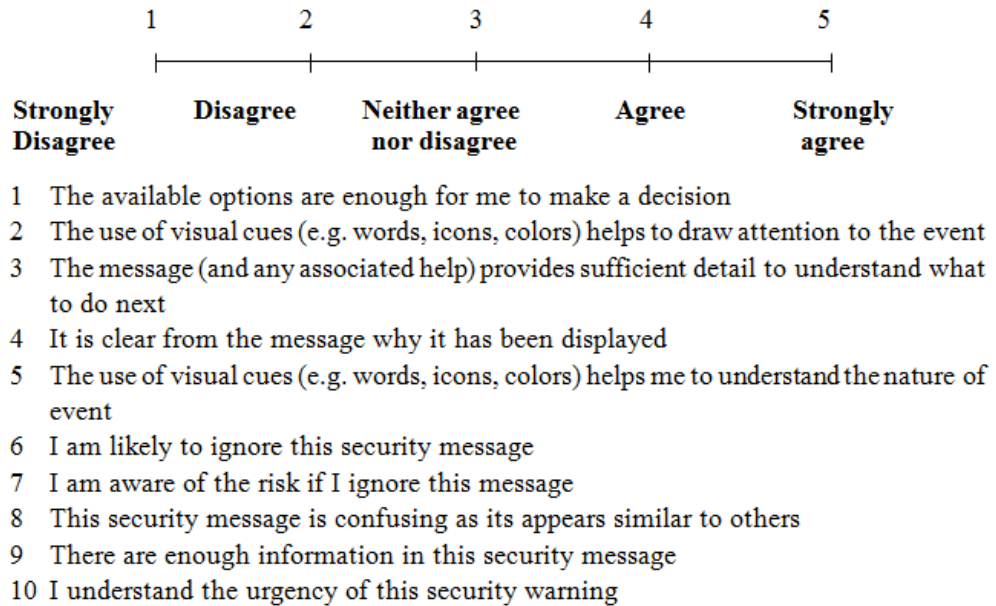


Figure 4.2: 5 likert-scales measurement with 10 questions

4.4.1 Study Protocol

In order to capture security message that users encountered, users used the short cut key (i.e. ALT-Z) instead of pressing the capture button on the main interface. The rationale was to simplify the capture action without showing the main interface again (i.e. did not want to distract current users' task). For every successfully captured process, notification appeared from users' system tray as depicted in Figure 4.3.



Figure 4.3: Notification upon successful captured every security warning

To ensure that users were able to access this page, they could double click the “U” icon or double click the notification from the system tray. The capturing process took less than five seconds per image captured and less than five minutes to read and answered the questionnaire. Users had been reminded that they were no right or wrong doing in this study. After fourteen days, users were required to send results using the “send files back” function on the software (i.e. data will be automatically zip and send to author’s e-mail). These were the summary steps undertaken by users in order to complete the tasks:

- 1) Firstly, users click any one item in the **List of pending questionnaires** until they see blue highlighted colour on the item
- 2) Then, users can preview the image in the **Image View** that they have captured.
- 3) Click on the image to zoom in and out (Note: once users’ mouse hovers inside the Image View, the border will change to blue and the mouse pointer will change to a magnifying glass icon).
- 4) Then, control the **panel** movement (up, down, left or right) to see the specific warning/message that you have captured.
- 5) Later, users answer the questionnaires with regards to the image that users have viewed. If they decide to do it later, press the **skip** button (It will minimize the program back to system tray).
- 6) If users decide to answer the questionnaire straight away, all questions are compulsory. They have to answer all until the save button is clicked.
- 7) At any time, if users would like to view again how many images are still pending in list of pending questionnaire, they double click icon U from system tray.
- 8) After 14 days, users receive an e-mail reminder that they need to submit the results of the study by clicking “**Send Files back**” to researcher’s specified e-mail.

(Note: Details of instructions (i.e. research information sheet and guidance sheet) are given in the Appendix B)

4.4.2 Study Participants

This study recruited 40 participants from both the university and public community (18 males and 22 females). It may be noted that from the previous study (i.e. user study 1 in Chapter 3), the total number of participants drastically decreased to only 40 participants with this user study 2. This indicated the inconsistency between both users study.

However, there were some rationale and considerations took place. It was a challenging task to get a committed participant especially when it involved them to install the software and sent the results back. Users were expected to give full commitment especially in regards to their time. Therefore, 40 participants were considered sufficient, as most of other studies related to warnings domain used between 20 to 40 participants in their experiments (Brustoloni & Villamarin-Salomon 2007, Stoll et al. 2008, Sharek et al. 2008, Keukelaere et al. 2009, Raja et al. 2009 and Kauer et al. 2012). However, from the author's point of view, the greater the number, the better the results. With this particular user study, only 40 committed participants fully completed the experiment.

Users installed the software to be used for fourteen days. All of the figures and percentages reported here were based upon the proportions of respondents in this study (i.e. due to rounding some of the presented results do not total 100%). The user was also reminded that they had the right to withdraw from this study at any time.

4.5 Results and findings

The overall outcome of user study 2 was presented in Table 4.1. It can be revealed from this finding that surprisingly, more female participants participated than male participants. This result had a similarity with user study 1 which had been conducted and explained in Chapter 3. The majority of participants were aged 26-35 years, whilst the minority group were from the age of 46 and above. This result was not surprising, as the majority of participants had grown up in an information, communication and technology (ICT) era. In terms of educational background, the majority claimed to have at least higher education, and only two respondents had a GCSE/O level education. It may be noted that as this study was well promoted in the university's environment, it might contribute directly to a higher percentage of educational background as mentioned.

On the other hand, none of participants claimed to be a beginner in computing skills, and the majority declared with advanced and intermediate of level instead. As predicted, the majority of respondents demonstrated that they were using computer and Internet more than six years. Thus, this supported the previous results that majority of the respondents were from the younger generation that were more technical savvy based users. In terms of preferred web browser, the majority of users chose Google Chrome and Internet Explorer. This result was totally different as compared to the results in the user study 1 (i.e. Mozilla Firefox was the most popular option). Microsoft products (i.e. Windows 7, Windows Vista and Windows XP) were still the most popular choices for the operating system. With respect to the usage of security software, the majority of respondents demonstrated that they used antivirus or Internet security package as a precaution from malware attacks in their computer. Surprisingly one user claimed he/she was not sure about the use of security software.

This study also asked users about their perception of three issues (i.e. managing task using computer, satisfaction on layout of warning and level of concern on security of computer). The results as shown in Appendix B. It may be noted that most of the respondents found that managing task in computer was in the range of easy and very easy (i.e. equally split). With regard to satisfaction of security warning, 53% of respondents claimed they were satisfied, 33% chose neither easy nor difficult whilst leaving 8% claimed that it was difficult. Even though majority had claimed that they were satisfied but there were quite a high percentage (i.e. 33%) of responses unable to provide an absolute satisfaction with this issue. On the other hand, 68% were concerned with the level of security of the computer, 25% being were mildly concerned, and 7% did not know.

Characteristics (n = 40)	Frequency Distribution	Percentage Distribution (%)
Gender		
Male	18	45.0
Female	22	55.0
Age		
18 – 25	6	15.0
26 - 35	27	67.5
36 - 45	5	12.5
46 - 55	1	2.5
Above 56	1	2.5
Educational Background		
Postgraduate	18	45.0
Higher Education	19	47.5
Diploma, Further Education	1	2.5
GNVQ	0	0.0
GCSE/ O Level	2	5.0
Computing skills		
Expert	4	10.0
Advanced	21	52.5
Intermediate	15	37.5
Beginner	0	0.0
Years using computer		
<1	0	0.0
1 - 2	0	0.0
3 - 4	2	5.0
5 - 6	1	2.5
> 6	3	92.5
Years using Internet		
<1	0	0.0

Characteristics (n = 40)	Frequency Distribution	Percentage Distribution (%)
1 - 2	2	5.0
3 - 4	1	2.5
5 - 6	3	7.5
> 6	34	85.0
Preferred web browser		
Google Chrome	16	40.0
Internet Explorer	13	32.5
Mozilla Firefox	9	22.5
Safari	2	5.0
Opera	0	0.0
I do not know	0	0.0
Preferred operating system		
Windows 7	16	40.0
Windows Vista	4	10.0
Windows XP	18	45.0
Mac OS X	2	5.0
Linux	0	0.0
I do not know	0	0.0

Table 4.1: Summary table of user study 2.

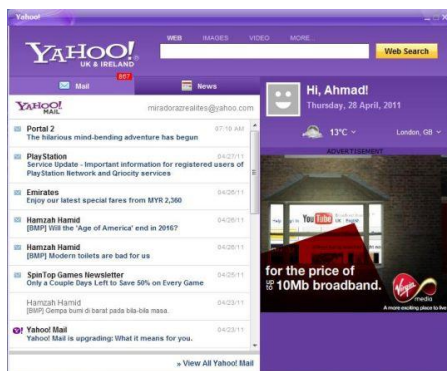
4.5.1 Classification of security warnings contexts

At present, Microsoft (2010) provides the guidelines for design concept of security warning for Windows products. For instance, the guidelines are applicable to Internet Explorer browser, operating systems and Microsoft Office packages that further explain the usage contexts (i.e. includes standard icons, dialog boxes, notification, warning messages and error messages). In order to probe the security warnings accordingly, this chapter presents five contexts of security warnings based on what users had captured. These five contexts are based on Microsoft guidelines as a basis reference for the study, due to its popularity and ease of use. The classifications were summarised briefly and presented in Chapter 2 (i.e. dialogue box, notification, balloon, in place and banner). Users were told that they had to capture security warnings in general (i.e.

without explaining specific contexts). However, the author provided one example in the Guidance sheet as a reference.

4.5.2 Misinterpreted scenarios

As users were able to capture the screen images based on their understanding, various types of perceived security warning were compiled. Users had their own interpretation of what they understood about security warnings, and they referred to guidance sheet to make sure that they did the right process. However, some still had false interpretations what might constitute a security warning, as depicted in Figure 4.4. It may be noted that users were unlikely to have captured these by mistake, as none of them reported this in any of their later feedback.



User 1



User 2



User 2



User 3



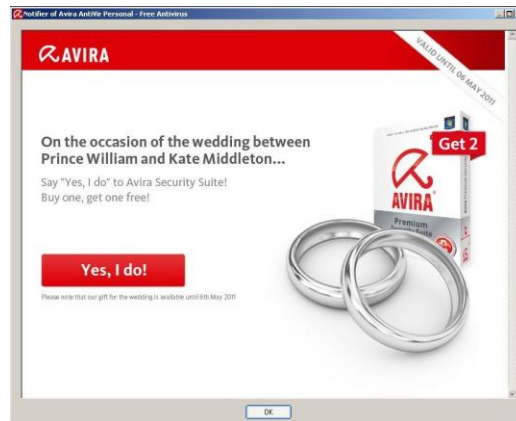
User 4



User 4



User 5



User 6

Figure 4.4: Dialogues that were misclassified as security warnings

It may be noted that most of the captured warnings can be categorized in advertisement type instead of the real security warning. Please note that respondents had been told about the definition and example of security warning in the guidance sheet. From these results, it can be confirmed that some users were still in baffled to identify the real security warning. For instance, user 5 and user 6 captured a dialog box of Avira anti-virus. This might be because they were aware of the brand name of Avira and the details on the dialog box related to security issues so that they considered it as security warning. A surprising finding was that one of the user derived a postgraduate degree and claimed as expert for computing skills as depicted in Table 4.2 but still unable to capture the right security warning. One possible reason that these is happening because respondents might interpret any type of pop-ups they received (i.e. with or without intention) on their computer as security warning. Hence, they simply capture it without thinking about whether it is a real security warning or not.


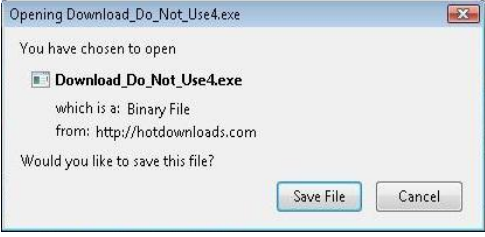
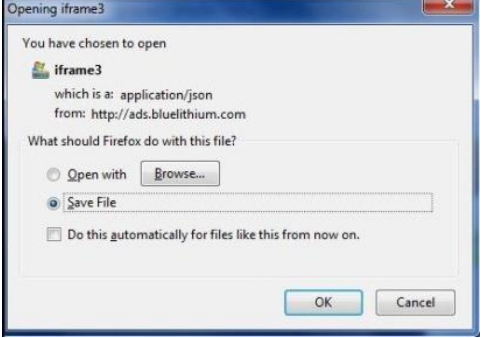
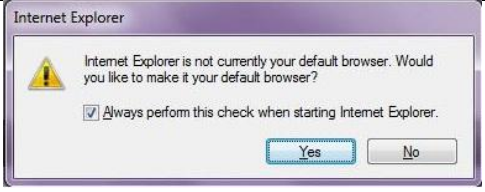


User	Education Level	Computing skills
User 1	Higher Education	Expert
User 2	Postgraduate	Expert
User 3	Postgraduate	Intermediate
User 4	Higher Education	Advanced
User 5	Higher Education	Intermediate
User 6	Postgraduate	Expert

Table 4.2: Comparison table on education level and computing skills

These results reflected how end-users assessed and identified the security warning on daily usage of computer. Having claimed themselves as advanced or even expert did not guaranteed that they really understood the real meaning of security warning. Overall, this indicated that some users had difficulty in identifying and understanding the security warning in the first place.

4.5.3 Results of classification

Overall, there were 234 security warnings images captured by participants, regardless of any context of warnings (i.e. dialogue box, in place, notification, banners and balloon). This section presented the results based on five classifications of warnings. The overall cumulative likert-scale referred to the total of likert-scale values (i.e. the sum of scale value on every question). Meanwhile, the average or mean referred to the overall cumulative likert-scale divided by total of security warning captured on each context (i.e. dialogue box, in place, notification, banners and balloon). It may be noted that the outcome from the table presented in each contexts was derived in general overview instead of derived it from one specific type of security warning. However, in certain scenarios (i.e. where more respondents captured the same security warnings) further assessment was discussed in greater details. Users generally demonstrated a satisfactory level of knowledge with regard to event details (i.e. event name and source of browser). However, in some contexts of warnings, they were still confused about how to classify it as presented in Table 4.3. The results portrayed as follows were derived from responses to multiple views on event name (i.e. Different respondents might views each dialogue differently).

Security warning image	Error message	Warning message	Info message	Help message	I do not know
 <p style="text-align: center;">A</p>		✓	✓		
 <p style="text-align: center;">B</p>		✓	✓		
 <p style="text-align: center;">C</p>		✓			✓
 <p style="text-align: center;">D</p>		✓	✓		
 <p style="text-align: center;">E</p>			✓		✓
 <p style="text-align: center;">F</p>	✓				

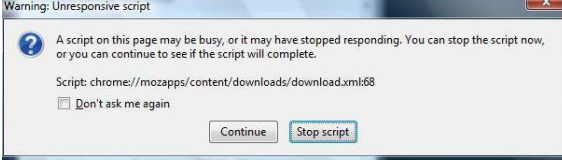


Security warning image	Error message	Warning message	Info message	Help message	I do not know
 <p>G</p>			✓		
 <p>H</p>	✓				
 <p>I</p>					✓

Table 4.3: Respondents’ event name classification based on the captured security warnings

It may be seen from this table that some of the respondents’ classified the dialogues correctly whilst leaving the others in baffled. For instance, dialogues box B was derived from Mozilla Firefox. It was supposed to be a warning message, but some users classified it as an information message. Based on the layout presentation, this security warning dialogue did not provide sufficient information to users. There were no icons or specific wordings to indicate risk levels, and no help features to help users to search for more information. By observing security warning C, respondents claimed that it was a warning message whilst some did not know about the event details.

On the other hand, dialogue in D was captured by one user whilst using Internet Explorer. He/she classified this warning dialogue as an information message. Surprisingly, based on the depicted dialogue, warning icon has been used. However

when reading the main question on the message “Internet Explorer is not currently your default browser. Would you like to make it your default browser?” it can be argued that by choosing “no” there was no bad implication at all, rather than having opportunity to use other browsers.

According to Microsoft (2010), a warning icon can only be used when the warning present a condition that might cause a problem in the future which is not happen with this security warning. Clearly in this scenario, there was a conflict on the usage of signal icon with the current context of warning. It may be suggested that it is better not to use any icon with this dialogue box to avoid any confusion. The information provided in the warning may convey the meaning of the message.

With regard to dialogue box E, some respondents classified it as information message (i.e. users might think that question mark icon is related to delivering information) whilst one user was unable to make a decision. Dialogue box in F clearly indicated the message as an error but surprisingly warning icon had been used. Similar problem occurred in warning G because question mark icon had been used instead of warning icon. In dialogue H, when users entered wrong username or password, users classified this as error message (i.e. in fact the right option). However, a warning icon was used to indemnify the error. On the other hand, one respondent was not sure about the event name of this banner albeit information was used. Having understood these circumstances, it was seen that some users perceived security warning differently as they had their own mind set with regards to the warning that they captured. It may be suggested that they just ignored some useful features available to help them make a better decision.

4.5.3.1 Dialogue box

Before going into further detail, each of the presented tables within this section refers to the questionnaire depicted in Figure 4.2. There were 191 security warning in dialogue box context that users captured. The likert-scale values were added together from the 191 security warning dialogue box context to get the overall cumulative values. Then, to get the mean values the overall cumulative likert-scale was divided with the total of warning (i.e. 191). It can be noted that the majority of respondents demonstrated that

they were in the middle range between “neither agree nor disagree” and “agree” with regards to their decision with almost all of the questions presented. From these results, among two lowest mean values presented were on question 3 and question 9 (i.e. this did not apply to question 6 and 8 – the lowest means better). This indicated that some improvements are needed with regard to helping function and information provided in the security warning. None of the results presented showed that users were fully satisfied with the current context of the security warning (i.e. likert scale value = 4).

	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10
Overall Cumulative likert-scale	697	737	676	691	700	531	700	494	632	702
Mean	3.65	3.86	3.54	3.62	3.67	2.78	3.67	2.59	3.31	3.68

Table 4.4: The mean respondents on answered questionnaire in dialogue box contexts.

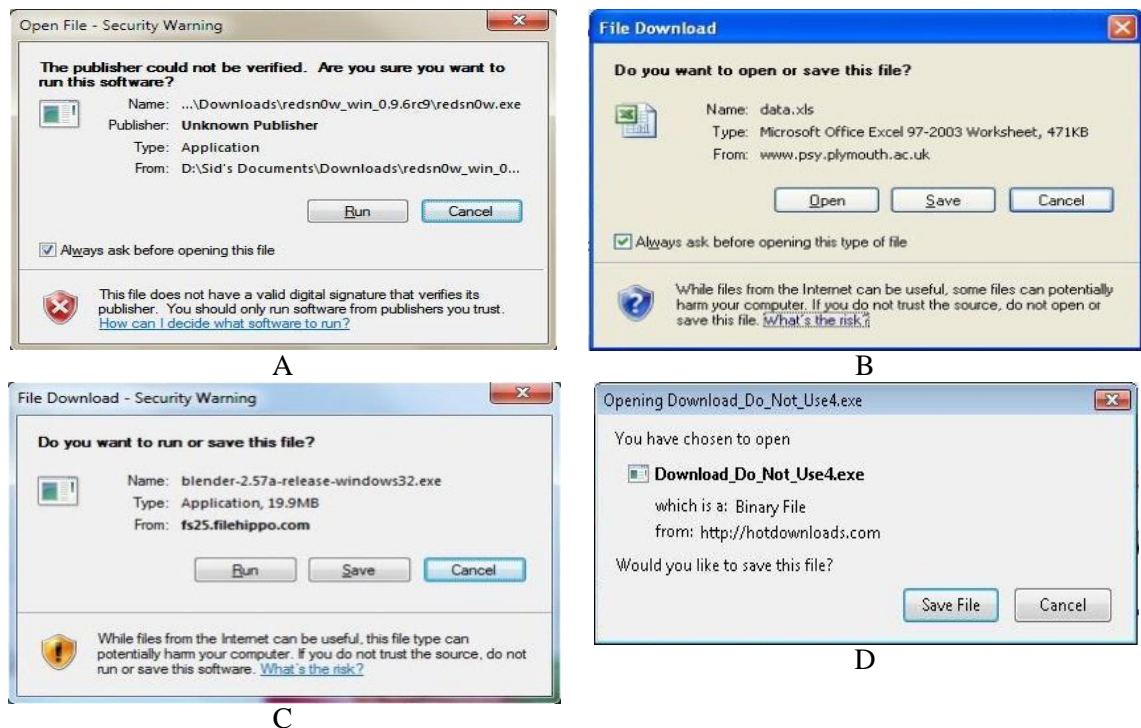




Figure 4.5: The most popular captured security warning demonstrated by respondents.

The security warning presented in Figure 4.5 was among the most popular captured by respondents. It may be noted that the combination of signal cues (icons and words), technical terminology, help options and available choices had been used in this context. For instance, two respondents had captured security warning A. Again with this security warning, the similar lowest mean value were on question 3 and question 9 as presented in (i.e. similar results with overall as depicted in Table 4.4).

	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10
Mean	4	4	3	3.5	4	4	4	2.5	2.5	4

Table 4.5: Mean value of security warning A based on the likert-scale

The author made a further assessment by evaluating the security features available to help users in this scenario. It can be revealed that the header of the warning indicated as “security warning” however in the footnote area, shield error icon was used. Based on Microsoft (2010), error icon should be used only to present error or critical but in this scenario, warning icon should be used instead to highlight a condition that might pose a problem in future. Based on the author’s observation, an error icon was used because the computer system was unable to recognise the publisher and did not have a valid digital signature to verify the status. The main question presented to users was “The publisher could not be verified. Are you sure you want to run this software”. In order for users to decide whether to execute or not, they clicked the link at the bottom (i.e. footnote area) to get more information. From the authors’ view, having two separated details of information was not effective as users’ might thinking the information provides at the bottom is something that is not related to the main question. It may be revealed that there was an issue with the clarity of information and that there were insufficient help features to guide user through.

	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10
Mean	4	3.67	3.33	3.33	3.67	3	3.33	3	2.67	2.67

Table 4.6: Mean value on security warning B

Three users captured similar security warnings, as portrayed in Figure 4.5 – B. With this security warning, users demonstrated with 2.67 on average with question 9 and question 10 as presented on Table 4.6. This indicated that the information and the urgency of this security warning should be improved. The main question on the security warning asked “Do you want to open or save the file?” however, there were four available options for users (i.e. open, save, cancel/close and clicked the hyperlink). It was not clear how this security warning was able to help users in the decision making process as there were no clear direction on what to do after reading the main question. Albeit the footnote area was provided at the bottom to give some additional information, it presented similar problem as mentioned in security warning A.

A comparison can be made between security warning B and C. Both of security warnings looked similar but the main difference was on the header (i.e. file download and file download – security warning). With security warning C, the name of the file was .exe and it reflected the usage of icon at the footnote area (i.e. warning icon) and the header of the warning. .exe files (i.e. executable file) portray significant dangers in computer systems, as most of the malware are easy to propagate using this method. Surprisingly, both security warnings in B and C used the same information in the footnote area, but with different icons (i.e. it was not really clear how to convey the risk level).

	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10
Mean	3.14	3.29	3.14	3.57	3.43	2.57	4	2.57	3.29	3.86

Table 4.7: Mean value of security warning D

Security warning D was depicted from Mozilla Firefox browser by seven respondents. With this security warning, users demonstrated that they were aware of the risk if they ignored this security warning (i.e. question 7) but for the rest of the questions, the result were remain between the same range as previous security warnings. It may be noted that on question 1 and question 3, users demonstrated among the lowest mean values

(i.e. available option and help function). As presented in Figure 4.5 – D, this security warning presented very minimalistic features. It asked users “Would you like to save this file?” instead of offered them to execute the file straight away. However, no further information has been provided with regard to the risk or even more information about the file users wished to download. In this context, there was no further guidance for users to rely on in making decisions as to whether to save the file or not.

	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10
Mean	4.5	4	4	3	4	2.5	4.5	3	2.5	4

Table 4.8: Mean value on security warning E

On the other hand, two users captured security warning as presented in Figure 4.5 – E. This security warning was straight forward as the header of the warning clearly indicated as “security warning”. An exclamation icon was used to match the context of the message. With regard to the overall mean values, mostly respondents demonstrated that they “agree” with most of the questions presented. However, these two respondents demonstrated 2.5 on average with regards to the information provided as depicted in Table 4.8. This might be because of the information provided in this warning using more technical wordings in order to explain the current circumstances which lead to the complexity for users to understand.

	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10
Mean	3	4	2.5	2.5	2.5	3	3	3	2.5	2

Table 4.9: Mean value on security warning F

With security warning as depicted in Figure 4.5 – F, only two users captured the same warning. The header of the warning stated as “Microsoft Office Outlook” instead of using one specific name. These respondents agreed that the visual cues helped to attract their attention, but for the rest of the question, the mean values were not really convincing. The lowest average value was on question 10 (i.e. the urgency of the warning). These were similar results to the other warning which had been presented before, question 3, 4, 5 and question 9 portrayed among the lowest values with 2.5 on average as depicted in Table 4.9. By viewing the warning in detail, no further detailed features was provided for users, and not enough information was depicted except to request that users allow or terminate the process.

4.5.3.2 In Place

There were fourteen in place security warning context that users captured accordingly. As depicted in Table 4.10, the majority of users demonstrated their understanding of the in place context of security warnings. This was not a surprising finding because it related to an e-mail log in scenarios. It showed that users demonstrated that they were familiar with this context and most of these respondents might use e-mail services on a daily basis.

	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10
Overall Cumulative likert-scale	61	60	59	62	57	30	58	27	56	58
Mean	4.36	4.29	4.21	4.43	4.07	2.14	4.14	1.93	4	4.14

Table 4.10: The mean respondents’ on answered questionnaire in in-place contexts.

As presented in Figure 4.6 - A and B, most in place warning were captured from e-mail services. As most of the respondents were familiar with e-mail usage, it was not surprising that most of the average values were in the range of “agree” to “strongly agree” (i.e. except in question 6 and question 8). It may be noted that this context of security warning was not a frequent warning that users normally encountered, as compared to dialogue box contexts.



Figure 4.6: In-place security warning contexts captured by respondents

4.5.3.3 Notification

A documented guideline by Microsoft (2010) stated that notifications must be ignorable (i.e. at least temporary). It did not require user to take an immediate actions as it only shows user with unrelated event to the current users’ activity. If the users are not distracted or feel obligated to read it, then the notifications can be considered successful. However, in reality, designers created a notification to get users’ attention so that they will not ignore it. Microsoft (2010) used its design pattern for notification implementation, as depicted below in Table 4.11.

Pattern	Descriptions
Action success	It will be used to notify users when asynchronous and users initiated actions completed successfully
Action failure	It will be used to notify users when asynchronous and users initiated actions fail.
Non-critical system event	It will be used to notify users on significant event that can be safely ignored. (temporarily)
Optional user task	It will be used to notify users of asynchronous tasks that they should perform. (Optional or required, it can be safely postponed)
FYI	It will be used to notify users of potentially useful and applicable information. (Notify users of information if it is optional and users opt in)
Feature advertisement	It will be used to notify users of newly installed, unused system or application features.

Table 4.11: Design pattern for notification in Microsoft

	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10
Overall Cumulative likert-scale	40	42	41	43	41	39	37	26	36	41
Mean	4	4.2	4.1	4.3	4.1	3.9	3.7	2.6	3.6	4.1

Table 4.12: The mean respondents’ on answered questionnaire in notification contexts.

Overall, ten notifications had been captured by respondents. It can be revealed that most of the respondents did not find much problem with this context of warning as depicted in Table 4.12. The lowest mean value (i.e. except in question 6 and 8) was on question 9 with regard to the information provided. One of the possible reasons that contributed to the high mean value (i.e. 4 or more) was that notification appeared only for few seconds, with rare frequency. Therefore, most users might not realise it, and ignore the existence of such warning. Based on the captured security warning notification contexts on Figure 4.7 (A-D), various levels of information and icons were used.

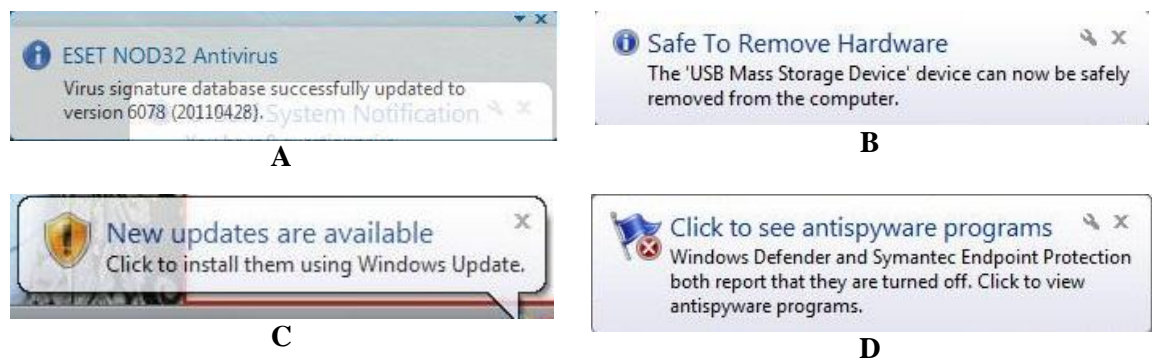


Figure 4.7: The average respondents' on answered questionnaire in notifications contexts.

4.5.3.4 Banners

This study reveals that eighteen banners images were captured. According to Microsoft (2010) information icons can only be used in a banner context and not with other contexts. The reason was that another context was able to communicate the information to end-users sufficiently. However, results revealed that there were a variation of signal icons been used for banners as depicted in Figure 4.8 (A - F) (i.e. some of these were not from Windows platform). Generally, users demonstrated their understanding with "neither agree nor disagree" with questions related to banner as depicted in Figure 4.7. This might be because of this context of security warning appeared occasionally. In addition, it appeared in a tiny size to view and at a specific location on the web pages which made respondents unaware of their existence (i.e. below the toolbars and address bar). It may also be noted that some of these banners using technical jargon such as pop up blocker, add-on and restore. It may be seen that the least mean value (i.e. except question 6 and 8) was on question 5. Respondents claimed that they were not really

sure about the visual cues (e.g. words, icons and colours) that helped them to understand the nature of the event.

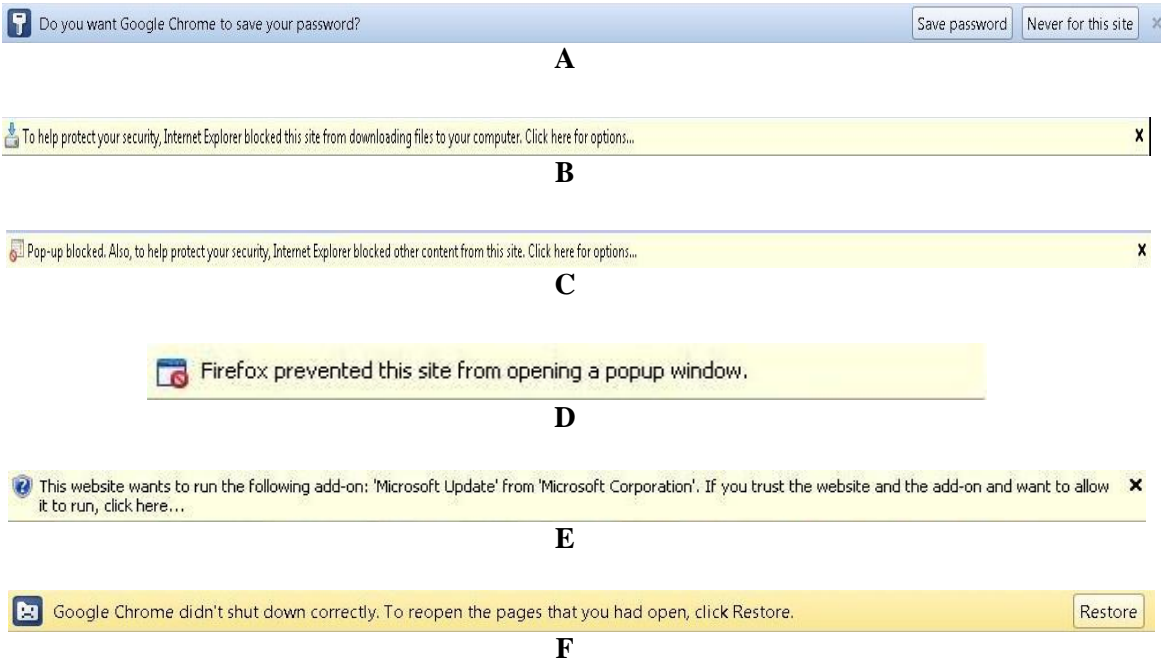


Figure 4.8: The average respondents' on answered questionnaire in banners contexts.

	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10
Overall Cumulative likert-scale	64	58	64	65	57	55	61	52	60	67
Mean	3.56	3.22	3.56	3.61	3.17	3.06	3.39	2.89	3.33	3.72

Table 4.13: The mean respondents' on answered questionnaire in banners contexts.

4.5.3.5 Balloons

Surprisingly, only one user captured security warnings in a balloon context as results in Table 4.14. This might happens because users are not aware of the balloons as one of the security warnings contexts. Therefore, even if they had encountered or experienced balloons contexts, they did not classify them as a security warning in the first place. It can be noted that this respondents did not face many problems with regard to the balloon warning contexts that he/she had captured. All of the questionnaire questions were answered without any level of difficulty. The author's believed that because the

existence of the balloon was very short-lived, users did not have much problem dealing with it.

	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Q8	Q9	Q10
Overall Cumulative likert- scale	5	5	4	5	5	1	4	1	5	5
Mean	5	5	4	5	5	1	4	1	5	5

Table 4.14: The mean respondents' on answered questionnaire in balloon contexts.

4.6 Users' feedback

Users' feedback was derived from an e-mail sent by responses upon completion of this user study. This feedback was not a compulsory task for users. Although not representative, below are the selected responses:

- i. "I have not experienced this concept of experiment before and I found it to be unique and useful (i.e. install in computer and send the zip file)" (User 5)
- ii. "Having manually captured security warnings is a good idea but sometime it is tedious job when you do it repeatedly" (User 12)
- iii. "I am not so sure what a security warning is. As long as it pops-up in my computer, I would assume it is a security warning" (User 23)
- iv. "Whatever it is I think that the presentation of computer should make it easy for users to use. Warnings seems to look very similar between one and another" (User 31)
- v. "Some of the security warnings that I have encountered presented with technical details that I do not understand it at all. and no further help for me to rely on" (User 38)

Based on these comments, one user claimed that security warning was presented with some difficulties with the usage of technical terminologies (i.e. consistent results with user study 1). The user also claimed that security warnings looked very similar between

one and another. Hence, it made him/her baffled because of the difficulty of differentiating the problem. It would be useful if this study could examine in further detail with the comments presented to further clarify the problems.

4.7 Discussions

Overall, this study has highlighted how end-users dealing with security warning features on daily basis. Based on the five contexts of security warning presented in previous section, generally users demonstrated good understanding of the features provided in the warning, especially in three contexts (i.e. in-place, notification and balloon). However, with regard to the other two presented contexts (i.e. dialogue box and banners) significant attentions are needed (i.e. satisfactory level). Based on the mean values presented on both contexts, users demonstrated their decision were in the middle range between “neither agree nor disagree” and “agree”. There was no absolute answer (i.e. “agree” or “strongly agree”) chosen within these two contexts. A small percentage (i.e. 15%) of overall participants misunderstood what they believed security warning was in certain security warning which they had captured. Albeit it only occurred among few participants, it indicated how end-users viewed and understood security warning in one perspective (i.e. end-users mental model). This study also revealed that some users were unable to classify the correct warning classification upon presented event details (i.e. users chose event name from drop down list).

It may be noted that security warning in dialogue context became the most popular context captured by all of the respondents. This revealed that this context of warning became the dominant context to present warning from most of developers. In addition, end-users were more aware of the existence and realised the concept of security warning in dialogue box context. Thus, this reflected the less popular captured security warning in other contexts. Based on some presented scenarios, it may be revealed that some of users were still having difficulties with current implementation of security warning especially with regard to help features and information provided in the warnings. From the authors’ observations, some conflicts occurred with regards to the implementation of signal icon and signal word (i.e. inappropriate usage). Some of security warning presented still use technical terminology to explain to users about current context of warnings. In addition, there was no specific guidance available for users to rely on

before they able to make any decision except the link provided at the bottom in certain warning dialogues (i.e. footnote area).

Therefore from the holistic investigation results, this study produced encouraging results, especially with regards to security warning dialogues and banners contexts. By using this method of study (i.e. users identified and manually captured what they believed security warning was) provided an insight into how users comprehend the warnings in various contexts.

4.8 Constraints

The software that users installed was unable to detect the security warning automatically, as the task was set to be a manual task for end-user to identify the security warning, and later answer the questionnaire. Users were able to capture the same security warning more than one time as the software unable to detect the duplication. The questionnaire was created using HITL framework elements, but it did not come out with final results in regards to users' behaviours as proposed in HITL. The user had to choose fixed answers instead of having open-ended type of answers on the presented questionnaire. Hence, there was less flexibility in terms of providing some useful thoughts whilst experiencing what they believed security warnings were.

4.9 Conclusions

Having understood all of the evidences from this user study, it may be concluded that there is a need to improve the current implementation of security warning, especially in dialogue box contexts. Some conflicts even occurred based on the aforementioned results presented based on the authors' observation (i.e. end-users might not realised it as no specific questions were asked related to this). None of the overall mean values in security dialogue context was recorded as more than four. Most of the users within this contexts demonstrated that help function and information in security warning could be further improved (i.e. Users demonstrated overall mean value range was between three to four with regards to question 3 and 9). Even though the mean value was not statistically significant, the presented value at least presented some indication how end-users assessed the current features of security warnings. It provided empirical evidence

to highlight the real problems encountered by end-users. By understanding and evaluating the problems, this thesis helps to further appraise computer warnings in real-time contexts in Chapter 5.

CHAPTER 5

Further Appraisal of Security Warnings in Real-Time Contexts

5 Further Appraisal of Security Warnings in Real-Time Contexts

5.1 Motivation

Having gathered all of the aforementioned evidence, it is useful to confirm from the end-users whether they really need to have more information with regard to the security warning dialogue that they received in real-time contexts. In the aforementioned Chapter 4, the author focused on how end-users dealt with security related events warnings in the various contexts that they may encounter during the day-to-day use of their systems. This involved practical tasks, in which security warning dialogues were manually identified and captured by the end-users. This provided a basis for an understanding and assessment based on features that were useful and important so as to ensure that users comprehended the meaning of every security context they received and were able to use the features accordingly.

After manually capturing what users believed a security warning was, they were required to answer the event details and questionnaire section. Based on the findings, users demonstrated that they understood the overall presentation of warnings, especially in the in-place, notification and balloon contexts of warnings. Users experienced significant problems with dialogue box and banners contexts (i.e. mean values in the range of 3 to 4). Even though the results were merely at a satisfactory level, this gave some indication that users were still in a dilemma within the questionnaires presented. It may be revealed that within these two contexts, there was no absolute answer (i.e. “agree” or strongly agree”) based on the mean value presented. 15% of overall users misunderstood what they believed security warnings to be, mostly by capturing advertisement dialogues which looked like security warnings. From the questionnaire results, end-users mostly had significant problems with regards to the help features and information provided in the warnings (i.e. Dialogue box mean values Q3 = 3.54 Q9 = 3.31).

If users are unable to understand the information provided (i.e. by using the help facilities provided) this may lead them to make incorrect decisions that may jeopardise security and protection on their computers. Therefore, in continuation of the previous

investigation, this chapter seeks to reveal whether sufficient information was provided for end-users for each security warning dialogue received in real-time contexts, on a daily basis. In order to achieve this aim, a software prototype was developed to detect the dialogue box pops-ups automatically. Once this software detected the dialogue box (i.e. via class name/application name), a custom dialogue box automatically popped up shortly after users made a decision regarding the dialogue box they received earlier. Then users able to answer the survey via a custom dialogue box in real time contexts. In these contexts, the author focused only on the detection of dialogue boxes.

5.2 Methodology

A survey tool was developed to assess users' understanding of whether enough information was provided on the current security warning dialogue boxes. This software was designed to detect the header, class name, application type, dialogue received time and dialogue decision time. However, the main detection process was based on the class name/application name of the dialogue box used on the first place. Based on the author's knowledge, it was seen as difficult to detect one specific type of security warning dialogue, especially when this involved different web browsers and applications. Therefore, a possible means of detecting security warning dialogue box contexts was by using the class name or application name, as depicted in Table 5.1. For the purposes of this experiment, a security warning dialogue box from three main web browsers became the focal point of the investigation (i.e. Internet Explorer, Mozilla Firefox and Google Chrome). However, dialogue boxes from operating systems and other applications that shared a similar class name were also captured.

ClassName	Application name (.exe)
#32770	Explorer.exe
Chrome_WidgetWin_0	Chrome.exe
MozillaDialogClass	Firefox.exe
MozillaUIWindowsClass	Firefox.exe
MozillaWindowClass	Firefox.exe

Table 5.1: Example of Class Name and Application name from three web browsers

As the detection process of specific security warning was difficult to achieve, every dialogue box that users received was considered to be a security warning. The rationale behind this was that most security warnings came in the form of a dialogue box. Therefore, end-users were more aware of the security warning within this context, rather than other forms of security warnings (i.e. results from user study in Chapter 4 for further details). In addition, every dialogue box that users received involved many features to help them comprehend the meaning of the message (e.g. signal icons, words, help or guidance features), and this became one of the main investigation concerns of this study.

On the other hand, Microsoft (2010) guideline was used as a reference or basis for this study. The author realised that this guideline could only be used with Microsoft products but it is still relevant to use it as a main reference in order to compare on how other browsers implemented such features (i.e. as discussed in Chapter 2, 3 and 4) because no other guidelines was available as complete as Microsoft version (i.e. based from the author knowledge). However, the main focal point of this user study was to assess the security warning dialogue that specifically involved with end-users decision making that impacted security and protection of their computer (e.g. downloading software, updated security patches, passwords). To be more specific, most security warning dialogues within these scenarios presented at least two or more options for users to choose.

If users encountered security warnings with one option, it is still useful for the author to analyse the effectiveness of current implementation of security warning dialogue with regards to the adequacy of information provided to help users. Security warning with one option was inclined to focus on fixed decision such as “Yes” and “Ok” instead. Therefore, these contexts of warning tended to give instant information, rather than show the criticality of decision making that significantly impacted the security and protection.

For every security warning dialogue that users received, they had to make a decision by choosing any available option given (i.e. by pressing any button or close). After this, users were presented with a custom dialogue box (i.e. in real-time), and were asked about the sufficient level of information on the warning dialogue that users had just

received. This software also captured the “receiving time” for every security warning that users received, and “action time” with regards to the time when users took any action on the security message (i.e. by pressing any button or close). Later, the outcomes of this user study were sent via zipped file to the principal investigator by e-mail or drop box application (refer to Appendix C).

Based on the initial investigation by the author, no specific technique had to be abided by in order to conduct research into security warnings. Therefore, the author made use in this study of assessing warning in real-time contexts. This task was seen to be very challenging because the program needed to interact with the operating system and other application (i.e. in order to hook security warnings in the first place). Further details will be provided in the next section.

5.3 Study design

The survey tool was developed using Microsoft Visual Studio Professional (2010), specifically using C# Programming language. This platform was chosen because of its ability to interact with Windows application programs and other browser developments. Users installed this software for five days in their own computer and they were able to use their computer as usual. All detection processes was conducted in the background. However, at some point, the custom dialogue boxes popped (i.e. for every dialogue box) as a distraction to end-users. Thus, users had been explained about this and they were aware about it on the first place. This user study was promoted using a similar approach with Chapter 4 (i.e. via e-mail, news entry information on university internal staff and student websites and word of mouth) in December 2011.

5.3.1 Survey

After the users had installed the software on their computer, they then needed to fill in a demographic survey. This section comprised demographic information on users’ background and experience related to general usage of computer (i.e. age, gender, education, computing skills, years of using computer and Internet, preferred browser and operating system). It may be noted that there were similarities in regards to the demographic details between this user study and the previous ones (Chapter 3 and

Chapter 4). The final part of this section required users to answer specific question related to decision making upon receiving security message in general context rather than to one specific type of security warning. This provided some basis for understanding end-users' perceptions of the security warning in the period before the main user study began.

5.3.2 Study protocol

In this study, each dialogue box that popped up on the users' computer was detected by a custom built-in program based on the Windows handle (i.e. class name, header and application name) from three main web browsers (i.e. Internet Explorer, Mozilla Firefox and Google Chrome) and from the other applications that shared a similar class or application name. These three web browsers were chosen because the majority of users have indicated that they were their preferred web browsers in previous user studies (i.e. Chapter 3 and 4). In addition, W3Schools (1999) also claimed that these three web browsers was considered to be the most popular choices. Users firstly had to install the software as with the previous user study in Chapter 4. Once the installation was complete, users received notification as depicted in Figure 5.1. This indicated that the software was now running and that the detection process of the dialogue box may begin at any time.



Figure 5.1: Notification appeared once the software was installed

For every single dialogue box that users encountered, they made a decision by pressing any of the available options provided (i.e. in this context, options were referred to buttons instead of the hyperlink). Once the dialogue box popped up, the software captured the "receiving time" and later, when users clicked any buttons, "action time" was also captured. In addition, the dialogue box image was captured and saved accordingly in a folder which pinned up a specific id in the database. After users clicked any of the buttons available, they quickly received a custom dialogue box

asking them: “Did you have enough information to understand the security dialogue that you just answered?” with three options; Yes, No and Not sure as depicted in Figure 5.2.

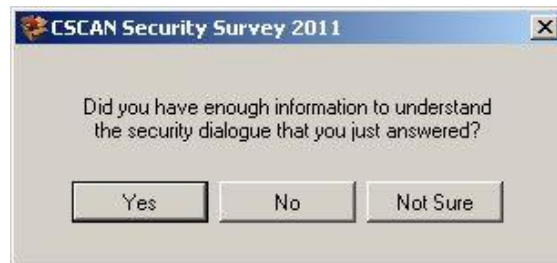


Figure 5.2: Custom dialogue box

Users received a custom dialogue box instantly or in real-time after took any action (i.e. by pressing any button or close) with previous security warning dialogue box. All users' decisions were saved in the database accordingly. Once everything was completed, users were required to send the results using the Dropbox application, which had to be installed in advance (See guidance sheet in Appendix C). This was a summary of the steps undertaken by the user to complete the tasks:

- 1) Firstly, users received a standard security message/warning (i.e. dialogue box)
- 2) Then, users made a decision (i.e. clicked any options)
- 3) Subsequently, users were presented with custom dialogue box with the questions about security decision making process.
- 4) Then, the user made a decision (i.e. clicked any options) and the results saved in database accordingly.
- 5) After 5 days, users were required to send the results either by handing in the pen drive or via the Dropbox application.

(Note: Details of instruction are given in the Appendix C)

5.3.3 Study Participants

This study recruited 36 respondents, which comprising 14 males and 22 females (i.e. almost consistent with previous Chapter 4). Respondents were primarily staff or students from Plymouth University, and some were from the public community. These respondents were allowed to use the software either in their workplace or home as long as they consistently used the same computer for five days. It may be noted that all

figures and percentages within this chapter were based on the proportions of respondents in this study (i.e. due to rounding some of the presented results was not total to 100%). Every user was reminded that they had the right to withdraw at any stage in the study.

5.4 Results and findings

From this user study, it may be revealed that 69% of total respondents were aged 26 -35 years, with at least an undergraduate level of study as depicted in Table 5.2. As this study was well promoted within the university's environment, it reflected the high percentage of higher and postgraduate level of education. In terms of computing skills, surprisingly, the majority claimed to be intermediate, albeit they claimed to have at least a higher education level. All respondents claimed to have used the Internet for more than six years. These results show that the majority of users were well versed in the usage of information technology. Interestingly, these results were similar to the previous findings, as discussed in Chapter 4. This study also revealed that Internet Explorer, Mozilla Firefox and Google Chrome were among the top choices in terms of their preferred web browsers. The majority also preferred to use a Windows-based operating system (i.e. Windows 7, XP and Vista) whilst only one user preferred Mac OS X. It may be noted that the vast majority of respondents demonstrated that they used security software (94.4%) whilst others were not using this, or were not sure (5.6%). The last question asked of users related to their perception with regard to the ease of use of security warnings in general. Users indicated here that they were able to make a security decision (44.4%), having difficulty (13.9%) and not sure (41.7%). Hence, 55.6% of total respondents claimed that they were still baffled with regards to the security warning decision that they had made in general. Based on this evidences, end-users had significant problems with regards to the decision making process that impacted the security and protection of their computers.

Characteristics (n = 36)	Frequency Distribution	Percentage Distribution (%)
Gender		
Male	14	38.9
Female	22	61.1
Age		
18 - 25	6	16.7
26 - 35	25	69.4
36 - 45	4	11.1
46 - 55	0	0.0
Above 56	1	2.8
Educational Background		
Postgraduate	16	44.4
Higher Education	17	47.2
Diploma, Further Education	0	0.0
GNVQ	0	0.0
GCSE/ O Level	3	8.3
Computing skills		
Expert	3	8.3
Advanced	13	36.1
Intermediate	19	52.8
Beginner	1	2.8
Security software usage		
Yes	34	94.4
No	1	2.8
Not sure	1	2.8
Years using Internet		
<1	0	0.0
1 - 2	0	0.0

Characteristics (n = 36)	Frequency Distribution	Percentage Distribution (%)
3 - 4	0	0.0
5 - 6	0	0.0
> 6	36	100.0
Preferred web browser		
Google Chrome	17	47.2
Internet Explorer	7	19.4
Mozilla Firefox	12	33.3
Safari	0	0.0
Opera	0	0.0
I do not know	0	0.0
Preferred operating system		
Windows 7	18	50.0
Windows Vista	1	2.8
Windows XP	16	44.4
Mac OS X	1	2.8
Linux	0	0.0
I do not know	0	0.0
Easy to make security decision in general		
Yes	16	44.4
No	5	13.9
Not sure	15	41.7

Table 5.2: Respondents demographic background

5.4.1 User interaction with various dialogue boxes

Each user faced different type of dialogue box based on their usage of web browsers and applications on daily basis. Overall, all 36 users captured 5923 dialogue boxes (i.e. that included the duplications). This software minimised the duplication processed by allowing the duplication to occur only once. If it occurred again, the dialogue box was ignored and no custom dialogue box would pop up. This thesis will not discuss every

single dialogue box captured; however it seeks to highlight the most suitable and appropriate within the context of this study (i.e. focused were given to security warnings dialogues that involved end-users decision making that impacted the security and protection of their computer).

Based on these findings, users experienced many types of dialogue box (i.e. some can be considered as security warning and some were actually not). Even though all pop-ups were treated as a security warning, the author later made their own classification, choosing the most relevant to be discussed in this chapter for further clarification. With regard to dialogues boxes which did not impact end-user security and protection, the author did not ignore or reject these, but used them to further probe the effectiveness of the features available (i.e. signal icons, signal words, technical terminology and help options). Table 5.3 presents some classifications of the dialogue box based on the application name. These classifications were derived from the most popular application name which focused specifically on three main web browsers Internet Explorer, Mozilla Firefox and Google Chrome. Therefore, the author believed that because of the familiarity of the dialogue box contexts by end-users, many security warnings dialogue box that users encountered would be derived from the mentioned web browsers. It may be revealed that on average, 52% of respondents of the three web browsers (i.e. Chrome.exe, Firefox.exe and Iexplorer.exe) chose no and not sure with regards to the information depicted in regards to understanding the security message that they received on daily routine within five days of the conducted studied. On the other hand, users demonstrated on average 33% with no and not sure with regards to the level of information based on four Microsoft Office applications (i.e. Excel.exe, Outlook.exe, Powerpnt.exe and Winword.exe). In terms of other applications, Acrord32.exe was generally related to the Acrobat process. Rundll32.exe, meanwhile, was related to the Dynamic Link Library files normally included in every application folder (i.e. open file and add/remove program) that can be accessed from multiple applications. Both were presented with 31.3% and 41.6% respectively.

Application Name	Quantity Detected	Yes	No	Not Sure	% No and Not Sure
Acrord32.exe	272	187	55	30	31.3
Chrome.exe	274	159	44	71	42
Excel.exe	73	58	7	8	20.5
Explorer.exe	679	416	110	153	38.7
Firefox.exe	363	133	141	89	63.4
Iexplorer.exe	422	214	108	100	49.3
Outlook.exe	581	500	32	49	13.9
Powerpnt.exe	47	21	10	16	55.3
Rundll32.exe	221	129	28	64	41.6
Winword.exe	503	292	66	145	41.9
	3435				

Table 5.3: Results of the classification of dialog box based on application name

The results indicated in Table 5.3 provided evidence that users generally faced difficulties in regards to the information presented on every security warning dialog box that they encountered on daily basis. The next following sections address the specific scenarios or cases that users experienced.

5.4.2 Conflicts with guidelines scenarios

In Chapter 4, the author used Microsoft (2010) as the basis or reference with regards to the guidelines that covered the design concept of security message contexts. Therefore, the assessment conducted was based on the Microsoft Guidelines. The purpose of the custom dialog box presented after each dialog box was to determine an answer from users based on the following question:

“Did you have enough information to understand the security dialog box that you just answered?”

Whilst assessing users’ feedback, the author compiled a set of security warnings that were considered to have problem with the usage of signal cues (i.e. icons and words) and its context. According to Microsoft (2010), there were four types of standard icons that had been used with a specific meaning:

- i. Error icon – It presents an error or problem that has occurred
- ii. Warning icon – It presents a situation that might cause a problem in future
- iii. Information icon – It presents useful information
- iv. Question mark icon – It been used as a Help entry point

By using this guideline as a reference for this study, it may be noted that conflicts occurred with the usage of icons in the dialogue box contexts, as depicted in Figure 5.3 (A-F).

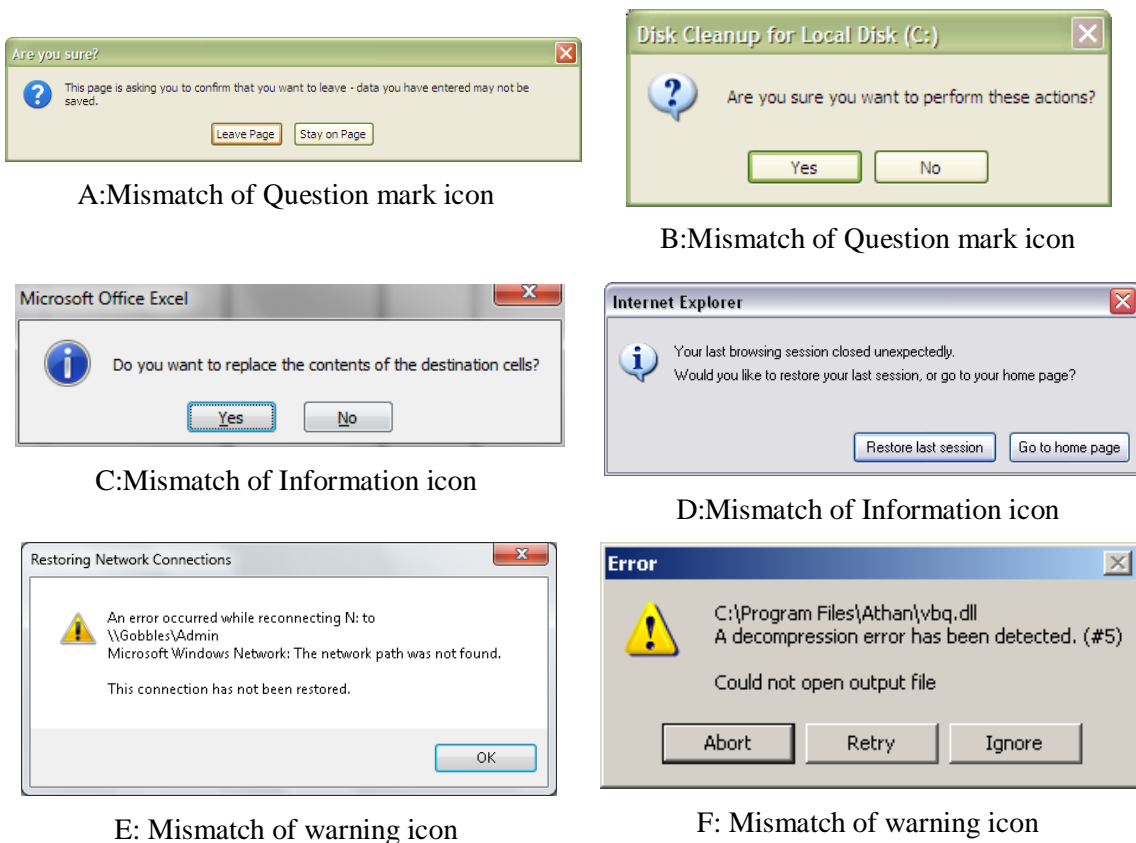


Figure 5.3: Conflicts on security warning features

Figure 5.3-A was derived from Mozilla Firefox. It used a question mark icon, in line with the header “Are you sure?” which can be portrayed as a question. Surprisingly, the other dialogues boxes were captured from Internet Explorer applications. Figure 5.3-B used the question mark icon to ask question whether the user should proceed or not to clean up the disk space. This clearly conflicted with the main purpose of the question mark icon that should be used as help entry point. On the other hand, Figure 5.3 (C & D) used the information icon, but surprisingly, it presented a question statement to users. Based on Microsoft (2010) Guidelines, the information icon may only be used to

present information in the banners context, and not in the dialogue box context. On the other hand, Figure 5.3 (E & F) used a warning icon to explain the severity of the message. However, the information provided in each warning had been described as an error (i.e. error whilst connecting and decompression error). Clearly, this conflicted with the basic use of a signal icon in the first place.

5.4.3 Consistency of warning dialogues

This section presents the significant security warnings scenarios that users encountered, based on their participation in this user study. Not all the security warnings captured will be discussed in this section, but the most suitable and relevant will be presented accordingly, case by case. Security warnings with regards to file download were among the most popular experienced by the participants, as depicted in Figure 5.4. It may be noted that this shared similar headings, but was presented with different options, information and signal icons. These were the dialogues that were captured from the Internet Explorer browsers, as depicted in Figure 5.4 (A-D).

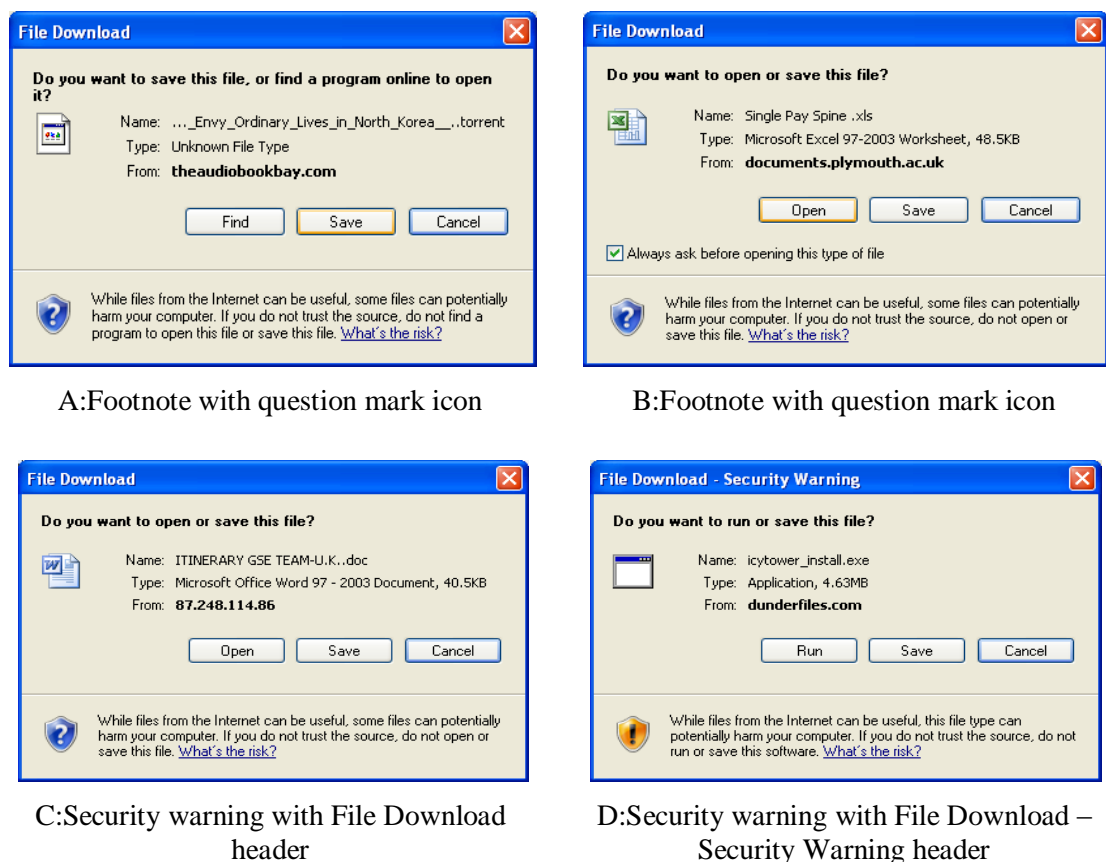


Figure 5.4: Consistency of security warnings

The Table 5.4 was determined to highlight the comparison based on the header title, options available, signal icons, signal words and technical terminology. More details of comparison had been discussed in a conference paper (refer to Appendix C).

Differences	Details of description
Header	All dialogue box using the same “File Download” header except on Figure 5.4-D using “File Download – Security Warning”.
Options available	<p>There were three types of options presented, as follows:</p> <ul style="list-style-type: none"> • Find, Save, Cancel and Close • Open, Save, Cancel and Close • Run, Save, Cancel and Close <p>The available answers were provided based on the given question to users. One interesting observation can be made from here, namely that even though the decision making process involved some potential risks (e.g. downloading malware), users still were allowed to proceed.</p>
Signal Icons	In terms of signal icon usage, it can be noted that 2 types of signal icons (i.e. question mark and warning) been used in the dialogues box (i.e. particularly in the footnote area). It may also be noted that there were four other types of icons been used based on the type of files detected (i.e. top left corner). For example, Figure 5.4 (B & C) were using Ms Excel and Word icon whilst the rest using unknown icon (i.e. white square background).
Signal Words	It can be noted that Figure 5.4-D used “security warning” signal word as compared to others as the file was detected to be .exe file.
Technical terminology	It can be noted that users were presented with different level of information upon detection the filename. Some available features used technical expressions to explain to users (i.e. name of the file, type and from). For instance, having presented with 87.248.114.86 URL was

Differences	Details of description
	not useful at all for end-users. They were unable to learn with regards to the decimal representation of URL without explaining what it meant and the purpose of having it in the first place.

Table 5.4: Comparison on the features of the warnings

In terms of the header title of the security warnings, only Figure 5.4-D used a different header name. The main reason that “Security Warning” terminology was used was that the file name extension was detected as .exe by the computer. This therefore posed a significant danger to users if they proceeded to execute the file (i.e. an executable file can easily propagate malware). On the other hand, for other types of security warnings, it was of an identifiable type such as Excel and word files, whilst Figure 5.4-A was derived from an unknown file type, but surprisingly, the header remained the same as Figure 5.4 (A & B).

From the perspective of the available options, both Microsoft files warnings (i.e. Excel and Word) offered three options (i.e. open, save and cancel): Figure 5.4-A with find, save and cancel and Figure 5.4-D with run, save and cancel. Where the computer was unable to detect the file extension or type, the “find” option was available to users, whereas if the file was an executable file, the run option was provided. For other types of file extension, as presented, the open option was used. From these layouts, the primary question posed to the users was a question with two options for the user to choose, such as the following:

“Do you want to save this file or find a program online to open it?”

Do you want to open or save this file?

Do you want to run or save this file?”

The security warnings presented required users to make a choice without further explaining the current contexts or problems that users faced. It would be troublesome, especially to the laymen or general population, to make such decisions without proper knowledge of the computer. It would meanwhile be interesting if all of these security warnings could be presented at the same time and then end-users would be able to share

their insights. In terms of the signal icons, two observations can be made. The first was the icon used in the content area, and the second was in the footnote area. With regards to the icon on content area, Figure 5.4 - B & C used specific word and an excel file icon. However, with Figure 5.4 – A & D, an unidentified program icon (white background) was used that was not understandable. On the other hand, a question mark and warning icon were used accordingly in the footnote area. Surprisingly, even though two different icons were used, the information presented in the footnote area still remained the same. Therefore, the users were not convinced the severity of the message (i.e. different icons had different impacts).

In terms of signal words, only Figure 5.4-D used security warning jargon to indicate the severity of the message (i.e. executable file .exe). For the rest of the security warnings, no specific signal word was utilised. Finally, with regard to the technical terminology presented on each warning, the author focused on the information provided in the footnote area. It may be noted that all four warnings shared the same information except for the signal icon used. The way that information on the footnote area was presumably simple and understandable except users had to click the link to get more details (i.e. will pops-up help dialogue). One critical observation may be made from this, namely that having a separated content and footnote area drew a distinction as to whether the information provided at the bottom was meant for the current problems (i.e. content area) or a separate document to explain general help functions. For users who were able to explore more details, they might understand the use of this link. Nevertheless, for the laymen, it is difficult for them to understand that the link provided actually helps function for them.

5.4.3.1 Warning dialogues case by case

In continuing from the previous section, this section further explains the outcomes of the user study. Eleven participants received warning dialogue boxes as depicted in Figure 5.4 (A-C) and on average they took five seconds to take any action (i.e. pressing any buttons or close). Nine out of eleven participants had chosen no and not sure with regards to the custom dialogue box they received. On the other hand, with regard to the security warning dialogue in Figure 5.4 – D, eight participants experienced it and it took on average twelve seconds to take any action (i.e. by pressing any button or close).

Three respondents did not encounter any problems and took less than three seconds to make up their minds, leaving seven respondents baffled and replying no and not sure. It may be speculated that a security warning with an executable file had more impact in terms of user decision processes, as users demonstrated that a longer period of time was needed.

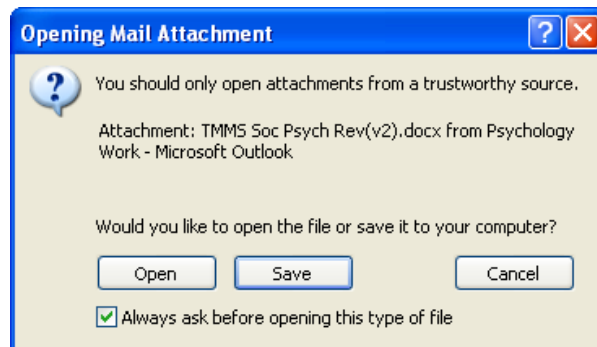


Figure 5.5: Security warning from Microsoft Outlook

On the other hand, four users had used Microsoft Outlook and received the same security dialogue with regards to opening a mail attachment, as depicted in Figure 5.5. It may be argued that the question mark icon was used in incorrect position as it supposed to be used as help entry point. A warning icon should be used instead because the main content of this dialogue box stated that “you should only open attachments from a trustworthy source”. Therefore, it warned users to take precautions before opening the file. Based on this scenario, conflict occurred with regards to the usage of question mark icon. Surprisingly on average, respondents took only three seconds to make a decision. It may also be noted that there no proper help or guidance in this security warning dialogue was provided that users could rely on.

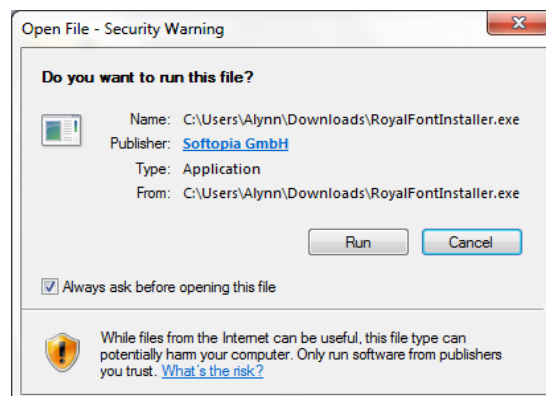


Figure 5.6: Security warning to opening file in Google Chrome

Based on Figure 5.6, six respondents experienced this type of security warning. Clearly, with the “warning” wording on the header and the warning icon in the footnote area, users were likely to be alerted to the severity of this warning dialogue box. Respondents took on average ten seconds to make a decision. This might be because users needed to obtain more information as to whether to proceed or not, as it involved some risks. Two out of six respondents claimed that the information was sufficient, whilst leaving the rest as no and not sure. Although the footnote area provided some useful information, it still used technical words to explain the context of the warning (i.e. publishers you trust). With regard to this warning, one observation can be made, namely that Google Chrome shared almost the same method of presenting security warnings as Microsoft in terms of presentation of warnings (i.e. content and footnote area). From the author’s assessment, in having a distinct separation between content and footnote area, users have to go down further to find the help link, instead of having it in the content area. Even though information was provided in the footnote area, users may ignore it because they have to read all the details.

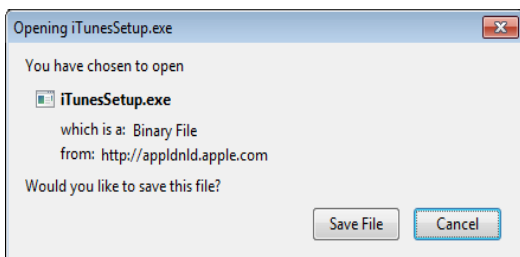


Figure 5.7: Security warning on downloading file from Mozilla Firefox

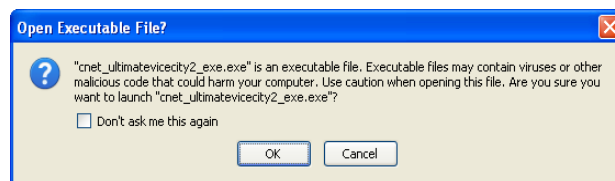


Figure 5.8: Security warning once users execute the save file on computer

On the other hand, seven users encountered security warning regarding the download file from Mozilla Firefox, as presented in Figure 5.7. This dialogue box looked very simple, insofar as no sufficient or useful information was given to user. Neither was there any proper signal cues used to indicate to users the severity of the current security message except the “program icon”. Respondents took approximately four seconds on average to take action in response to this security warning. It may be noted that users can only proceed by saving the file or cancelling the operation. Two of the seven respondents claimed that there were no further problems with regard to the information provided, whilst the rest decided on ‘no’ and ‘not sure’. Interestingly, only one respondent actually clicked the saved file from the warning dialogue and received another security warning as depicted in Figure 5.8. As this security warning was

derived from Mozilla Firefox, it clearly contradicted the Microsoft Guidelines. For instance, the header title was depicted in the form of a question, and a question mark icon was also used in the primary area of the warning. It may also be noted that more technical jargon was used within this dialogue (e.g. malicious, executable file and the file name) without proper guidance to help users.

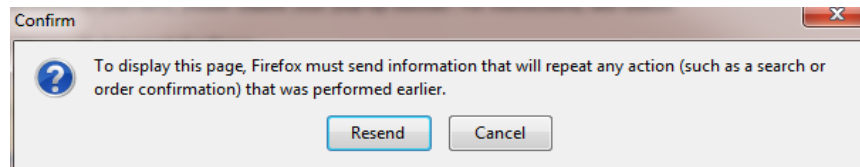


Figure 5.9: Security warning from Mozilla Firefox

A further example derived from Mozilla Firefox was experienced by four respondents on Figure 5.9. All of these respondents were not satisfied with the level of information provided in this dialogue box and took three seconds on average to make up their mind. The way information had been delivered was confusing. It appeared that the question mark icon was used to ask the user a question instead of providing a help entry point, as mentioned in the Microsoft Guidelines.

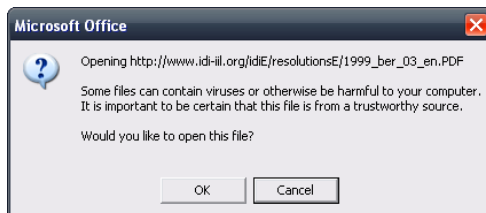


Figure 5.10: Security warning whilst opening link from Microsoft Office

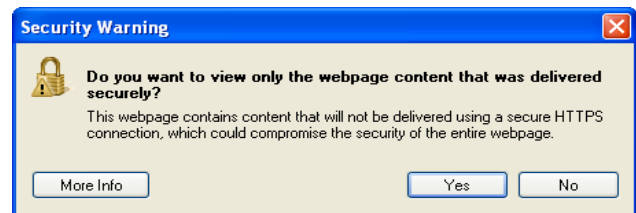


Figure 5.11: Security warning to view webpage

Three users experienced security warnings as portrayed in Figure 5.10. On average, they took three seconds to make a decision and all of them claimed they were not satisfied with the information provided. It may be noted that the information provided in the content area used technical terminology (i.e. “viruses” and “trustworthy source”) and simultaneously, no further guidance was provided. Surprisingly, users took a very short time to proceed with the decision. It may be noted that the real impact if users were to proceed to open the file was significantly dangerous, because it might have a direct impact on the whole computer system (i.e. presumably the file contains malware). On the other hand, three users took three seconds on average with regards to making a decision based on the security warnings on Figure 5.11. All of these users claimed that

there was insufficient information for them to understand the warning message. The information depicted in the content area on the dialogue box used some technical jargon (i.e. “HTTPS” that indicates as Hypertext Transfer Protocol Secure and “compromise the security”).

Figure 5.12 portrayed three different types of security warning, with the usage of complicated information. There were two respondents experienced on each of the dialogue, and on average, it took less than three seconds to make a decision. All of the users claimed no and not sure with regards to the custom dialogue box they received. It may be noted that the level of information depicted in the warnings was too technical, and would be unable to allow users to comprehend the current context: for instance, the usage of technical terminology such as protected mode, debug, error report, and unresponsive script. This might contribute to a quick decision process by the users (i.e. user might learn to visually dismiss the warning dialogue when they are not happy or in baffled with it).

Lay users experiencing this security warning were likely to be baffled by the decision making process. Furthermore, the look and feel of these warnings was complicated, with too much information being provided. Figure 5.12 – C for instance depicted with long scripts URL which was totally confusing. Users were unable to learn anything from this. In terms of help function with these warning, it may be noted there was a link provided, as presented on Figure 5.12 (A & B). Although the link was there, users demonstrated that it was still not sufficient (i.e. possibly with users attitude as demonstrated in previous findings where they neglected to read computer warning (Sunshine et al. 2009 and Bahr & Ford 2010), and implementation was too complicated for general users (Egelman et al. 2008 and Whitten & Tygar 1999) and they were unable to understand complex terminology (Zaaba et al. 2011, Bravo-Lillo et al. 2011 and Zaaba et al. 2012).

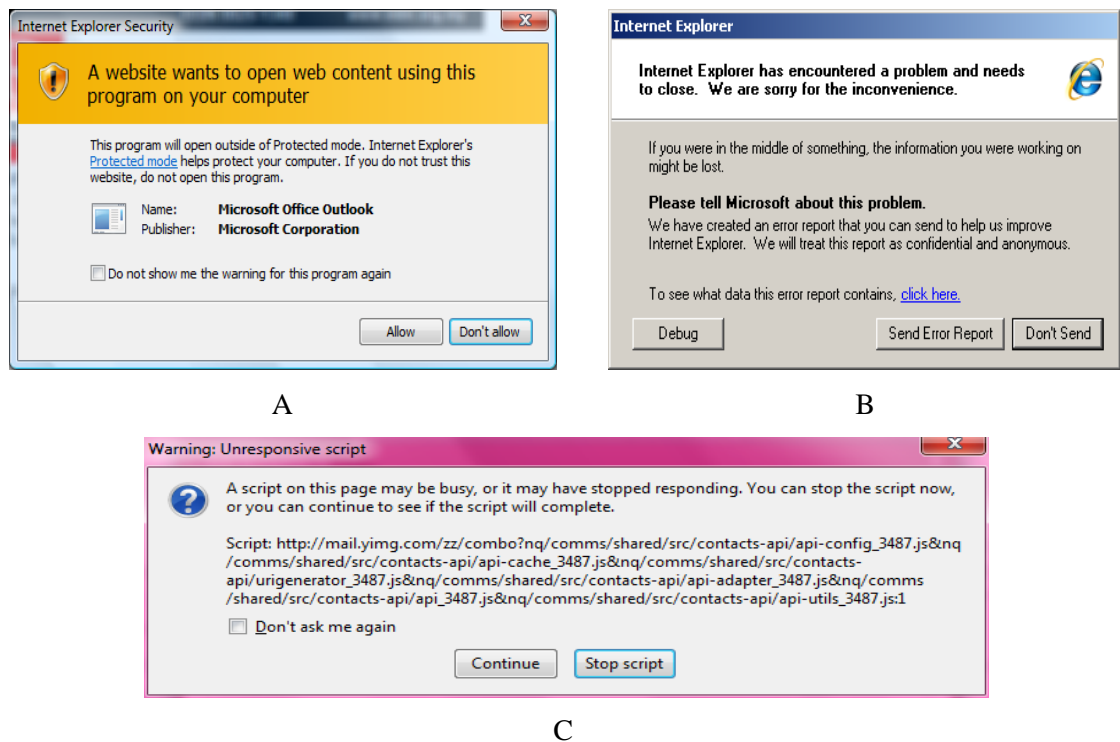


Figure 5.12: Security warnings with complicated information

5.5 Feedback comments

User feedback was derived from e-mails sent upon completion of the study, which is similar to the previous user study. It was not compulsory for users to send the feedback, but some did not hesitate to do so. Whilst not fully representative, below are some selected responses:

- i. "This software captures many security warnings and sometimes it interrupts my current task" (User 5).
- ii. "It would be useful if this software able to ask more different questions such as providing a textbox where users can give some comments or opinions" (User 13)
- iii. "I really like the idea sending the results using Dropbox. Normally I send any experiment results just by e-mail. Having used the software, I able to learn something new and beneficial" (User 25)

- iv. “The software is quite sensitive and able to detect most of dialogues box in my computer but it is very light program. I can understand the flow of the software easily especially with the help of guidance sheet” (User 28)
- v. “The overall information is mixed up between important and unimportant things. I cannot find any help unless I click the link. It is frustrating because too many details were provided” (User 30).
- vi. “There were information provided most of the time but sadly I do not understand it” (User 32)
- vii. “I am ok with some of the information provided. But it could be more meaningful if developers can explain it in a simple way” (User 35)

Based on these comments, some users demonstrated that they had problems in understanding the information regarding the security dialogue, and they suggested that it should be presented in a simple way, and with clarity (i.e. enough explanation on technical terminology, useful features to communicate the risk). In addition, users expressed their feelings with regard to the usage of Dropbox as a new tool (i.e. able to learn new thing). Hence, it may be suggested that this method helped to open a new dimension of data collection for future research.

5.6 Constraints

The software can only be used on three specific web browsers (i.e. Internet Explorer, Google Chrome and Mozilla Firefox) and on some other application that shared a similar class or application name. As mentioned before, all dialogue boxes that users received were treated as security warnings in the first place (i.e. due to the difficulty to classify one specific type of security warning dialogue and the general classification was based on class name or application name). With regard to the other dialogues box that were not impacted users’ decision (i.e. security and protection), this was not ignored directly, but assessed and selected if problems with security features existed (i.e. signal icons, signal words, technical terminology and help options).

5.7 Discussions

This chapter presented the results of users' understanding of whether enough information was available for them to understand the security dialogue that they encountered on a daily basis. As discussed earlier, this user study was a continuous study from Chapter 4. A software prototype was used as a tool to probe a sufficient level of information in a real time context. A custom dialogue box pops-up on every security warning that users' receive (i.e. after users took an action by pressing button or close).

This chapter also highlighted several noteworthy similar contributions from the aforementioned Chapter 4. It further revealed that technical terminology was widely used in dialogue box contexts, and that these might complicate users' understandings of the warnings. In some circumstances, signal icons and words was used in the wrong contexts. It can be noted that the help function was provided in some of the warnings, but that users still claimed the information was not enough (i.e. presumably the way information been delivered was not effective). The main reference for users to rely on during the incident was the help function. If these functions could not be comprehended and guided users in terms of decisions and explaining the current problems, it significantly impacted the wrongdoing decision.

Based on the findings from 36 respondents, it may be suggested that end-users still faced significant problem with level of information in security warnings they encountered. Evidences that had been gathered in this chapter (i.e. Table 5.3 and other presented scenarios) indicated the need for methods to guide users in terms of how information should be presented to help users understand the problem they encountered, the level of risk, the consequences of actions and any possible action to take. In most tasks, users took on average less than three seconds to view the security warnings they received, then they quickly made decision. The three seconds time frame was considered lower, and they possibly merely skimmed the overall warning message. These findings also support the results of Bahr and Ford (2010), namely that people quickly learnt to visually and cognitively dismiss the warning. This current study confirms the previous findings in Chapter 3 and 4 regarding the fact that not enough

information was provided for users to make decision with regards to the warning that impacted user's decision process, system and computer.

5.8 Focus and direction of study

The major concern that this thesis sought to highlight was the decisions that users had to make. If they made incorrect ones, this might jeopardise the security and protection of users' computers as a whole. Therefore, in order to reduce the risks of becoming a victim of computer menace resulting from wrong decision, security warnings must be improved accordingly.

Chapter 4 examined the comprehensibility of issues on information security in general, but particular attention was given to computer warnings in computer scenario study. From the results of the 564 respondents, it may be suggested that possible action needs to be taken to improve perception and usability, specifically with regard to the design of the current security warning interface. 54% of respondents claimed that not enough information had been presented with regard to the security dialogue. They (25% of responses) also claimed that they had difficulties with regards to the phishing warning, especially in relation to technical terminology, the nature of the event being described and the available choices.

Chapter 4 continued to investigate the wider evaluation of perceived security warnings contexts (i.e. dialogue box, notification, balloon, in place and banner) by giving flexibility to users to capture security warning based on their beliefs. Focus was given to the usage of signal icons, signal words, help function, technical terminology and available options (i.e. consistent with previous findings). The results from the 40 respondents indicated that they still experienced significant warning problems, especially in term of dialogue boxes and banners. It may be noted that none of the mean values in warning dialogue box (191 captured) was designated as "agree" or "strongly agree" with regards to all the questions presented on the questionnaire (i.e. to indicate users are satisfied with the implementation). Among the lowest mean values derived from question 9 "There are enough information in this security message" and question 3 "the message (and any associated help) provides sufficient details to understand what to do next" with 3.31 and 3.54 respectively. This result indicated consistent problems

occurring with regards to the level of information provided in warnings in the aforementioned Chapter 3.

Based on the two user studies (i.e. Chapter 3 and Chapter 4) conducted, issues of information became prominent. Crucially, if users are unable to understand the information provided (i.e. by using help facilities), the possible consequences can lead them to the wrong decision. Later, this may jeopardise the security and protection of users' computer. Therefore, Chapter 5 looked in particular at probing end-users within a real context, specifically with level of information provided in a real-time context. Based on the 36 responses, it may be noted that 52% of overall respondents of three web browsers had chosen "no" and "not sure" with regards to the information depicted in warnings to help them understand the message. Conflicts and inconsistencies with the guidelines still occur, especially concerning warnings from Microsoft products (i.e. signal icon, signal word, technical terminologies). It may also be revealed that users took less than three seconds to view the warnings they received (i.e. time was measured based on the difference between the dialogue appearing and the time of users' decision by pressing any button or closing). Based on these overall results, it may be indicated that users consistently have difficulties in assessing the information available on security warnings. A security warning dialogue box became the focal point of this thesis, based on the results presented in Chapter 4 (i.e. the most captured and identified as security warnings by responses).

This thesis has made use of all of the evidence from the literature reviews (Chapter 2), the initial examination on comprehensibility of information security issues (Chapter 3), investigation of the practicality of the warnings context (Chapter 4) and further appraisal of warnings in a real context (Chapter 5) to confirm that end-users experience significant difficulties with security warnings, especially in regards to the information provided for them. The problems encountered consistently were based on the empirical evidence presented in this thesis. Therefore, this thesis draws a line by proposing a new technique to present warnings in a better way (i.e. improve version). It is anticipated that the next study will utilise the information (i.e. via help function) so that users are able to comprehend the current contexts of the problem and able to guide them to make safe decisions with regard to the security and protection of users' computer systems.

An Automated Security Interface Adaptation (ASIA) is introduced as a novel framework to improve security warnings, as explained in detail in Chapter 6, and the results of the evaluation and validation of the framework are presented in Chapter 7.

5.9 Conclusions

In conclusion, Table 5.3 provides evidence that users generally face difficulties with regard to the information presented on every security warning dialogue they encounter on a daily basis. In terms of time usage, most users took less than three seconds to view the security warning and then quickly made a decision to get rid of the warnings given. It may be noted that the information provided still did not reveal what was happening, and guided them to make a better decision. It may also be noted that the usage of technical terminology still existed in the current security warnings. However, there was a guideline (i.e. Microsoft), with conflicts still happening especially in the usage of signal icon and signal words. In terms of consistency of warnings, it may be noted that there were some issues and confusion that could be highlighted (see conference paper in the Appendix E). Having assessed the evidence, it may be suggested that the presentation of the warnings dialogue may be significantly improved in order to convey the meaning of the message, and promoted secure manner decision for end-users.

CHAPTER 6

A Novel Architecture for Automated Security Interface Adaptation (ASIA)

6 A Novel Architecture for Automated Security Interface Adaptation (ASIA)

6.1 Introduction

Having considered the positive empirical evidence from user studies (Chapter 3 – Chapter 5), it is essential to design a novel architecture to provide end-users with improved security warnings. Automated Security Interface Adaptation (ASIA) has been introduced based on the rationale that end-users are still facing difficulties when encountering security warnings from web browsers as demonstrated in a series of user studies in Chapters 3 –5 (refer to the focus and direction of study section in Chapter 5). The results suggest that end-users consistently experienced significant problems in security warnings that they encountered especially in relation to the information that had been provided for them. A series of user studies had been conducted to explore, to investigate and to probe for further details about the initial problems in terms of users understanding of security warnings via a survey, user trials and real-time study in relation to security warning dialogues that end-users encountered on a daily basis. Some of the results obtained through the user studies based on different types of web-browsers, users background specifically education and types of security warnings are as the following:

- Web browsers- In Chapter 5, it was revealed that on average, 52% of respondents that encountered security warnings in three web browsers (i.e. Google Chrome, Mozilla Firefox and Internet Explorer) demonstrated that there was not enough information provided in the warning dialogues.
- Users background- It can be noted that the majority of these respondents reported that they were educated to a higher education or postgraduate level. In addition, they classified themselves as expert or advanced (44%), intermediate (53%) and beginner (3%) and all of them had been using the Internet for more than 6 years.

- **Warning Types-** In a more specific example, nineteen users experienced the “File Download” type of warnings (the most common warning that end-users encountered). Fourteen of them (nine females and five males) had chosen No and Not Sure with regards to the custom made security dialogue pops-up for them with five claiming to understand the warning information presented. On the other hand, six respondents (four females and two males) experienced the “Open File – Security Warning” type of warning. It can be revealed in two out of six respondents indicated the information was enough whilst leaving the others (four females) with no and not sure.

Therefore, this suggested that the participants were derived from people who had a good education background and were also demonstrating a level of familiarity in terms of using computers based on their reported skills and period of using the Internet. Even though they had experience using the Internet for more than six years, it can be noted that a significant amount of end-users (especially female participants) had chosen ‘not sure’ or ‘no’ in relation to the information provided in the warning dialogues. This reflects the need for further understanding on how the security warning dialogue would be able to improve by utilising the information that are expected to help and to navigate users in acting in a secure manner. By gathering all of the presented evidence in the previous chapters, this thesis proposes a new architecture to present warnings that will cater end-users need based on the information provided namely “Automated Security Interface Adaptation (ASIA)”.

6.2 Related Works

In order to improve the current circumstances with security warnings, several approaches have been discussed in Chapter 2. As most of the previous research focused on redesigning the warnings in order to improve the performance and understanding, a lack of focus had been given to developing an architecture or framework that would be useful as a guidance to improve warnings presentation. However, based on the work outlined previously, only one of these studies had produced an architecture or framework as a new way of interaction for end-users with security warnings dialogues. Therefore, this chapter builds on the findings to develop a novel architecture. The

comparison of several approaches had been discussed in Chapter 2 but in this chapter a specific comparison would focus on comparisons between the author's architecture and the ASD architecture. A more detailed comparison can be viewed in Appendix D accordingly. The author's work has similar underlying intention to improve security warnings as proposed by Keukelaere et al. (2009) with their Adaptive Security Dialogs (ASD). Interestingly, both studies highlighted the important aspects of usability of warnings to ensure the effectiveness, efficiency and users satisfaction

However, a parallel to be drawn from both studies is very clear where ASIA improve security warnings (i.e. utilising 50 respondents) by encouraging users to use the help function in order to generate security warnings based on their preferences on how warnings should be presented in the whole systems. In addition, it utilises the additional and useful functions (i.e. hover with quick information, risk level bar, guidance information and matching the signal cues with current context of warning) to ensure that warnings are presented in a presentable fashion. On the other hand, ASD (i.e. utilising 24 respondents) improves the warnings based on the risk that users are exposed to in five fixed different types of dialogue box (i.e. warn & continue multiple choice, security training, blank filling and clarification) where it matches the complexity of security warning dialogues with the risk associated based on the decision that has to be made by users. ASD adapted security dialogues to the risk that they had been exposed to. Thus, when users received security warnings from opening text file and when opening pdf file will be different (i.e. to change the common scenarios on security warnings). On the other hand, ASIA adapted security warning dialogues based on users' choice of preferences on what type of information should be presented in security warnings. Thus, based on their preferences, users will receive security warnings that cater to their needs rather than the default security warnings. The common ground from both is that both warnings improved in respect of presentation and usability of security warnings from the standard version. On the other hand both versions of warnings also worked differently in the sense that it caters to different goals.

Based on the detailed comparisons, ASIA can be viewed as an improvement on ASD in the sense that it offered users the information that they wish to see rather than the standard version of security warnings. A user would be able to view the security

warnings that satisfy their preferences and they can change their preferences at their convenience. In addition, ASIA utilised many new features especially with regard to how the help function can be presented to end-users so that it would provide more useful information. The new features (i.e. hover with quick information, risk level bar and signal cues matched with current context of warnings) had been introduced to make ASIA more intuitive and able to cater to end-user needs which had not been addressed clearly by previous studies. The elements of novelty lay in how ASIA uniquely caters to end-users needs on how security warnings dialogues can be presented in more understandable manner. As mentioned before, end-users are still experiencing significant problems with regards to the current security warnings that they encountered. Thus, ASIA is proposed to provide the possible solution with the new features and elements that convey the meaning of the message and promoted secure manner decision for end-users.

This research is generally heading to the same intention to improve warnings but utilising different method and aims. Understanding individual differences is useful to move towards better model of human decision making process (Böhme and Köpsell 2010). Then, it will lead to the creation of interface style that had significant effects on perceived ease of use and usefulness to use the system (Hasan & Ahmed 2007). The empirical evidence to support the author's proposes architecture is presented in Chapter 8. This chapter considers in particular the novel approach of ASIA, its process and the algorithm that will provide better warning comprehension, communicate the risks easily, and guide users to make a better decision in practice.

6.3 A novel architecture of security warnings

In order to provide a usable and presentable security warning, a novel architecture of Automated Security Interface Adaptation (ASIA) which can provide a new way of presenting warnings and information is proposed. This architecture generally focuses on the adaptation of every security warnings dialogue that can be identified by the system. Based on the user's preferences (i.e. selection from the preferences list), security warnings will be adapted and used in place of the standard version. Therefore,

in order for the warnings to adapt and feed the current warning implementation and be able to improve the interface of the dialogue box, ASIA's aims are as follows:

- i. To adapt the presentation of security warnings based on user preferences;
- ii. To increase users' comprehension of security warning dialogues before making a decision by enhancing the available help.
- iii. To improve the usability (i.e. effectiveness, efficiency and satisfaction) of security interactions;

These aims have been achieved by utilizing a combination of engines and processes within the novel architecture as illustrated in Figure 6.1. Generally, this architecture provides a basis to further understand how security warnings are presented to users. Users can make up their minds by choosing standard security warning (i.e. the default version) or security warning based on their preference (i.e. *Security Warning Enhancement*¹). At this stage, this architecture is set for dialogue box context of warnings rather than other contexts (i.e. in place, notification, balloon and banners). In essence, the entire procedure involves two process engines and databases, as follows:

- i. When the user encounters a warning dialogue (*standard warning*) for the first time, the *Program Executor* will communicate with the *Engine Manager* to check what are users' options (i.e. standard warning vs. *security warning enhancement*). The *Engine manager* will check the status from *User Support Data (USD)*. If nothing is detected, standard security warning is presented. Users will make decision as usual. Then the decisions will be saved in *Community Decision Data (CDD)* accordingly. After this, the *Engine Manager* presents Preferences lists (i.e. list of options to enhance security warning). A choice will be made and the preference will be saved in *User Support Data (USD)*. After this, the *Engine Manager* shows the *Dialogue options* that will require user to choose whether to receive the standard warning or the *security warning enhancement*. Simultaneously, there is a checkbox "Don't ask me again" where by default the system will present a warning based on users' preferences. Again, it will be saved in USD. It may be noted that before all

¹ The complete/full version of security warning is known as "**adapted warning**" where it comprised all elements that are required in computer warnings based on the preferences available.

processes and components within this stages is basically will be managed by the *Engine Manager*. This *Engine Manager* will be acting as manager to decide on the initial procedure before warning adaptation occurs.

- ii. If standard security warning in *Dialogue options* is chosen, then the decision will be saved in USD as instructed by the *Engine Manager*. Hence, every time users log on to the system, a *standard warning* will be defaulted. All users' decision on *standard warning* will be saved in CDD. Users will continue to use the *standard warning* until he/she decides to change.
- iii. In contrast, if *security warning enhancement* is chosen, the *Engine Manager* will first check the USD on users *Dialogues options* and *preferences list*. Once this has been confirmed, the *Engine Manager* will update the *Adaptation Engine*. The *Adaptation Engine* will pick up collective data from USD, DRD and CDD to generate warnings. First, however, the *Simplified security warning* is presented. Only if the "Help button" is clicked will all gathered data in the *Adaptation Engine* be used to present a *Security Warning Enhancement*. When a decision is made within the warning received, it will be saved accordingly in CDD, as managed by the *Adaptation Engine*.
- iv. However, if other options is clicked (e.g. run, cancel or close) only then *Simplified Security Warning* is shown. Then their decision will be saved in CDD.

(Note: It can be noted that all figures in this chapter are intended to be indicative data for illustration purpose. It also applies to all tables presented, as it is not intended to represent the formal database schema).

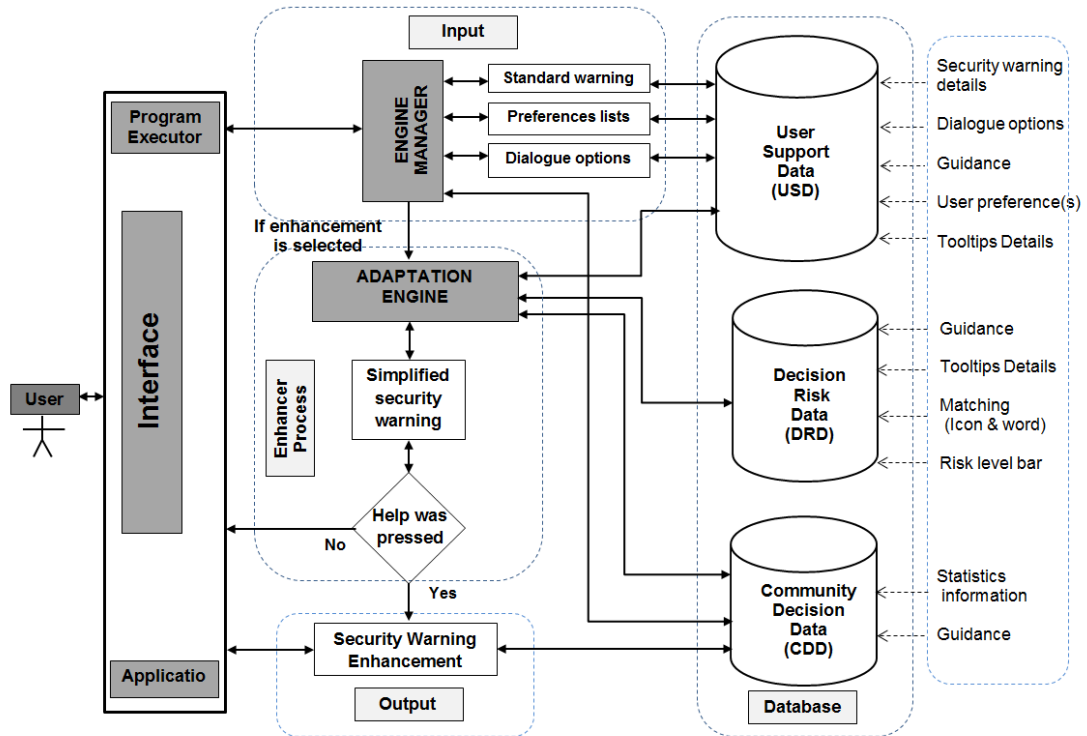


Figure 6.1: The architecture of Automated Security Warning Interface Adaptation (ASIA)

6.4 Process Algorithm

It may be noted that both the *Engine Manager* and the *Adaptation Engine* are fundamental elements that controls all other elements within the architecture presented. Therefore, this section will further explore the overall process algorithm, in order to better understand how *Security Warning Enhancement* is generated. Before this chapter proceeds, however, it is preferable to view the *Process Algorithm* based on the components involved, as presented in the ASIA architecture. The *Process Algorithm* explains how this architecture begins, the checking phases, and ends by presenting a *Security Warning Enhancement*, as illustrated in Figure 6.2. It has three checking phases as depicted in Table 6.1.

Checking Phases	Descriptions
1- Does Dialogue options contain data?	It checks whether the Dialogue option contains any users' decision.
2- Dialogue options decision	It checks user's decision as to their preference on standard security warning or <i>security warning enhancement</i> .
3- Was help button clicked?	It checks whether users' clicks help button to generate <i>Security Warning Enhancement</i> .

Table 6.1: Three phases of checking

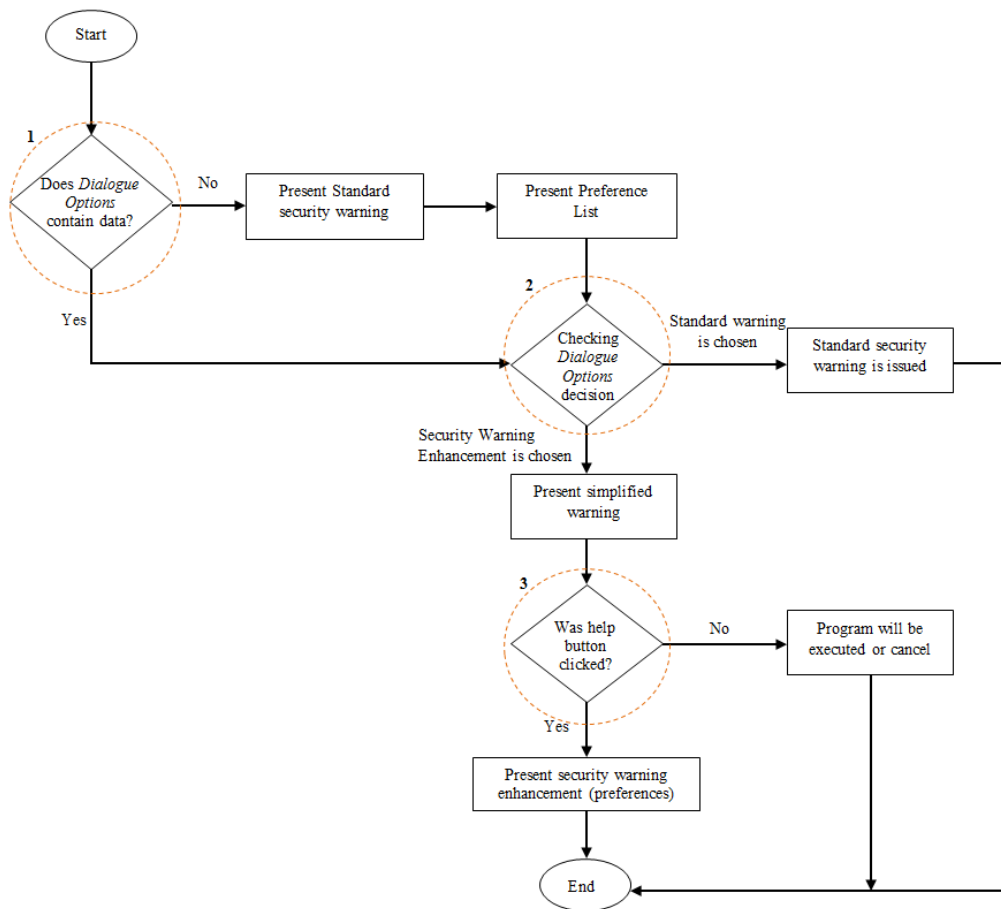


Figure 6.2: Overall Process Algorithm

These checking phases are essential in order for users to receive a *Security Warning Enhancement*. The *Process Algorithm* may be regarded as a straight forward process, where the focal point of this overall process is to encourage users to click help in order to receive *Security Warning Enhancement* and to get more information to help users with their decision making process. The first checking phase is part of *Engine Manager*

responsibilities to check whether there is data available (i.e. decision on *Dialogue Options*). If there is data available (i.e. *Dialogue Options* not equal to 0), then once again, the *Engine Manager* will check the main user's preference in *Dialogue Options* which is the second checking phase (i.e. whether standard warning or *security warning enhancement*). On the other hand, if no preference exists yet in the *Dialogue Options*, then a standard security warning is presented. Decisions will be made and recorded. Shortly after this, the *Preference List* dialogue is presented, and this offers the option to improve the security warning presentation layout. Users' decision on this preference will be recorded and will be used again in the *Adaptation Engine* later on. After this, a similar process will be repeated as if users have chosen their preference in the first checking phase.

As previously mentioned the second checking phase focuses on user's selection of receiving standard or *security warning enhancement*. Again, the *Engine Manager* will navigate to present standard security warning dialogue (i.e. if user decides with this version) or it will communicate directly with the *Adaptation Engine* when the user decides on the *security warning enhancement*. The *Adaptation Engine* will gather the collective information from the databases and present the *Simplified Security Warning* (i.e. details of the process is explained on the next section). At this stage, the third checking phase is conducted. This will verify whether the help button is clicked or not. If it is not clicked, then users are able to execute the program (e.g. if run is chosen) or terminate the process (e.g. when cancel or close button is chosen). On the other hand, if the help button is clicked, the *Adaptation Engine* will play a role in presenting a *Security Warning Enhancement*. The warning layout will be varied depend on users' decision with the *Preference List* in the early stage. The *Adaptation Engine* will ensure that users will receive the warning based on their needs. The full detail of each process involved includes the interaction with the database described in the next following sections.

6.5 General Functionality descriptions

Table 6.1 provides general insights into the entities involved in the ASIA architecture. Further details of the main processes and databases are explained within this chapter in further details.

	Functions	Descriptions
Input		This manages three types of dialogues (to/from <i>User Support Data</i>). It will check from the USD before deliver information to the <i>Adaptation Engine</i> . So every time a user logs on to the system, the <i>Engine Manager</i> will act as the first point of contact (i.e. to decide whether to show standard or <i>security warning enhancement</i>). <i>Security Warning Enhancement</i> only occurs if, and only if users click help button.
Enhancer Process	<i>Adaptation Engine</i>	This engine will receive instructions to generate security warning from the <i>Engine Manager</i> . It will gather all information from three databases (i.e. USD, DRD and CDD). Following this, the <i>Simplified Security Warning</i> will be presented to users. Security warnings are configured with some new features (i.e. tooltips details, about this file, Location link, signal warning/word and risk level bar).

	Functions	Descriptions
Output	<i>Security Warning Enhancement</i>	Users will only be presented with a <i>Security Warning Enhancement</i> if they click help button in the <i>Simplified Security Warning</i> . The warning is adapted and generated from the preferences that users had chosen before. All information with regards to the warning will be there in warning dialogues, albeit help is clicked (i.e. Name, Type, Location, Main statement and additional information based on users' preferences). The additional information will be embedded together on the same page instead of on a new dialogue box (i.e. standard dialogue box when help is clicked).
Databases	<i>User Support Data (USD)</i>	This database contains security warning details (i.e. class name, application name), dialogue options choice, Guidance information (i.e. what is the summary, what should I do and what else should I know), users preferences (based on the options) and tooltips details.
	<i>Decision Risk Data (DRD)</i>	This database contains Guidance information (i.e. what is the risk), the risk level bar information (i.e. indicator), matching signal icon and word and tooltips details
	<i>Community Decision Data(CDD)</i>	This database contains statistics information (i.e. users decision with particular type of warning dialogue), about this file (i.e. web key search information) and guidance information (i.e. what did others do).

	Functions	Descriptions
Others	Program Executor	Program executor will be defaulted in every web browser/ operating system from the software that user installed. It will communicate straight away with the <i>Engine Manager</i> to update the current status of users' options (i.e. standard vs. <i>security warning enhancement</i>).
	Interface	Graphical user interface that presents the security warning to users.
	Application	Any type of software or program that users use. Based on their action, clicking any button or link will generate a security warnings dialogue.
	User	Any particular person that uses a computer

Table 6.2: General description about the entities in ASIA architecture

6.6 Processing Engines and storage

The ASIA's architecture relies on two main engines, namely the *Engine Manager* and *Adaptation Manager*. A predominant role of these engines is to carry out various tasks such as to receive and to deliver data, verifying users' choice or preference and most importantly showing security warning to users (i.e. *Simplified Security Warning* and *Security Warning Enhancement*). On the other hand, three main databases involve within this architecture namely *User support Data (USD)*, *Decision Risk Data (DRD)* and *Community Decision Data (CDD)*. All of these databases are essential in storing useful information that has been gathered from process involves. Each of these engines and the databases will be fully discussed in the following sections.

6.6.1 Engine Manager

The *Engine Manager* is classified as part of the input process. The main function of the *Engine Manager* is to become the first point of contact after the user interacts with the security warning, as depicted in Figure 6.3. The main component within this engine is

known as the *Engine Manager Controller*. The *Program Executor* will verify with the *Engine Manager Controller* first to check the availability of data in dialogue option (i.e. whether to receive the standard or *security warning enhancement*) on specific type of warning from the *User Support Data (USD)*. If there is nothing detected in the *Dialogue Options* from the database, the user will be presented with a standard security warning (i.e. where ASIA able to interact and handle warning from operating system and web browsers). Standard security warning here can refer to a security warning dialogue box that users normally receive on a daily basis whilst using the computer. However, the scope of standard warnings in this architecture focuses on the warnings involved, with at least two options for users to choose, and it involves the user in making decisions that might affect security and protection (i.e. as it require users to pay more attention on the decision making process).

It may be noted that on every standard security warnings presented to users, it will comes in many different layout as it is associated with the browser and operating system where the warning comes from on the first place (i.e. it will cater all forms of warnings from different browsers and operating system). For instance, Internet Explorer, Mozilla Firefox and Safari use different mechanisms to present warnings. Therefore, from the bigger perspective, the security warning identification process can be a difficult task and tedious job because of the system need to identify each of the security warnings. However, as this process is conducted in the background, users will not have much problem in handling this operation.

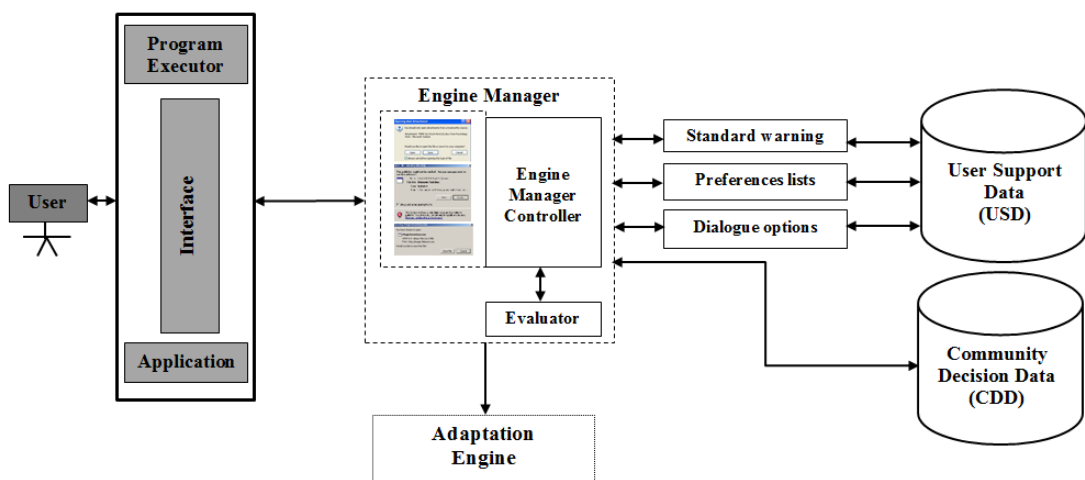


Figure 6.3: Engine Manager

ID	Dialogue	Warning class	Application Name	Header Name	Group ID	Option 1	Option 2	Option 3	Option 4	Option 5	Option 6
1	Yes	#32770	Chrome.exe	Open File - Security warning	1a	1	1	-	1	1	-
2	No	#32770	Firefox.exe	Open File - Security warning	1b	-	1	1	1	-	-
3	No	#32770	explorer.exe	Open File - Security warning	1c	-	1	-	1	1	-
4	No	#32770	Chrome.exe	Open File - Security warning	1d	-	1	1	-	1	-

Table 6.3: Record in USD

The *Engine Manager Controller* has the ability to identify the warning class, application name and the header name of warning. By using this information, warning can be differentiating from where it derives and the *Engine Manager* in general uses it to generate a unique Group ID. This is to ensure that each warning is unique from one another. This information is essential in order to decide whether every security warning dialogue received can be categorised and recorded in USD. Therefore, the *Evaluator* component will be referred to by the *Engine Manager Controller*. The *Evaluator* will again make use of the information (i.e. warning class, application name and header name of warning). In addition, the *Evaluator* also has the capability to detect how many options exist in each warning that been presented. If all requirements are satisfied, the *Engine Manager Controller* saves all information after user been presented with the standard security warning. Users make their decision as usual in the warnings they receive (e.g. by pressing run or cancel). Every user's decision will be recorded and saved in *Community Decision Data (CDD)* accordingly as depicted in Table 6.3. Simultaneously, the *Engine Manager* via its controller updated the Group ID information on *Community Decision Data (CDD)*. This group ID will be used later on in providing statistical information in the *Enhancer Process* (i.e. explained on the next section). In contrast, if the *Evaluator* is not satisfied with all of the requirements, then data will not be categorised and recorded. Hence, standard security warnings will be used by default.

After this, one dialogue box namely *Preference List* been presented to users. *Preference List* utilised the available options (i.e. list of choice to improve warning) for users to choose. These options are presented in the form of a checkbox, so that users are able to click any options that can satisfy their needs. In this context, the lists are derived from the results of author's user studies (i.e. method to improve security warning from end-users experienced dealing with computer warnings). Therefore, the lists can be updated from time to time to suit the needs and requirement. The following are examples of six options that can be used as the *Preference Lists* for user to choose:

Option 1: More information regarding the reason for the dialogue

Option 2: More descriptive information to guide me on what to do

Options 3: Recommendations based on other users' actions in response to this dialogue

Option 4: Consistent/explicit/clear usage of signal icons and words

Option 5: Information presented in clear sections in the form of question/answer

Option 6: Using non-technical language to describe the problem

Based on the decision on the *Preference Lists*, users are likely to be presented with various version of *Security Warning Enhancement*. Further details of these combinations are explained in Chapter 7. Therefore, once users have decided on their *Preference List*, the *Engine Manager Controller* will then present a dialogue option to user once again (i.e. by asking users preference on receiving the standard or *security warning enhancement*). It may be noted that this dialogue option contains a checkbox with an option "Don't ask me again" where it means by default the system will automatically present warning based on users' preference. This decision or preference will then be updated in USD.

In contrast, if users decide to receive standard security warnings when the *Engine Manager Controller* present to them with Dialogue Options, then the *Engine Manager Controller* will update the CDD with users' decisions. Thus, every time users wish to log in their system, a standard warning will be automatically defaulted for them. They will continue to use this warning until they decide to change it. If users decide to change this option, they will need to change the option in the settings provided in their computer. From an overall perspective, the *Engine Manager* plays a vital role as a mediator to interact between another processes and databases. For instance, from Table 6.3, all data in the record will be sorted accordingly based on the interaction manage by the *Engine Manager*. This data will be used when the *Engine Manager* starts to interact with the *Adaptation Engine* provided when users choose the *security warning enhancement* in *Dialogue Options* (i.e. *Dialogue Options* = Yes).

6.6.2 Adaptation Engine

The *Adaptation Engine* is the core process involved in this architecture. It consists of three main components namely *Receiver*, *Negotiator + Updater* and *Internet Search*. This engine is classified as the *Enhancer Process* where the adaptation of security warning initially begins. It will have the direct interaction from the *Engine Manager*. When users decide to choose *security warning enhancement* in the *Engine Manager* processes, the *Engine Manager Controller* will first verify with UDD with regards to users selection on *Dialogues Options* and *Preference Lists*. Once this is confirmed (i.e. example on Table 6.3- ID = 1, *Dialogue Options* = Yes and *Preference List* with some selections), the *Engine Manager Controller* initiates the interaction with the *Adaptation Engine*, as illustrated in Figure 6.4.

When the *Engine Manager* makes its first contact with *Adaptation Engine*, the *Receiver* component will receive the instruction (i.e. the security warning enhancement is selected in *Options Dialogue*) and it will notify the *Negotiator + Updater*. At this stage, *Negotiator + Updater* verify the information again with USD (i.e. *Dialogue Options* for this particular warning is equivalent to “Yes”). If it is satisfied, the *Adaptation Engine* (i.e. via *Negotiator + Updater*) will generate the *Simplified Security Warning*. This *Simplified Security Warning* is generated based on the information gathering by the *Negotiator + Updater*. It may be noted that the *Simplified Security Warning* is created to imitate the standard warning layout or presentation. In contrast, some additional information is added to ensure that warning message can be delivered in a simple and better way. The imitation of standard security warning here can be defined so as to make use some available features from the standard security warning to be used again in the *Simplified Security Warning*. This is to ensure that users will consistently able to familiarise with the new warning been presented to them as it share similar style and function in standard security warning. Therefore, users are likely to be able to correlate their previous mental model (i.e. based on the exposure they already have) with the additional features of the *security warning enhancement*.

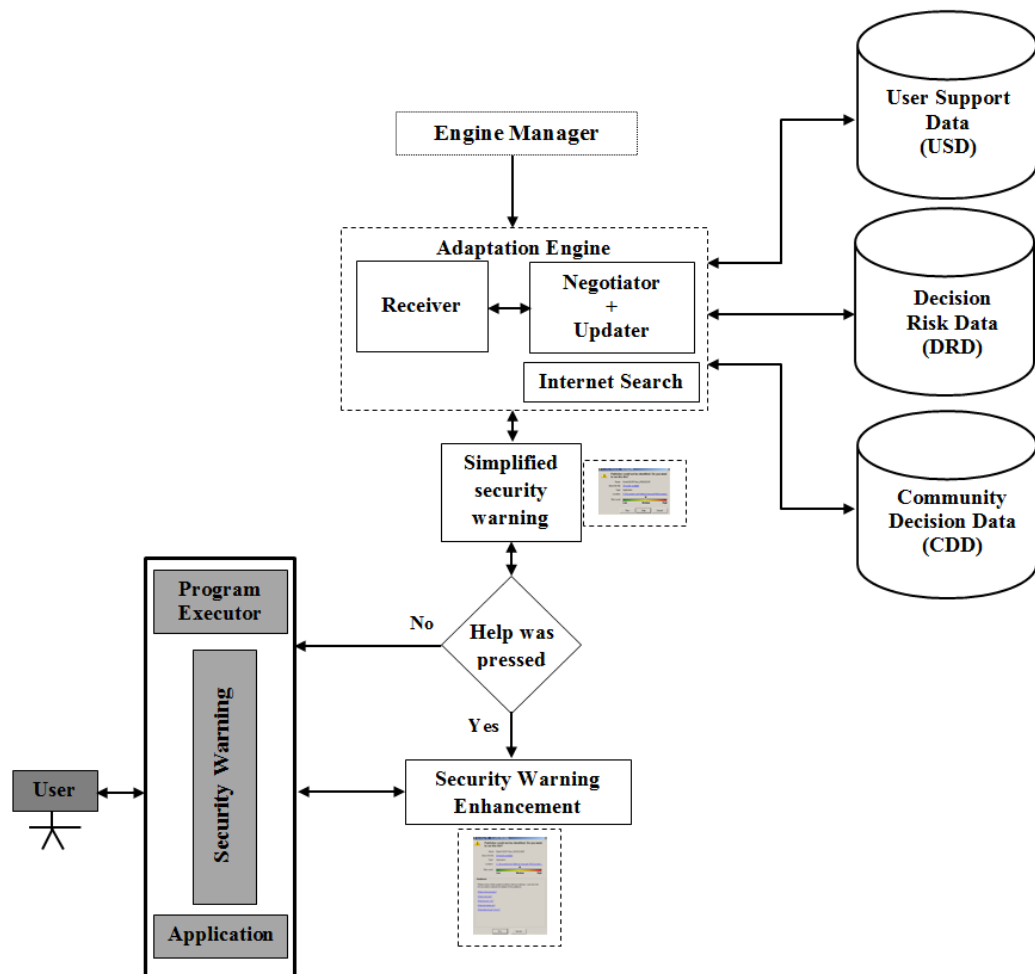


Figure 6.4: Adaptation Engine

The sources of information to generate the *Simplified Security Warning* are derived from Table 6.4 to Table 6.7.

The *Simplified Security Warning* layout made used some useful information from the *standard warning* (e.g. name, type and location). However, some improvements are made to add more functions, such as concerning this file, risk level bar, appropriate usage of signal icon/word and hovers elements. About this file is a function that is generated by the *Internet Search* process in the *Adaptation Engine*. It will automatically get more information with regard to the warning dialogue that user encounters. By referring to the file name of the warning, it will automatically browsing more information about it and provides useful search terms for users. This means that when users click this link, they will be navigated to Google page that contains straight away search term related to the file involves. Thus, users will be able to see straight away anything involves to the file name (e.g. discussion about the filename, comments

from the users and review about the file). Instead, users manually type data to get more information, this function simplified users' task. However, it may be noted that users still need to make their own judgement with the information presented to them. On the other hand, the risk level bar provides user with the risk level information to communicate the risk level clearly. Therefore, it gives users some early indication with regards to the severity level of risk that users currently experience. These features describe the current severity of risk involved to comprehend the users (i.e. by describing the wordings and colour schemes involve).

ID	Tooltips details 1
1	Name_of_the_file
2	File_type
3	Location_of_the_file
4	Information_about_this_file
:	:

Table 6.4: Tooltips detail from USD

ID	Tooltips details 2
1	Low_information
2	Medium_information
3	High_information
4	Risk_level_bar_information
:	:

Table 6.5: Tooltips detail from DRD

ID	Matching icon & word
1	Warning_Icon
2	Error_Icon
:	:

Table 6.6 : Matching icon and word from DRD

ID	Risk Level Bar
1	Indicator_ &_ colour scheme
:	:
:	:

Table 6.7: Risk level bar from DRD

When users hover to the available features on the simplified warning (i.e. name, about this file, type, location, risk level bar and risk information), they will be provided with quick information about the meaning of these function (i.e. derived from Table 6.4, Table 6.5 and Table 6.6). Each of these pieces of information will be complied by the *Negotiator + Updater* from the available record so that *Simplified Security Warning* can be presented in accordance. Simultaneously, this warning seeks to match the current context of message by matching the usage of signal icon and words (i.e. derived from Table 6.6) which do not always occur in the *standard warning*. Based on the author's previous user study, it can be revealed that conflicts or mismatched on the usage of signal icons and signal words happened (Zaaba et al. 2011 and Zaaba et al. 2012). Hence, this proposed architecture tries to improve the condition. When users receive the simplified warning, they will have to make decision by pressing the available option (i.e. by choosing one of these options: run, help or cancel). If they press run, the program will be executed and users can proceed to the next stage. A similar thing happens when users decide to cancel; the operation will be cancelled and the cancellation will be notified to users.

In contrast, the focal point of this operation is when users press the help button. ASIA architecture works differently and uniquely because it encourages users to click help upon receiving security warning. This help function can be associated with more information that embedded in the warning (i.e. instead of presenting with another help dialogue box separately). This method of implementation combines some other user help techniques which lead to usable security (Herzog & Shahmehri 2007). It also made used questions and answered style interaction as proposed by Baecker et al. (1991) to produce an effective warning based on what users normally ponders in their mind upon completing their task. When the help button is pressed, the *Adaptation Engine* via *Negotiator + Updater* plays it roles to update USD as illustrated in Table 6.8. By

using this information, the *Negotiator + Updater* sort the relevant information based on the combination that users choose earlier. For instance, if a user decides to click all available option, his/her preference can be classified as combination 1 (i.e. by the assumption this is the complete version of security warning that contains all information). It may be noted that based on users decision in the earlier stage (i.e. by choosing *Preference Lists* checkbox), it will generate various type of warning outcomes. This is to ensure that only the information that is needed by users will be presented. Details of assessment are discussed in Chapter 7.

ID	User Preference
1	Combination_1
2	Combination_2
3	Combination_3
4	Combination_4
5	Combination_5
6	Combination_6
:	:

Table 6.8: Combination of user preference based on List preferences

ID	Guidance 1
1	Summary
2	Guidance_information
3	Investigative_information
:	:

Table 6.9: Details on guidance area (USD)

ID	Guidance 2
1	Risk_level_information
:	:
:	:

Table 6.10: Details on guidance area (DRD)

ID	Guidance 3
1	History_information
:	:
:	:

Table 6.11: History information based on what others have done (CDD)

ID	Statistics details	1a	1b	1c	1d
1	Run_counter	-	1	1	1
2	Cancel_counter	-	-	-	-
3	More_info_counter	1	-	-	-
:	:	:	:	:	:

Table 6.12: Statistics information based on the type of warning message

After it is confirmed with the selected combination, it will gather all other information (i.e. to be embedded in the warning) which derives from Table 6.4 to Table 6.12. Again a similar process as mentioned in the creation of *Simplified Security Warning* will be repeated on *Security Warning Enhancement* (i.e. combination 1 – complete version of security warning). The additional information as added elements on the *Security Warning Enhancement* (i.e. in the guidance area) is derived from Table 6.9 (details about the summary, guidance and investigative information), Table 6.10 (risk level information) and Table 6.11 (history information regarding what other people do which are based from Table 6.12). After the gathering process is completed, user is then been presented with the *Security Warning Enhancement* (e.g. combination 1). All of this information are presented to comprehend users with new details information (i.e. to guide users to utilise the available guidance information where they able to embrace secure manner decision action, to explain the technical terminology within current context of the message and most importantly to encourage users to use help option where it adapt new method of presenting warning). Once he/she makes a decision with regard to the *Security Warning Enhancement*, the decision will be updated in the *Community Decision Data* (i.e. where a new warning record will be created) as illustrated in Table 6.13. The value “1” in column “Y” meaning that one user had chosen run as his/ her decision where ID- 1A can be referred to the standard security warning that has been replaced with *Security Warning Enhancement* (i.e. which has

been group in ID 2 as Com 1 or initially combination 1). Later, this statistics information will be used again in statistical presentation (pie chart) that will be presented depend on the *Preference Lists* that users choose.

ID	ID 2	Statistics details 2	Y	N
1A	Com1	Run_counter	1	-
		Cancel_counter	-	-
:	:	:	-	-

Table 6.13: Statistics information based on *Security Warning Enhancement* (users' preferences)

6.6.3 Databases

There are three main databases involved in this architecture, namely *User Support Data (USD)*, *Decision Risk Data (DRD)* and *Community Decision Data (CDD)*. In the early section, it has been notified that all figures in this chapter are intended to be indicative data for illustration purposes, and it also applies to all tables presented as it is not intended to represent the formal database schema. These three main databases contain different types of information where the Adaptation Manager will become the mediator to decide which information to select and use before warning can be presented to users. From Figure 6.1, the *Engine Manager* interacts with *User Support Data (USD)* and *Community Decision Data (CDD)* whilst the *Adaptation Engine* communicates with all databases.

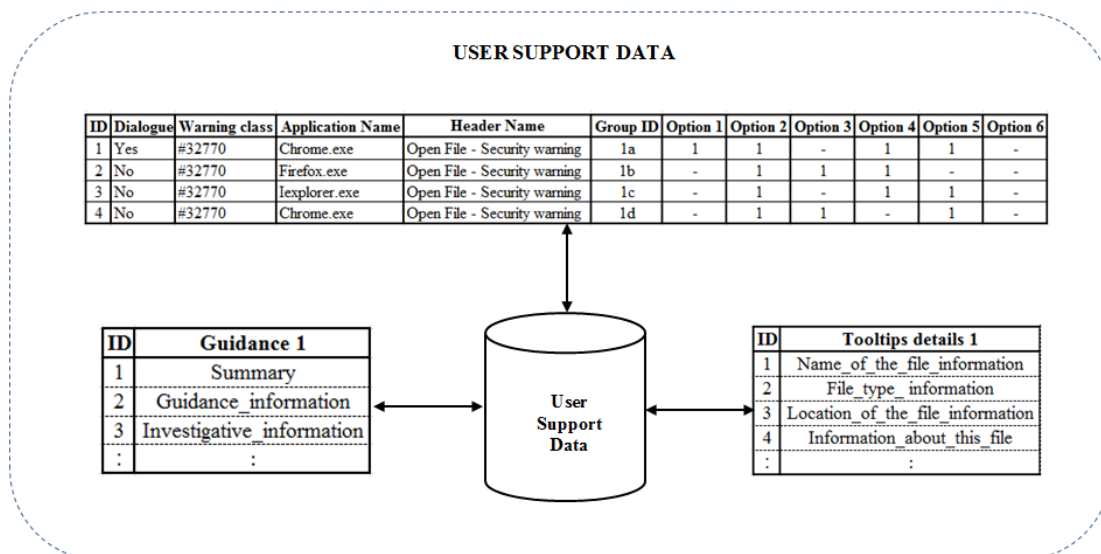


Figure 6.5: Table representation in User Support Data (USD)

Figure 6.5 portrays three tables representations involved in USD. It can be noted that this database consists of most of the record (i.e. security warning classification related such as warning class, application name, header name and Group ID). In addition, users decision with regards to the *Preference List* and *Dialogue Options* are recorded in the same table. Guidance 1 consists of records that will be appeared in *Security Warning Enhancement* (i.e. guidance area) whilst Tooltips details 1 would be used in the *Simplified Security Warning* and *Security Warning Enhancement*. Therefore, at this stage, the *Engine Manager* manages all of these components accordingly before it can be delivered to the *Adaptation Engine*, in order to generate warning.

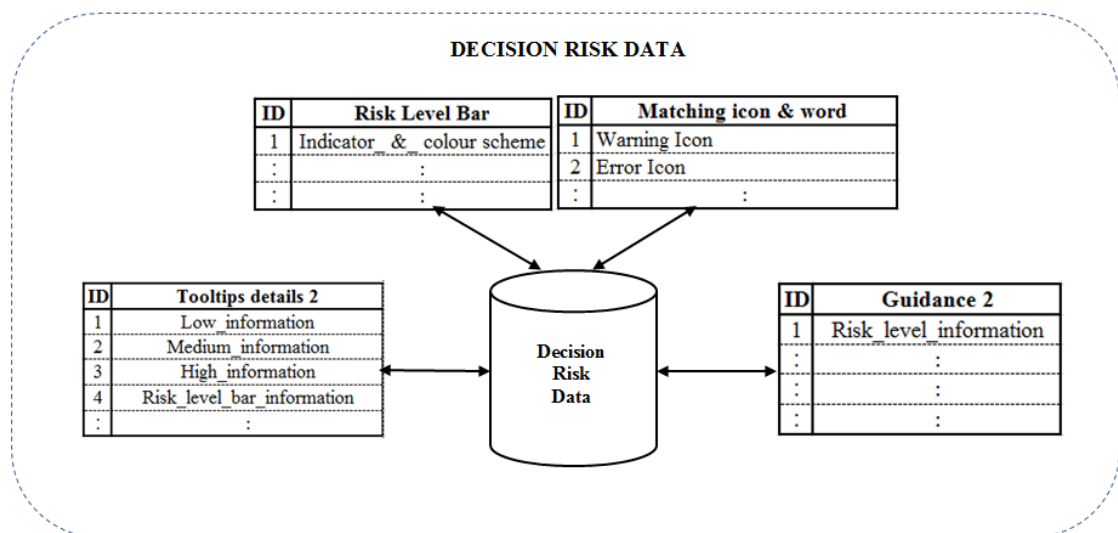


Figure 6.6: Tables representation in Decision Risk Data (DRD)

From the view of *Decision Risk Data (DRD)*, four main table representations are depicted in Figure 6.6. When the risk level bar is used, it will be associated with Tooltips details where information about risk will be presented. For instance, when one particular user hovers to words in the warning such as low, medium and high, he/she will be presented with quick information about the meaning of those words. On the other hand, this table also contains information on matching the signal icon and word based on the current context of warning message. This improvement is suggested based on previous author's user studies, where a mismatched usage of signal cues occurs even when the guideline are used. Providing the correct usage of signal cues is essential so that users able to incorporate their understanding as part of their mental model process.

The last table representation can be referred to Guidance 2 table where it provides the risk level information on the guidance area. Therefore, it is clear that *Decision Risk Data (DRD)* will be used to provide details of information that specifically caters for the risk that involves (i.e. in order indicating the severity on the current usage of warning message).

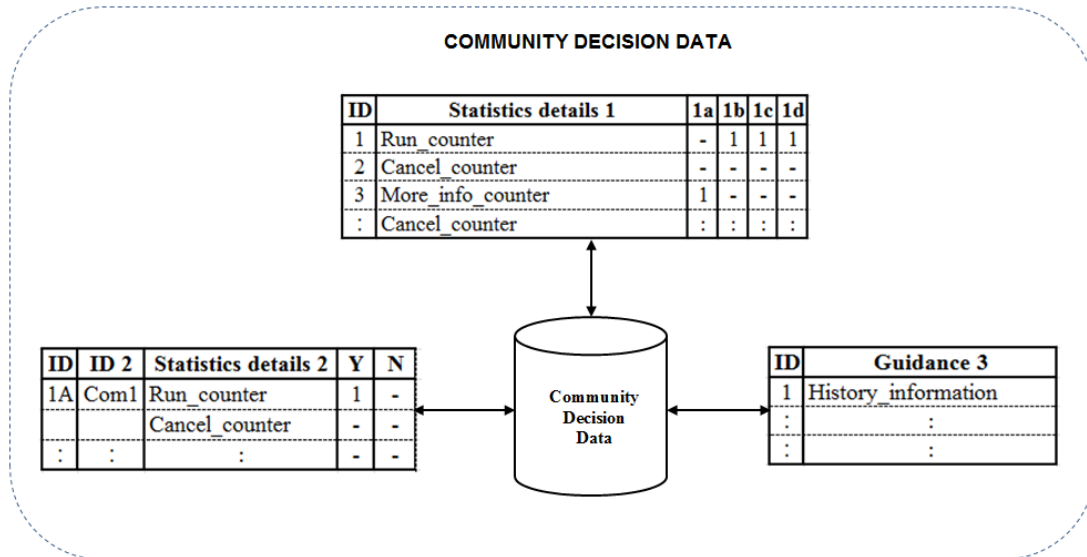


Figure 6.7: Tables representation in Community Decision Data

The final database (i.e. *Community Decision Data*) involves three main table representations. Statistics details 1 consist of users' decision upon receiving standard security warning via the *Engine Manager* processes. The warning will be automatically classified and group accordingly (e.g. 1a, 1b, 1c and 1d). In addition, Statistics details 2 shares similar function but it will focus on users' decision upon receiving *Security Warning Enhancement* (i.e. Com1) that also can be associated with the standard security warning (i.e. 1A) that users should receive. On the other hand, Guidance 3 contains history information that will be used in the guidance area in the warning presentation. *Community Decision Data* can be viewed to provide information from the external source, where it utilises decisions as to what other people do upon receiving such warnings. This will provide useful input to improve security warnings, where users can rely on other peoples' views as to what possible action to take (i.e. social navigation).

6.7 Conclusions

In this chapter, ASIA architecture provides simple, transparent and encouraging safety behaviour for users when faced with security warning dialogues. This architecture has been designed to accommodate end-users' needs on warning messages and the components and functionalities of the architecture are described in detail. By providing end-users with security warning based on their preferences, it can generate open a new dimension on how warning design can be improved. Based on the previous user studies that had been conducted, it providing useful input to this architecture where method to improve warnings can be used (i.e. *Preference List*). In addition, from time to time developers can further evaluate the suitability of the *Preference List* where it can be added at any time based on users' needs. By utilising all the components using two major engines (i.e. the *Engine Manager* and *Adaptation Engine*), users able to view warnings that is usable, understandable and promote secure manner action before one particular decision being made. The warning presentation has been improved when users are presented with the *Simplified Security Warning* and when help button is clicked *Security Warning Enhancement* is generated. In this context, warnings and useful information (i.e. additional information) are embedded together in the same dialogue, rather than presented separately as a help dialogue box.

In order to achieve the highest level of satisfaction, the proposed architecture used useful information from three databases (i.e. *User Support Data (USD)*, *Decision Risk Data (DRD)* and *Community Decision Data (CDD)*). After all the information has been gathered and compiled (e.g. Guidance information, tooltips details, matching signal cues, risk level bar and statistical information) warning design can be improved to suit current contexts of warning in a way user can understand the meaning of the message and there are useful information as a guidance provided for them. Therefore, a novel ASIA architecture is a robust framework that is able to achieve its aims. In Chapter 7, Automated Security Interface Adaptation (ASIA) will be evaluated and validated in prototype software.

CHAPTER 7

Evaluation and Validation of the Automated Security Interface Adaptation (ASIA)

7 Evaluation and Validation of the Automated Security Interface Adaptation (ASIA) prototype

7.1 Introduction

Based on the evidence gathered from the previous user study presented in Chapters 2 to 5, the Automated Security Interface Adaptation (ASIA) was developed to enhance current security warnings dialogue (describe in Chapter 6). This chapter describes the evaluation and validation of the proposed framework via the implementation of a prototype system and its use within a final experimental study.

Many techniques have been demonstrated to improve security warnings (e.g. matching complexity of risks, security automation, rewarded security behaviour and mental model). However, none of these techniques have been adopted by developers. Current security warning implementations do not provide enough information to inform users and guide them in making secure decision. Although useful features have been provided (i.e. signal words, icons, computer terminologies, colours and useful help functions) many users were still confused especially as some of these features conflicted with the guidelines provided. For example, when the help button is pressed, a new dialogue box will often pop up. This can distract users from the current task. In addition, excess wording or information was provided in the help dialogue, which made the decision making process more complicated. Users often had to read all the information and sometimes had to search for more (i.e. answers provided were not users oriented).

These limitations meant that, users quickly learnt to ignore the help function and made a decision based on what they believed to be safe. The main concern here is that if the decision making is not suitably informed. Users might compromise their own security leaving their computer vulnerable to attack. In reality, ASIA has been presented as a prototype rather than a full implementation. However the results as presented in this chapter are convincing. In the future, ASIA could be implemented as a full system. There are many challenges to implementing ASIA with more research needed to see how ASIA can integrate with various types of web browsers and operating systems. A high level of understanding and technical ability is required so that ASIA can be put in

place without any conflicts with the computer systems (i.e. different platforms). However, it should be possible to improve the current security warnings if there is collaboration among the vendors of web browsers and operating. For instance, developers from Microsoft, Google and Apple can use this architecture as the basis for further assessment and evaluation on how security warnings can be implemented in their products. More user studies can be conducted to assess end-users' understanding and needs, especially in real-time scenarios, which might be useful to provide solid evidence. This will not be an easy process but many considerations must be put in place in relation to satisfying the end-users' needs and without jeopardising the security and protection of the computer. This final user study (study 4) utilised prototype software which was developed with the assumption of being able to present a method to improve security warnings based on user preferences and to be able to fulfil the aims of ASIA, as presented in Chapter 6.

7.2 Methodology

User study 4 is based upon a prototype implementation of the ASIA architecture. The participants were recruited predominantly from among Plymouth University staff and students. This experiment was conducted on a one-to-one basis via a software prototype, combined with questionnaires and interviews (all conversations were recorded for later analysis).

Before the session began, participants were given a brief by the principal investigator about their right to withdraw at any stage of this experiment. Then, the users were required to give their consent before they were briefed on the overall flow of the experiment (i.e. role-based and contextual scenarios) and that they were allowed to ask questions at any stage. This method has been widely used in warning research in order to provide context whilst examining their comprehension and understanding of computer warnings (Egelman et al. 2007, Brustoloni & Villamarín-Salomón_2007, Keukelaere et al. 2009, Bravo-Lillo et al. 2011 and Raja et al. 2011).

Two investigators read the recorded transcript independently, identified the common ideas and later coded and classified the results. Based on the coding, the principal investigator used the results as the final answers with regard to user feedback on the

interview session. This technique has previously been used in order to increase the validity of similar studies (Raja et al. 2010 and Bravo-Lillo et al. 2011b).

7.3 Study Design

Participants were registered on a “first come first served” basis. Therefore, only the first 50 participants were selected (i.e. they received e-mail notification stated their allocation date, time and location accordingly). ASIA was developed using Microsoft Visual Studio Professional (2010), specifically using Visual Basic. In this prototype software, users were required to adopt the role of a management trainee in IT Company, dealing with technical and non-technical tasks on a daily basis. Their responsibilities involved dealing with the installation of software products, research and development, managing inventories, writing reports, managing the company’s e-mail and other task as directed. Whilst dealing with these tasks, they encountered security warnings (simulated via seven tasks) and they were required to make at least one preference regarding features or elements that should be depicted in the warning message. The use of the prototype software can be divided into three main phases:

i. Capturing demographics

This involved nine questions related to user’s background, skills, preferences and knowledge.

ii. Practical tasks

This involved a series of seven computer security warning dialogue boxes in different scenarios and web browsers (i.e. Internet Explorer, Google Chrome and Mozilla Firefox). In each task, users were required to choose at least one preference for the given question. Task 7 was repeated after this (presenting an enhancement of previous security warnings based on user preference).

iii. Post-trial questionnaires and interviews

Users were told that they would receive three security warnings. Firstly, users were presented with the standard security warning (Task 7) followed by a questionnaire and interview. Secondly, they received the security warning

enhancement based on their preferences, followed by a further questionnaire and interview. The final section was only shown to users if they did not choose all the options, or at least option 2 in the repeated question (i.e. Task 7). This is because the user would not be presented with security warning enhancement (adapted warning) if they did not choose those options. Then, a comparison could be made (i.e. standard security warning vs. security warning enhancement (adapted warning)²) by stating users' preference and probing some questions with regard to the usability of security warnings (i.e. interview session).

Within the prototype, in every task that the users encountered, six preferences were presented to them. Users were required to choose at least one of the available preferences/options, as follows:

Option 1: More information regarding the reason for the dialogue

Option 2: More descriptive information to guide me on what to do

Option 3: Recommendations based on other users' actions in response to this dialogue

Option 4: Consistent/explicit/clear usage of signal icons and words

Option 5: Information presented in clear sections in the form of question/answer

Option 6: Using non-technical language to describe the problem

These preferences were used based on the author's previous findings and the literature review from the aforementioned Chapters 2 to 6 (i.e. as well as from recommendations and suggestions from security practitioners). By choosing any of these preferences or a combination of preferences, a different presentation of security warning dialogues was generated. The adapted warning was generated only when all the options were chosen by users, or at least option 2 was clicked.

One essential element that was hidden from the users' view was that, if they chose option 2, it was equivalent to the function of "select all". The rationale not to use the "select all" wording was the possibility that users would automatically choose this option is available (i.e. would not read other information and click on the option that made their decision quicker). Therefore, this hidden element was not revealed to the users. Instead, the author used the "More descriptive information to guide me on what

² It is also known as security warning enhancement (complete) where all available preference is used to generate the warning.

to do” statement. It may be noted that this statement generally describes the whole concept of guidance, which covers all other elements normally required in order to comprehend security warnings (i.e. all other five options). The wordings “descriptive information” may be seen to emphasize the steps that are able to guide users by explaining the current issues of warnings circumstances and available features (e.g. signal icons, words, technical jargons and colours). Results of some other combination are presented in Appendix D.

There were seven identified tasks, which comprised security warnings in a dialogue box context that were derived from within three web browsers and applications (i.e. Internet Explorer, Google Chrome and Mozilla Firefox). These security warning dialogues were chosen to show the variety of available warnings and to ensure that users experienced the warnings that they normally encountered, rather than one that was unfamiliar. Within this chapter, detailed results are presented accordingly.

7.4 Results and findings

The majority of the participants were male, as compared to the last three user studies in Chapter 3 – Chapter 5 which were dominated by female participants (See Table 7.1). The majority of these participants were in the range of 18-25 years old and came from a wide range of educational levels (i.e. from GCSE/O-Level to Postgraduate). The majority had at least a higher education level.

In terms of computing skills, 54% respondents considered themselves as intermediate, 30% as advanced and 8% as expert and beginner respectively. The vast majority (90%) claimed that they had used the Internet for more than six years and the rest were in the range of 3-4 and 5-6 years. This indicated that this group of respondents were likely to be familiar with current technology. Google Chrome remained the preferred choice of browser by respondents, at 38% (i.e. as compared to user study 3 in Chapter 5 and 6) and followed by Internet Explorer 32%, Mozilla Firefox 22% and the respective balance 8% with Safari and Opera. Even though the majority of participants were derived from the University environment, this did not significantly impact the higher proportion of Internet Explorer as main web browser (i.e. Internet Explorer is the default browser in the university environment).

CHAPTER 7: EVALUATION AND VALIDATION OF THE AUTOMATED
SECURITY INTERFACE ADAPTATION (ASIA)

Similar results were found with user's operating system preference where the majority preferred to use Windows 7 with 64%. It followed by Windows XP with 16%, Mac OS X with 12%, Linux and Windows Vista with 2% respectively. Surprisingly, 4% (i.e. two respondents) did not know indicate a preferred operating system. With regard to the usage of security software, 70% of respondents claimed to use it leaving 8% with "no" and 22% with "not sure". When asking users regarding their perception on decision making based on security message in general, 62% claimed it was easy, 18% claimed it was not whilst 20% were unsure. Even though the percentage was not encouraging (e.g. more than 50%) but 38% can be considered a worrisome percentages. It is, however, concerning that 38% of respondents were either unsure or found the decision making process difficult when assessing their interactions with security dialogues. This indicates that users in general had significant problems with their decision making process on security message.

Characteristics (n = 50)	Frequency Distribution	Percentage Distribution (%)
Gender		
Male	31	62.0
Female	19	38.0
Age		
18 – 25	26	52.0
26 - 35	16	32.0
36 - 45	5	10.0
46 - 55	2	4.0
Above 56	1	2.0
Educational Background		
Postgraduate	18	36.0
Higher Education	19	38.0
Diploma, Further Education	8	16.0
GNVQ	0	0.0
GCSE/ O Level	5	10.0

CHAPTER 7: EVALUATION AND VALIDATION OF THE AUTOMATED
SECURITY INTERFACE ADAPTATION (ASIA)

Characteristics (n = 50)	Frequency Distribution	Percentage Distribution (%)
Computing skills		
Expert	4	8.0
Advanced	15	30.0
Intermediate	27	54.0
Beginner	4	8.0
Security software usage		
Yes	35	70.0
No	4	8.0
Not sure	11	22.0
Years using Internet		
<1	0	0.0
1 - 2	0	0.0
3 - 4	2	4.0
5 - 6	4	8.0
> 6	44	88.0
Preferred web browser		
Google Chrome	19	38.0
Internet Explorer	16	32.0
Mozilla Firefox	11	22.0
Safari	3	6.0
Opera	1	2.0
I do not know	0	0.0
Preferred operating system		
Windows 7	32	64.0
Windows Vista	1	2.0
Windows XP	8	16.0
Mac OS X	6	12.0
Linux	1	2.0
I do not know	2	4.0

Characteristics (n = 50)	Frequency Distribution	Percentage Distribution (%)
Easy to make security decision in general		
Yes	31	62.0
No	9	18.0
Not sure	10	20.0

Table 7.1: Summary table of demographic user study 4

7.4.1 Users' preferences in the experimental tasks (i.e. 7 tasks)

After the completion of the demographic section, users were presented with a security warning task 1, as depicted in Figure 7.1. This security warning was taken from the Mozilla Firefox web browser when users navigated to their intended Google page after pressing the enter button. As discussed in the previous section, if users clicked option 2, it was equivalent to ticking all available options. Therefore this section sought to reveal end-users preferences based on the options given. However, the focal point among these tasks was given to task 7. Security warning adaptation was generated based on the options chosen by users in this task. Then further assessments and evaluations were conducted for ASIA.

It can be reported that the majority of users had chosen options 1, 2 and 6 as their main preference for the task 1 as depicted in Figure 7.1 (i.e. from single option views). The 27 respondents (out of 50) chose to have all preferences, five respondents chose option 1 only and the remainder with other combinations. This dialogue box used the header as a security warning, but with a question mark icon. The information presented was incorporated the usage of technical expressions such as “unencrypted connection” and “third party”. By looking at the overall presentation of the warning, it can be noted there were no unique indicators to describe the risk levels, explain what is really happening and guidance to help users to make a decision.

CHAPTER 7: EVALUATION AND VALIDATION OF THE AUTOMATED SECURITY INTERFACE ADAPTATION (ASIA)

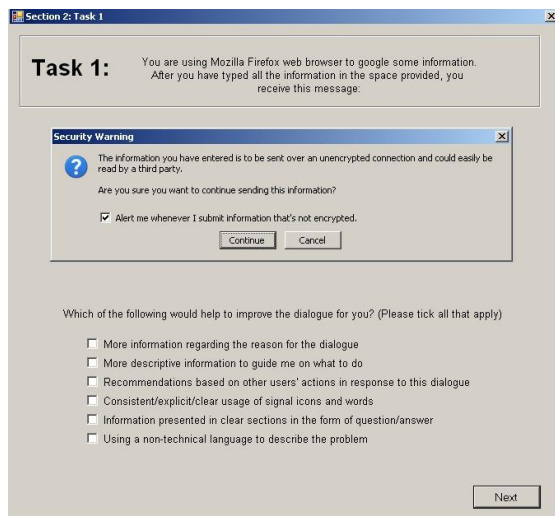


Figure 7.1: Task 1 security warning

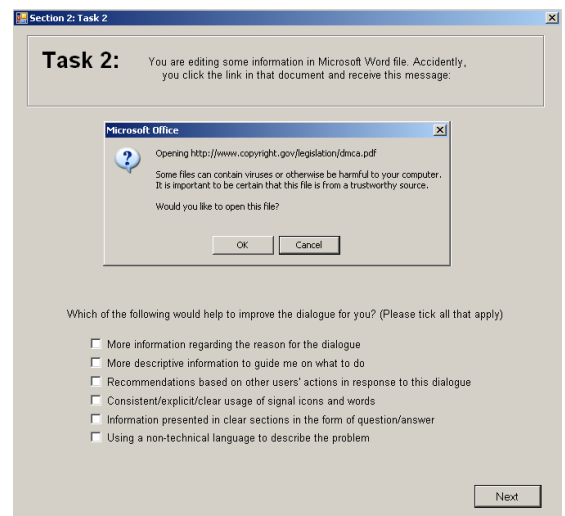


Figure 7.2: Task 2 security warning

After clicking next, users were presented with task 2 as shown in Figure 7.2. This security warning popped up when users clicked a link in a Word document to open a PDF document. Again, the majority of the respondents 29/50 had chosen all of the preferences followed by six respondents with option 1 only. The remainder had chosen other combinations. This security warning explained the risk of opening the file and that this file should come from a trustworthy source, but did not explain what it meant and how it could help users.

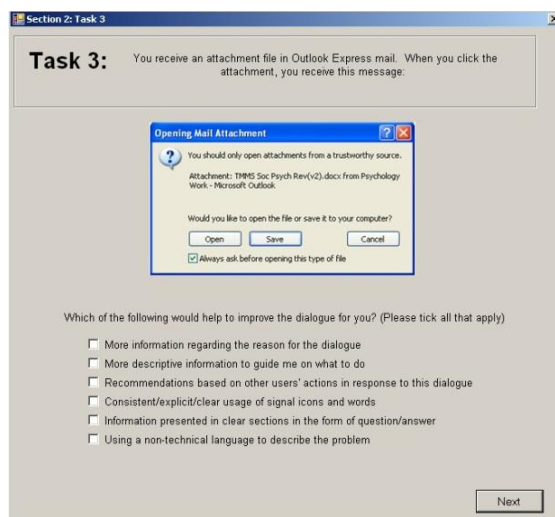


Figure 7.3: Task 3 security warning

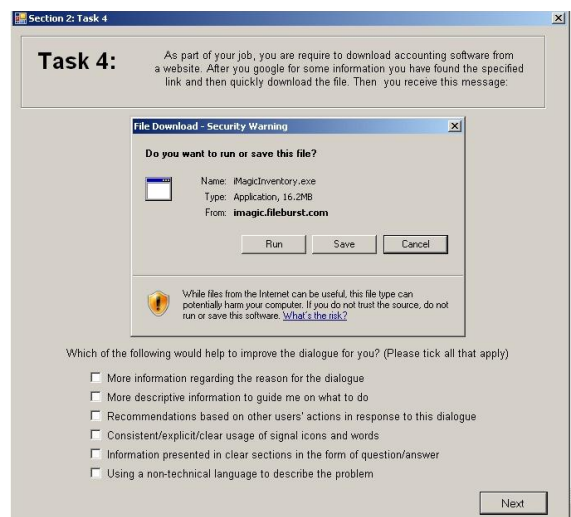


Figure 7.4: Task 4 security warning

In task 3 as presented in Figure 7.3, users were presented with a security warning titled “Opening Mail Attachment” from Outlook Express. It reminded users that attachments should only be opened when they come from a trustworthy source (e.g. if the user knows the sender). 26/50 respondents chose all options, eight respondents with option 1, 5 chose option 3 whilst the remaining chose other combinations preferences. Based on this warning, there was a possibility that users might execute the malicious content if they open the file straight away. However, the security warning did not convince users of the severity of the risks.

With regard to Figure 7.4 from Internet Explorer, 27/50 respondents decided to choose all available options when they were presented with a “File Download – Security Warning” message. Seven respondents decided to choose option 1, 4 chose option 3, 2 with option 5 and the rest with other combinations. With this security warning, the header title and the usage of signal icons were consistent (based on Microsoft (2010) Guideline). If users wished to utilise the help option, they had to click the link at the bottom (new help dialogue pops-up). The use of an unidentified program icon (white background) did not present a meaningful message to users.

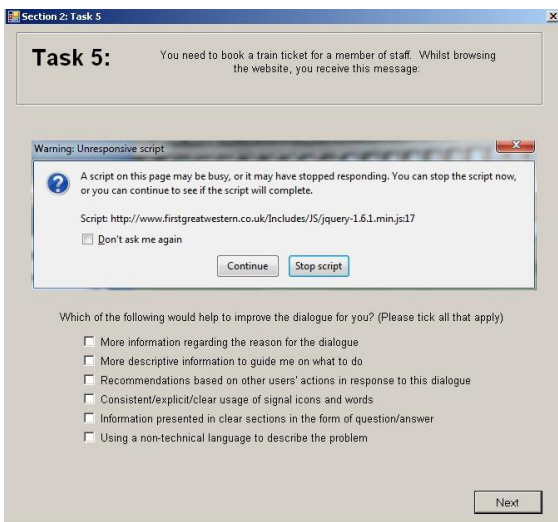


Figure 7.5: Task 5 security warning

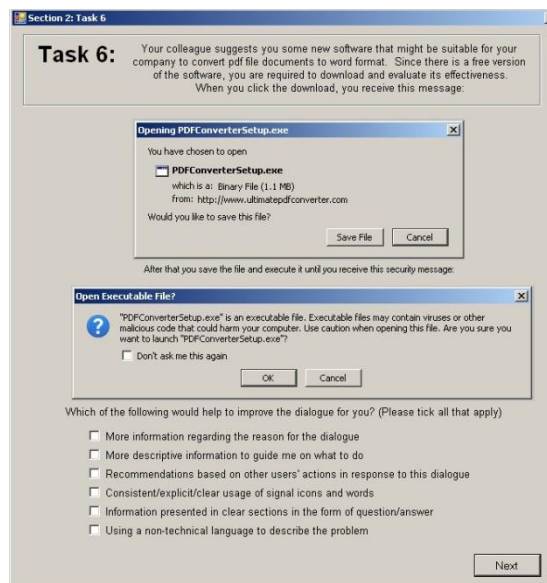


Figure 7.6: Task 6 security warning

After clicking next in task 4, users were presented with task 5 as depicted in Figure 7.5. The warning header “Warning: Unresponsive Script” was derived from the Mozilla Firefox browser. Within this warning context, 23/50 respondents chose all available options leaving eight respondents with option 1, 5 respondents with option 6 and the

remaining with other combinations. Some comments can be made on the usage of wordings to explain the circumstances of the message. The word “script” was used without further explanation and meaning and how it can affect the computer system. The information was delivered in a highly technical manner which was not suitable for general level users. Therefore, users might struggle to understand it.

Task 6 was the security warning related to an application download in Mozilla Firefox. The first security warning was presented to users when clicking the link to download the file. Once they had saved the file on their computer and executed the .exe file, they received another security warning with the header “Open Executable File?” This study revealed that 24/50 respondents chose all available options, five respondents decided to choose option 3, 4 respondents with option 1, 2 respondents with option 5 whilst the rest chose other options. This security warning did not have features that were able to convince users to make safe decision at all. Albeit users had to save the file in the first place, they should be given early information about the current warnings that they encountered (i.e. the severity/risk levels, consequences of actions and guidance on what to do). Only after they executed the file from their computer, they receive another warning. Again, in this warning, the information provided was too general.

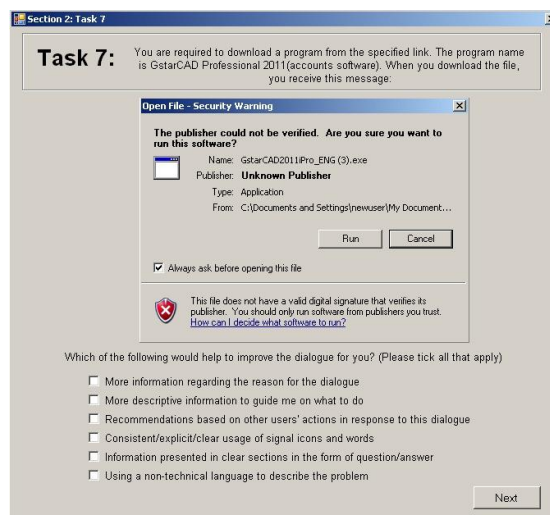


Figure 7.7: Task 7 security warning

With the final task 7, users received a security warning when they wished to download an application using Google Chrome browser. Based on user preferences in this task, security warning adaptation generated a new security warning after this. This task was chosen because users were expected to be able to make use of all the features in this

warning. It was also considered that users had greater familiarity with the downloading event, therefore this security warning was used as the focal point of this user study. End-user comprehension and further assessment will be described in the next sections. The majority of users 30/50 decided to choose all options leaving three respondents choosing options 1 and 3 respectively. Two respondents chose option 5, and the remainder other combinations.

7.4.1.1 Repeated task

Once users had completed all of the seven tasks, they were presented with a “Dialogue Enhancement Notification”, as depicted in Figure 7.8.

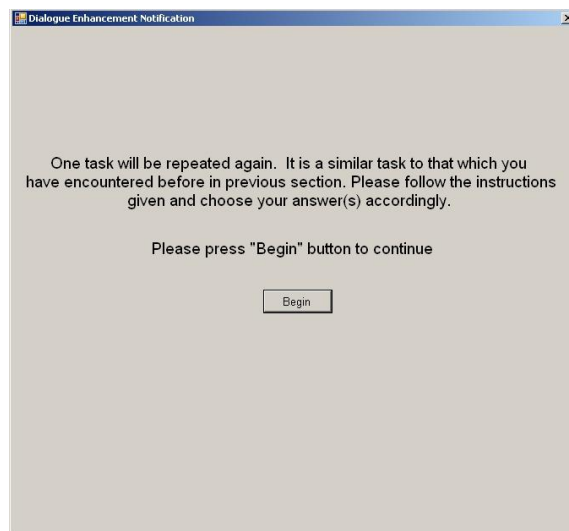


Figure 7.8: Dialogue enhancement notification

Users were notified that one task would be repeated. Then, after they pressed the “Begin” button, they were presented with task 7 once again, as depicted in Figure 7.9.

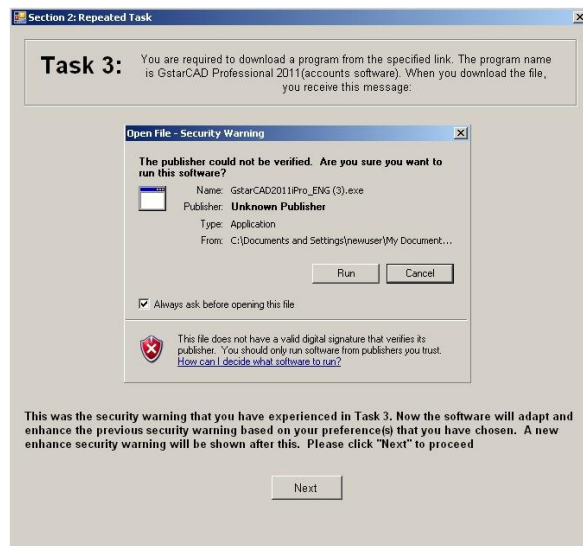


Figure 7.9: Repeated task

At this stage, it had been explained that an adaptation of security warning was made based on the preferences that users made in the previous task 7. Once they pressed the “Next” button they will be presented with a simplified security warning as depicted in Figure 7.10. Shortly after this, the principal investigator explained that this was the first warning that occurred and users were required to familiarise themselves with the features (i.e. click the link or hover over any texts available) and they can make a decision by choosing one out of the three available buttons. Later, they were asked questions about the decision they had made and the available features.

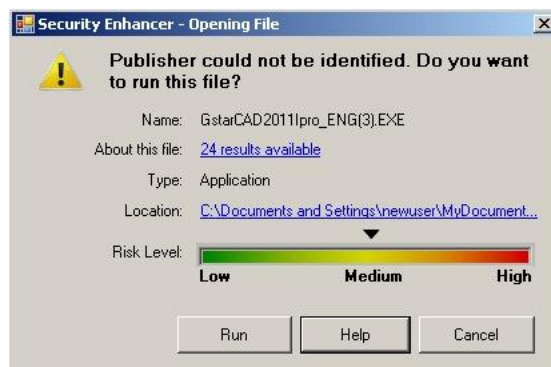


Figure 7.10: The simplified security warning

7.4.1.1.1 Analysis and observations of end-users perception and understanding when encounters with the simplified security warning.

After users had viewed the simplified security warning, as presented in Figure 7.10, they made their decision by choosing one of the available buttons. Once they had made up their mind by choosing one of the available option, the principal investigator asked them to stop and asked them questions to probe their decision making process. If the user hovered their cursor over certain features (i.e. icons or texts), tooltips would be displayed to provide a simple summary of the features. It was to be expected that this would provide some clarification to users in order to understand the warnings.

If users decided to choose help, they were presented with a security warning enhancement based on their preferences. Therefore they were unable to see the simplified security warning again. In order to counter this problem, users were again shown the image of a simplified warning in a word document, rather than on the prototype software (i.e. for the interview purposes). If users had chosen Run or Cancel, nothing would happen but user’s decisions would be recorded (i.e. users would continue to view the simplified security warning, as in Figure 7.10). Their decisions were classified, as presented in Table 7.2.

Options available	Total responses (n = 50)	Percentage (%)
Run	27	54
Help	16	32
Cancel	7	14

Table 7.2: Users’ decision upon receiving simplified security warning

The majority of users 27/50 decided to run straight away, 16/50 had chosen the help option whilst 7/50 users decided to cancel. Then principal investigator interviewed them to further understand their decision making process and with regard to the features available (i.e. comprehension and satisfaction). The first question was to probe the reason for choosing the presented options. Two investigators read the recorded transcript independently, identified common ideas and later coded the results, as presented in “the reasons” column in Table 7.3 to Table 7.5 (i.e. Please refer to the Appendix D for the details of the questions).

The reasons	Total responses (27/50)
I just feel it is safe to proceed	1
Risk level is medium	16
I ignore everything because I want to use this software so I take the risks to proceed	3
My normal behaviour always choose run	3
Filename is appropriate	1
As long as I have antivirus I will always choose run	1
About this file – I can get some evidence on the popularity of search regarding this file	2

Table 7.3: Reasons on choosing Run option

The majority 16/27 of users who chose run claimed the reason they chose this was that the risk level was set to a medium level. It was likely that they considered the medium range could not cause harm to their computer. All respondents claimed that they could see straight away the risk level bar that attracted them on the first impressions. On the other hand, three users demonstrated that they would ignore everything (i.e. take the risk) if they really wanted to use this software. Surprisingly, a further three users claimed that it was their normal behaviour to choose “run” all the time. When probing further, they said that they most likely ignored all of the details in the warnings as they believed it was safe to proceed based on their previous experienced. This indicated that users learnt from the past by ignoring the security warning, and because no obvious bad consequences happened to them. Two users claimed that this file had a positive impact on them as they could see that some other people had previously searched for more information about this file (i.e. by the assumption they can read good reviews about this file). One interesting finding was related to one participant who claimed that he/she would always choose run as long as he/she had installed antivirus software on the first place. When probing further, this person assured that antivirus would protect them from any malicious attack because this was the reason why they used the software.

The reasons	Total responses (16/50)
Publisher could not be identified	1
Risk level is set to medium and I want to get more information	13
Help is always best option as I think this operation is quite risky	2

Table 7.4: Reasons on choosing Help

With regard to the reasons for choosing help, the majority 13/16 decided as the results of the risk level was set to medium. They were not sure whether to proceed or not, thus, they wished to obtain more information. Some of these users claimed that they did not want to take the risk of becoming a victim of malware attacks, so help was the best option. At least within these contexts, users were able to view any useful information available to help them. When probing further, most of these users mentioned that they would be pleased to use the help function if this function provided straightforward information rather than generic information. Five users claimed that most of the help functions provided did not specifically solve problems, but rather, gave general information. Users had to view and click somewhere in the function to get to the solution, which was a cumbersome task.

The reasons	Total responses (7/50)
The risk level is medium - It is too risky to proceed	4
Publisher could not be identified – I do not want to take any risk	2
Entirely not looking secure	1

Table 7.5: Reason on choosing Cancel

On the other hand, only seven users chose cancel when the security warning was presented to them. After probing them with some questions, the majority claimed that they decided to choose cancel when they saw the risk level was set to medium range. For them, it was still a risky range. They defined the safe range when the risk level was set to low (i.e. green colour). Two respondents also used the statement “Publisher could not be identified” as their reason. For them, it was crucial if the computer was unable to detect the publisher so it is possible that the software came from an unknown source

which could cause harm to them. Again when asking further, they did not want to take further risk. One claimed that *“it is better not to download rather than crash your computer system”*.

The next question asked users “What features help you to understand the security warning” based on the depicted warning in Table 7.6. It can be revealed that almost half of the overall respondents liked the risk bar level used in the warning. Most of them stated that it looked attractive with the vibrant colours. Some of them claimed that they could quickly make up their mind with the decision based on the risk level bar presented (i.e. convey the risk level that users encountered).

The reasons	Total responses (n = 50)
Risk bar level	23
Overall presentation help me to understand warning	4
About this file feature	9
Visual will always come first	1
Signal icons (!)	5
Hover information	2
No specific features	2
Jargon busting – too many technical words	1
Use simple and plain English	1
Not sure	1
I ignore everything but visually I think it is nice	1

Table 7.6: Features that help users to understand the security warning enhancement.

9/50 claimed that this file (i.e. with the assumption it able to work) was useful because they able to view more information just by clicking. 5/50 indicated that the exclamation mark icon (!) made them aware of this security warning. These users claimed that the icon was clearly presented with a nice colour scheme. With the overall layout making them more focus on understanding the warning. They also claimed that some other features available within this warning contributed to the success of the overall layout. Two users appreciated the hover information (i.e. tooltips), whilst the other two surprisingly claimed no specific features helped them to understand the warning (See Table 7.6).

Level of satisfactions	Total responses (n = 50)
Yes slightly but more information is better	12
Very satisfied	30
I am not really sure	2
Yes but more details information should be there to explain the risk level	1
I hope to have online feedback features so that user can straight away give some thought to developer	1
Not enough information and it should be more explicit	4

Table 7.7: Satisfaction with the information provided

The final question “Are you satisfied with the information provided? Why?” was asked to evaluate the early stage of users’ reaction when encountered with the simplified security warning. This gave an early indication as to how end-users viewed ASIA (i.e. even though the security warning enhancement had not been viewed yet). From the interview session, the majority of users responded that they were very satisfied with the layout 30/50. 12/50 respondents claimed that more information should be there to make it more useful, and one claimed that the risk level bar should provide more detailed information. On the other hand, four users claimed that the information was still not enough and it should be presented in an explicit way. When they were asked how explicit they wished the information to be, some claimed that they did not mind if the information was in a long statement, as long as they could understand it without the need to view other sources. Only two users claimed that they were not really sure.

7.4.1.1.2 Early stage results

Having understood this early analysis and observations, the majority of users decided to run the file straight away from the provided options. With ASIA, it is expected that users will choose Help more readily. A new security warning (security warning enhancement) would be generated once the help button was pressed.

Users had not been told about it (i.e. choosing help) as the author wished to see how the simplified security warning changed users’ perception with regard to the new layout of

warning they encountered. In addition, it was important to see end-users normal decision upon receiving security warning dialogue. It was felt to be better to let users decide what they believed was the right thing to do, rather than make it compulsory for them to click Help at this stage (i.e. to avoid bias). However, shortly after users had made their decision (i.e. pressing run or cancel), they were briefed about the new help feature available once they had pressed the function. The next evaluation and validation stages provided more empirical evidence, as outlined in the next section.

ASIA encourages users to click help when they encounter a security warning because it combined two stages of an ideal security warning as discussed in Chapter 6. ASIA promoted a new dimension of presenting security warnings where upon clicking the help button users were still in the same security warning dialogue with new additional features based on their preferences (i.e. rather than having a new dialogue box pop-up). It basically integrated the simplified security warning and some other features based on what end-users really want it to be in the first place (preferences).

The way information and new features were presented in the simplified security warning was accepted by the majority of the respondents, with more than 80% of total respondents being satisfied with the level of information provided. They had highlighted some available features that helped them to understand the security warning (i.e. risk level bar, about this file, signal icon and hover tooltips information). Only two users responded that they were not really sure about the new layout of the security warning presented. Therefore, it may be concluded from the initial analysis and observations that ASIA provided a potential improvement that could lead users with better and improved decision making process that will be discussed further in the next section.

7.4.1.2 Enhancer Process and expected output

The adaptation of security warnings involved two main stages (i.e. the simplified security warning and the security warning enhancement). The first security warning that popped up after users clicked “Next” in the previous task is shown in Figure 7.10. This security warning was part of the enhancer process, where some of the available features in this warning were derived from the standard security warning. After the user

clicked next, the adaptation of security warnings started by enhancing the simplified security warning with some additional features based on user preferences. These additional features were used based on the suggestion in the previous studies of end-users (Chapters 3 - 5). Figure 7.11 is an example of the adapted warning (i.e. if users chose option 2 or all of the options).

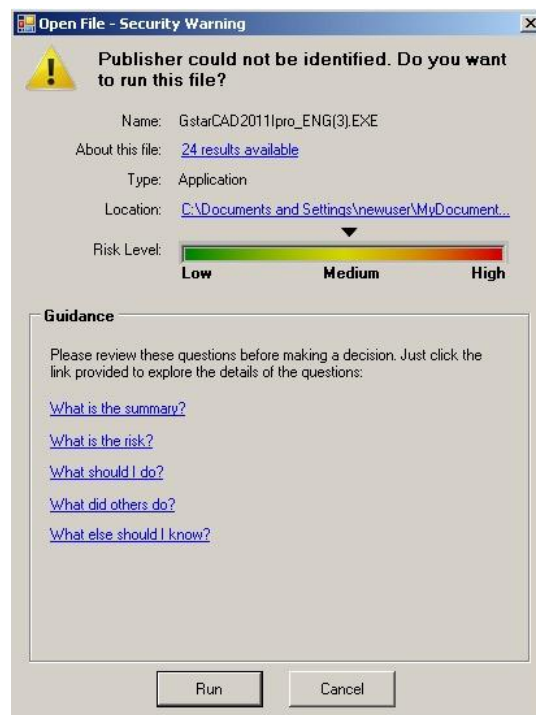


Figure 7.11: The adapted warning.

7.4.1.2.1 Help function details

Normally, the help function was represented by a hyperlink in the footnote area with some text explaining the risk level and other related information. When users clicked the link, they were presented with a new dialogue box which contained the help documentation (e.g. context sensitive help and online help), as shown in Figure 7.12.

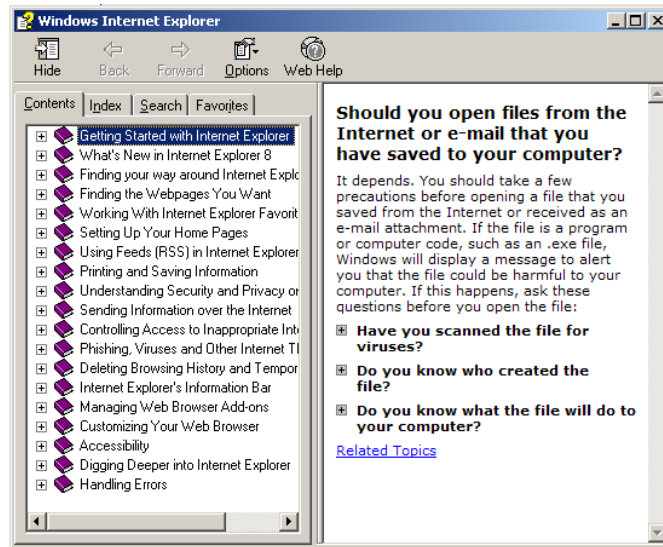


Figure 7.12: Help dialog box

However, within the ASIA framework, significant changes were made. The conventional help button was used instead of the hyperlink that was normally used in the standard security warning. The focal point to be addressed here was related to the main function of this help feature. All adaptation elements were generated once this button was pressed (i.e. the Engine Manager extracted information from User Support Data (USD), Decision Risk Data (DRD) and Community Decision Data (CDD)) in order to deliver the security warning enhancement.

7.4.1.2.2 Standard security warning vs. simplified security warning

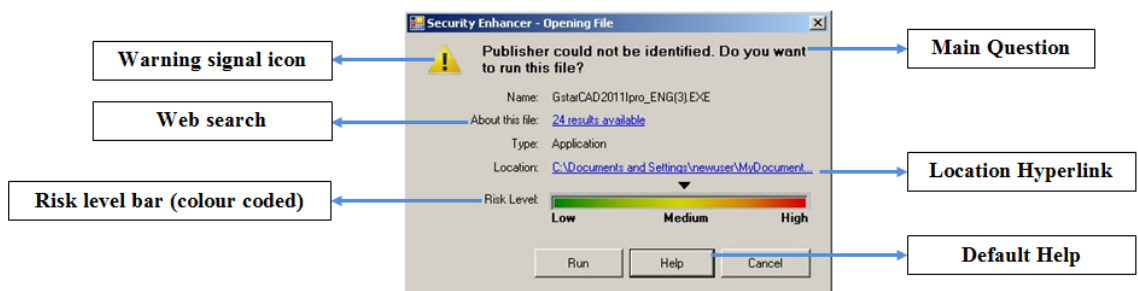


Figure 7.13 : Simplified security warning details

The simplified security warning used some similar features that were readily available in the standard security warning (i.e. name of the file, type, two buttons, background colours and texts). It kept some of the useful features and enhanced the security warning with some other additional information. The simplified security warning had

additional features, as presented on Figure 7.13. It consisted of the main question, about this file link (specific information via web search), location hyperlink, and risk level, help button functions and warning icon as described in Table 7.8.

Standard security warning	Simplified security warning	
	Similar Features	Additional Features
<ul style="list-style-type: none"> • Name of the file • Type • Two buttons (i.e. run and cancel) • Background colours • Texts 	<ul style="list-style-type: none"> • Name of the file • Type • Two buttons (i.e. run and cancel) • Background colours • Texts 	<ul style="list-style-type: none"> • The main question • About this file • Location • Risk level • Help button • Warning icon

Table 7.8: Comparison of availability of features between standard security warning and simplified security warning.

Some of these additional features were derived from features available in standard security warning (i.e. with an improvement in terms of wordings and layout). The significant changes in the additional details are given in further detail in Table 7.9, as follows:

Additional features	Descriptions
The main question	In the standard security warning the main question was posed as “The publisher could not be verified. Are you sure you want to run this software?” However in the simplified version, the wording was slightly changed to “Publisher could not be identified. Do you want to run this file?” . Instead of using technical expression (i.e. verified), the wording was changed to make it more easily understood.
About this file (web search)	This is a new functionality introduced by the simplified security warning. When users click this hyperlink, it navigates the user to a search page for the file. So instead of users manually typing for example “review about GstarCAD2011”, the generated hyperlink might be useful to provide details.
Location hyperlink	Initially, in the standard security warning, the location is known

Additional features	Descriptions
	as “From” and it did not have the hyperlink. To ensure that every feature is presented in a meaningful manner, the new term “Location” was introduced instead of “from”. The Location had been set up as a hyperlink so that users can see the specific location of the downloaded file (i.e. instead of presenting “from” with a static location.
Risk level	The risk level was introduced to convey the severity of risk involved with regard to the message presented. Every security warning dialogue should clearly communicate the risk so that end-users and aware of the possible actions to take. No specific risk level was used in the standard security warning.
Help button	In the standard security warning, the help function was represented using a link at the footnote area. Some information was presented to explain the scenario but using technical terminology. Therefore, the help function had been used to generate security warning enhancement (preferences) which were later able to achieve the aims of ASIA.
Warning icon	Initially from the standard security warning, two icons had been used (i.e. unidentified program icon with white background and warning error icon). In order to produce a more meaningful security warning in the first place, the unidentified program icon was removed. An error icon was replaced with the warning icon (i.e. based on Microsoft Guidelines 2010). An error icon should only be used when presenting an error condition.

Table 7.9: Description of additional features available on the simplified security warning.

7.4.2 The adapted warning

When users clicked the help button on Figure 7.13, they were presented with Figure 7.14 if they chose at option 2 or all of the available options on the preferences list. The adapted warning layout originated from the simplified security warning. The layout was expanded to become longer in terms of size, with additional functions. The decision areas that comprised the run and cancel button were moved to the bottom,

whilst the help button was expanded as “Guidance”. The guidance element consists of useful information presented as questions and answers (Baecker et al. 1995). The availability of questions and answered were depending on the preferences that the user had chosen in task 7. The details of the available features are presented in Table 7.10.

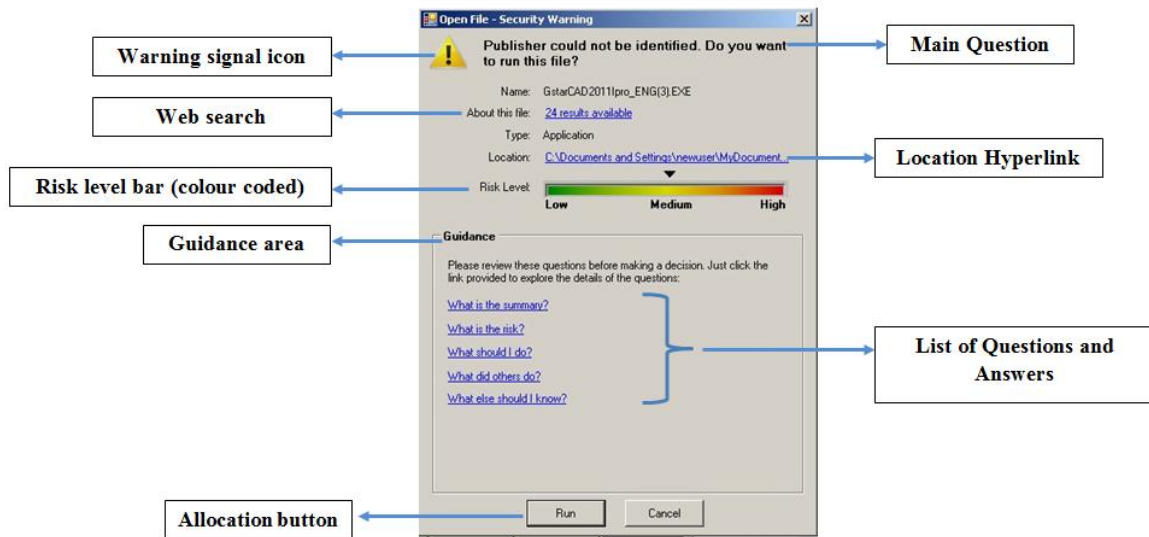


Figure 7.14: The adapted warning details

Additional features	Description
The main question	“Publisher could not be identified. Do you want to run this file?” It used a more straight forward question rather than the one in standard warning
Signal icon	The warning icon is used to be consistent with the header of the message. It conveys the message as a warning rather than an error or as information.
About this file (web search)	This function opened a search page that related to the file (i.e. information about how many people are searching for this particular file). So instead of users manually type for example “review about GstarCAD2011”, the generated hyperlink might be useful to provide details.
Location	Initially, in the standard security warning, the location is known as “From” and it did not have the hyperlink. To ensure that every feature is presented in a meaningful manner, the new term “Location” was introduced instead of “from”. The Location had been set up as a hyperlink so that users were

CHAPTER 7: EVALUATION AND VALIDATION OF THE AUTOMATED
SECURITY INTERFACE ADAPTATION (ASIA)

Additional features	Description
	able to find the specific location of the downloaded file (i.e. instead of presenting “from” with a static location).
Risk level	The risk level was introduced to convey the severity of risk involved with regard to the message presented. Every security warning dialogue should clearly communicate the risk so that end-users are aware of the possible actions to take. No specific risk level was used in the standard security warning.
Guidance area	The guidance area was introduced to help users to make a better decision. Therefore, useful information can be gathered by users before they were able to make a decision. Instead of showing this information in a new dialogue box, the information was depicted in the same warning dialogue (i.e. expansion areas).
List of questions and answers	This consisted of five questions and answers. These were the questions that users normally tend to ask upon completing computer tasks. The amount of questions and answers here can be varied based upon user preferences.
Allocation button	Run and cancel buttons were placed at the bottom after the expansion of the simplified security warning. This was to ensure that the options available were still consistent with the standard security warning.
What is the summary	This explains the summary of the warning presented
What is the risk	This explains about the risks involved (i.e. risk level, description and consequences). It provides further information based on the risk level bar on the main page.
What should I do	This explains possible actions that users should do or consider before taking any action.
What did others do	This provides statistical values (pie chart) on what other people chose when encountering the same warning.
What else should I know	This provides an investigative action for users based on gathering all available information.
Hover functions	This provides quick information to help users understand the context of warning (i.e. what is really happening) when hover to feature as the following:

Additional features	Description
	<p>GstarCAD2011 PRO_ENG(3).EXE Hover tooltips = This indicates the types of file that you are downloading.</p> <p>24 Results available Hover tooltips = A web search for the filename has found 24 results, which may potentially give further details about what it is.</p> <p>Application Hover tooltips = This indicates that the file is a program that you can download and run</p> <p>C:\Documents and Settings\newuser\... Hover tooltips = This indicates the location of the file on your system</p> <p>Risk level bar Hover tooltips = The risk level is set to Medium. The system was unable to detect the publisher of this file. It is recommended you to view all information given before making any decision.</p> <p>Low Hover tooltips = The green area means that the file that you are downloading is likely to be safe</p> <p>Medium Hover tooltips = The yellow area indicates that the computer is unable to identify the source of the file that you are trying to download</p> <p>High Hover tooltips = The red area indicates that the file you are downloading is likely to be harmful to your system.</p>

Table 7.10: Description of the adapted warning

7.4.3 Post-Trial Questionnaires and Interviews

This section highlights details of the questionnaire and interview with regard to the security warnings that users encountered (i.e. refer to Appendix D for details of the questionnaires). In order to reduce bias, users were presented with a standard security

warning first, followed by the security warning enhancement (i.e. Similar technique by Raja et al. (2011) was used in this prototype software). According to Cranor (2008), each individual had their own set of personal variables, intentions and capabilities that impacted warning information processing. Therefore, by presenting security warning enhancement first will produce element of bias (i.e. users had encountered simplified security warning before). To reduce the learning effects, the author counter balanced the order of presenting the warnings.

Based on Figure 7.15 there were three main sections involved. Firstly (i.e. section 3-1) users were presented with standard security warning. Then, they were required to answer questionnaire A followed by an interview. Then, in section 3-2 users were presented with the security warning enhancement (based on user preferences). Again, they were required to answer questionnaire B followed by an interview. Then, users could only proceed to section 3-3 if in section 3-2, user preferences were not equivalent to the adapted warning, as depicted in Figure 7.11.

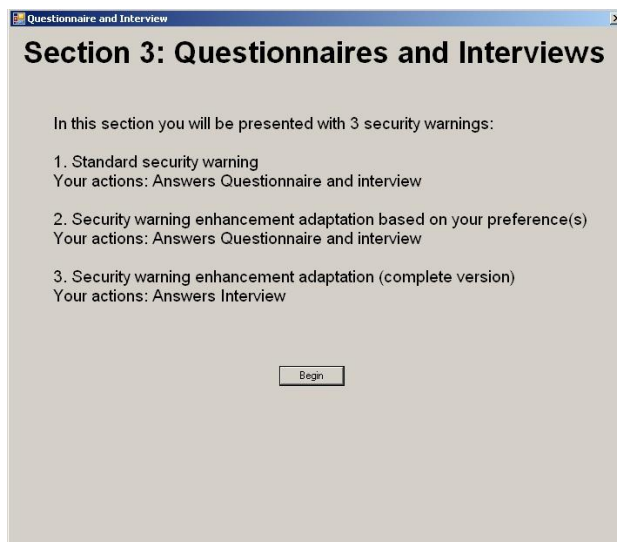


Figure 7.15: Questionnaires and interviews in section 3

The principal investigator gave ample time for users to be familiar with the adapted warning in section 3-3 (i.e. if this was not the users' choice in section 3-2). They were allowed to click any link, hover their cursor and click any possible button to read and familiarise themselves with the information provided. Shortly after that users were asked some usability related questions (i.e. effectiveness, efficiency and user satisfaction) to compare between the standard security warning and the adapted warning.

They were also asked about their main preference and what other elements should be there to improve the warnings presentation.

This study used the questionnaire and interview in two separate sessions (i.e. Questionnaire A and Questionnaire B). This was followed up by an interview session after the users had finished filling in the questionnaire section. There were twelve questions provided, comprising the assessment of users' knowledge about the nature of security dialogue, the types of problem that occurred and some other related questions related to usability issues. The first two questions were related to the comprehensibility of security warnings, whilst the remaining ten questions were focused on the questionnaire (i.e. likert-scale options). Comprehensibility questions were asked to examine users' knowledge about current security warning presentations, whilst the remaining questions were intended to evaluate end-users satisfaction, perception and understanding of the overall presentation of security warnings.

Ten questions presented in the questionnaire (i.e. likert-scale options) can be classified within two groups of connotation (i.e. positive and negative). The positive connotation can be defined as the positive feelings or expression with regard to the features, decision making, awareness and satisfaction (i.e. questions 2 to 10) whilst negative connotation focused on the negative impact as the results of using standard security warning (i.e. question 1). The following section discusses the standard security warning and security warning enhancement findings.

7.4.3.1 Standard security warning

Users were presented with standard security warnings as depicted in Figure 7.16. They were required to view all details and were allowed to click the hyperlink in the footnote area, and were presented with a new dialogue box which contained help as shown in Figure 7.12.

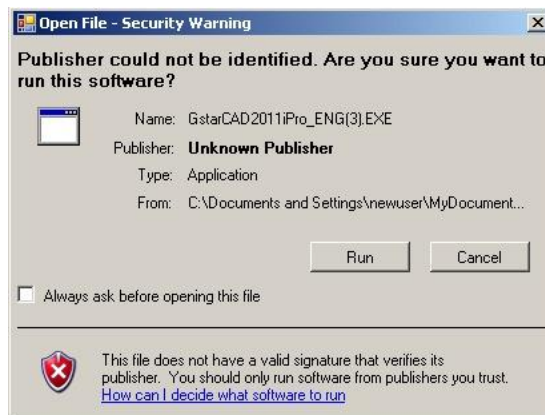


Figure 7.16: Standard security warning

Users had been told that the help dialogue box was not the real dialogue but a simulation of the real one. However, the information provided was copied from the real dialogue. Users had also briefed on the concept of help dialogue box that been presented to them in general (i.e. context sensitive help). Once they were satisfied with everything, they started to fill in Questionnaire A.

7.4.3.1.1 Questionnaire A

The first question that was presented to users concerned the nature of the security dialogue that appeared. It was expected that users would choose warning messages rather than other options. Based on the depicted image, this was clearly a warning message. This study revealed that 47/50 of respondents correctly identified the nature of the security dialogue presented to them, whilst three others claimed that it was an information and question message respectively. A surprising result was highlighted when two participants decided to choose two options (i.e. warning and information) messages, albeit the instruction provided stated only one option was allowed.

The second question was set to test users' understanding with regard to the type of problem as depicted in security warning. It is expected that users would choose only three options (i.e. option 2, 4 and 8) as the correct answer. Only six users successfully chose the correct answers. The full results of user decisions are presented in the following Table 7.11 (i.e. the results in this table were based on the combination of user decision. Thus the total will not equal to 50).

Type of problems	Users decisions (Combination)
Unable to download the software due to an error	2
Potentially became a victim of malware (e.g. virus, worms and trojans)	25
Trying to download.docx document	1
Downloads from unauthorized publishers	44
Does not facing any risk to proceed with the decision	2
Unable to view what other people do with regard to security message	17
Having difficulties to use guidance or help functions	6
Facing potential problem with regard to his/her action to download software	13

Table 7.11: Users decision with regard to the type of problems based on standard security warning

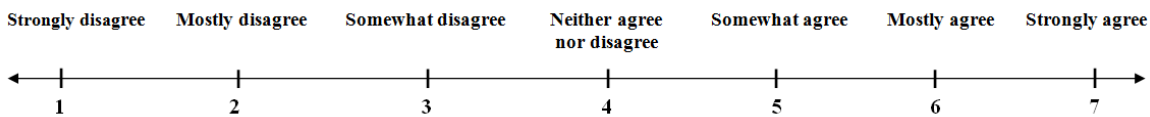


Figure 7.17: Likert-scales range (i.e. 1 to 7)

Overall, users indicated a satisfactory level of understanding where the two most popular options were from the correct options (i.e. option 2 and option 4). Some other types of problems were chosen as distraction options to evaluate user understanding and to ensure that users thought properly before a decision was made. Meanwhile, the next section comprised of ten questions related to end-user understanding, satisfaction and perception with regard to the overall presentation of standard security warning. Users were required to choose one of the available ranges from the likert-scale as presented in Figure 7.17.

On the other hand, Table 7.12 shows overall results based on descriptive statistics (i.e. frequency, mode and median). According to Boone and Boone (2012), the descriptive method is the appropriate one to analyse a series of individual questions. In addition, Bertram (2006) claimed that this implementation was easy to read and to complete by

participants. Therefore, the author made use of this technique to present the results as shown in Table 7.12.

Statements	Most frequent answer (n = 50)	Mode	Median
1. The security dialogue was too complex for me to understand	15 Strongly disagree	1	2
2. I spent enough time to view the information provided	22 Mostly agree	6	6
3. It was easy to understand the information provided	13 Somewhat agree	5	5
4. The way information was presented helped me to complete the tasks	12 Neither agree nor disagree	4	4
5. I could effectively complete my task using the information presented	13 Neither agree nor disagree	4	4
6. It was easy to find the information I needed	13 Somewhat disagree	3	4
7. The interface of security dialogue was understandable	11 Mostly agree	6	5
8. The security dialogue helped me to fix the problem in the way that I understood	12 Mostly disagree	2	4
9. The available help increased my knowledge and awareness about the contents and features of the dialogue.	13 Mostly disagree	2	3.5
10. This dialogue had all the functionality and capability I expected it to have	11 Somewhat disagree	3	4

Table 7.12 : Statistics on users' decision with regard to standard security warning

With regard to question 1, the majority of users selected “strongly disagree” and “mostly disagree” based on the median value presented. This demonstrated that they

did not think that the presented warning was a complex version. However, it can be highlighted that in terms of easy of finding information that users needed, the majority selected “somewhat disagree”. This indicated that users still facing significant problems with regard to the level of information provided. In terms of helped user to fix the problem and helped to increase their awareness and knowledge, the majority selected “mostly disagree”. This demonstrated that users still experienced some level of difficulties in making a decision, despite the features and information was provided. The final question covered almost all elements that comprised all other questions in the questionnaire. The majority of users said “somewhat disagree” to this question. This showed that users were expecting more in order to help them comprehend the message and help to make a decision in a secure manner. In the next section (covering Interview A), details of the investigation are presented.

7.4.3.1.2 Interview A

After users had filled in the questionnaire, they were asked six questions to probe their understanding upon receiving a standard security warning, as depicted in Figure 7.16. The listed questions were given specific attention to the available features (i.e. signal icon, words, technical terminology, help function and level of information provided), the opinion about action taken and satisfaction of overall experienced. The following section highlights the interview findings in further detail.

Users' decision	Total responses (n = 50)
The file will be executed /run with potential of risks	37
Unsure/Uncertain	8
It is dangerous to proceed so I'd rather click cancel	1
Negative effects/problem with my computer	4

Table 7.13: What do you think will happen if you click run?

When users were asked (as shown in Table 7.13) the majority of them gave the correct answer (i.e. the execution of the file). Surprisingly, eight respondents were unsure what to do. When further probed, the reasons they were uncertain were that they did not understand the information provided and they were afraid to proceed with uncertain level of risk.

Users' decision	Total responses (n = 50)
Information provided were ambiguous and difficult to understand	7
Combination of features (i.e. icon, wording and header)	15
Unidentified/unknown publisher	13
Type and name of file	2
Link provided	5
Icon/symbol and colour	8

Table 7.14: What do you think of the feature(s) that are available to help you make a decision in this security warning?

The next question asked about elements of warning that enabled users to make a decision as presented in Table 7.14. 15/50 claimed that the combination of features available on the warning such as the error shield icon, security warning header, type and name of the file, publisher could not be identified and unknown publisher allowed them to make a decision. On the other hand, seven respondents claimed that information provided in this security warning were ambiguous thus difficult for them to understand. When probing further, users mentioned that they were unable to make use of the help function because the information provided was too simple and general. They would expect the information to be straight forward to give them a solution rather than general advice. Having understood this, users demonstrated that they were aware of the features available in the security warning. One possible reason was because users might be experienced with this security warning before. Therefore this significantly affected their understanding. One observation can be made from this, namely that some users realised some features that existed on the warning after they were asked by the principal investigator (i.e. after giving full attention to reading the warning). This indicated that these users did not pay attention to warning details. Therefore, they may not have understood the features presented to them (i.e. meaning and function wise).

Users' decision	Total responses (n = 50)
Uncertain decision whether to run or cancel	5
Publisher could not be identified	9
Technical terminology or wording that makes it difficult to understand	4
Unknown filename	4
It is easy and straight forward	21
Insufficient information from the hyperlink	4
Information provided is too general	3

Table 7.15: Were there any aspects of the warning that you found hard to understand or interpret?

When asked about specific elements of warning that were difficult to understand, the majority claimed that it was easy and straight forward 21/50 as shown in Table 7.15. One possible reason that contributed to this was because users might have encountered this type of security warning before (i.e. had experienced or seen). Some other users mentioned that they did not understand that the publisher could not be identified 9/50, uncertain decision 5/50, unknown filename 4/50, problem with technical jargon 4/50, insufficient details from the hyperlink 4/50 and information provided is too general 3/50. Overall, users still experienced a significant level of difficulty with regard to the security warning dialogue they received. Even though some features were presented to help users in making decisions, it was still insufficient to convince users to make better decisions.

Users' decision	Total responses (n = 50)
Yes with previous experienced in this field	2
It is easy to understand/straight forward/basic/simple	36
It is difficult to understand the technical jargon	7
Not entirely understand	5

Table 7.16: Do you understand the way information was presented especially with technical wording?

In terms of understanding the technical language, the majority 36/50 claimed it was easy (i.e. straight forward, basic and simple) as shown in Table 7.16. However 7 users claimed it was difficult whilst the other five were not entirely sure. From this observation, the standard security warning is quite straight forward with the level of information provided. However since the majority of respondents classified themselves as intermediate 27/50 and beginner 4/50 users, it might be difficult for them to judge. The information depicted in this security warning should be presented clearly in terms of concept and explanation (i.e. simple and plain language and proper explanation).

Users' decision	Total responses (n = 50)
Insufficient options with limited explanation	38
Enough option	9
Enough options with the link at the bottom	3

Table 7.17: Do you feel that this security warning was presented with enough options to guide you?

Almost 80% of total respondents demonstrated that there were insufficient options with limited explanation with regard to the warning presented as shown in Table 7.17 whilst the remainder claimed there were enough options. When probing further, the majority of users mentioned that the option that they were looking for was guidance to help them make a decision. Some of these respondents even suggested an automated decision option. They claimed that the decision making process should be made on their behalf by the computer to reduce the possibility of becoming victims of computer problems.

Users' decision	Total responses (n = 50)
Not really helpful	26
Insufficient information	8
Satisfied with the link but it is still unclear	6
Satisfied with overall	10

Table 7.18: Do you feel satisfied with help available for this warning?

The final question probed users' satisfaction with regard to the help function available. 26/50 users claimed that the current help function was not really helpful whilst another eight users claimed there was not enough information on the help provided as shown in Table 7.18. Only ten users were satisfied with the overall help function whilst six were partially satisfied. Based on these results, it indicated that the current implementation of the help function was still not sufficient to satisfy users. Therefore, the help function should be designed accordingly and can be associated with more useful information.

Based on the overall results, it can be summarised that end-users still face significant problems with regard to the standard security warning dialogue presented to them. They had demonstrated a considerable level of understanding with regard to decisions when clicking run and the way information was presented especially with technical language. On the other hand, they claimed that current options in the security warning were still insufficient with limited explanation. In addition, the help provided was not really useful. It gave clear indication that users had experienced difficulties with regard to the security warning they received. In the next section, users were presented with the security warning enhancement based on their preferences.

7.4.3.2 Security warning enhancement (i.e. based on users preferences)

The full results of users' combination preferences are presented in Table 7.19 based on task seven. The adapted warning as shown in Figure 7.11 was the most popular option. This was the complete version of the security warning enhancement when user clicked option 2 or all of the available preferences. It can be noted with regard to the other preferences, option 1 "more information regarding the reason for the dialogue" and option 6 "using a non-technical language to describe the problem" were among the most common chosen ones by the users based on the results presented.

All the available preferences or options that had been offered were suggested from the previous users' studies results in order to improve the security warning dialogues. In section B, the reported results were based on 50 respondents overall. However, focus was given to the adapted warning, where the majority of participants had their preferences in order to make a fair and relevant comparison later on (refer to Appendix D for example of security warning enhancement images based on users' preferences).

Security warning preferences classification	Total responses	Warning Group
Security enhancement 1 (complete version where users choose at least option 2 or all options / the adapted warning)	30	A
Security enhancement 2 (i.e. Option 1 only)	5	B
Security enhancement 3 (i.e. Option 3 only)	5	C
Security enhancement 4 (i.e. Option 1 & 3 only)	3	D
Security enhancement 5 (i.e. Option 5 only)	2	E
Security enhancement 6 (i.e. Option 1,3 &4 only)	2	F
Security enhancement 7 (i.e. Option 3 & 6 only)	1	G
Security enhancement 8 (i.e. Option 1 & 6 only)	1	H
Security enhancement 9 (i.e. Option 1, 4 & 6 only)	1	I

Table 7.19: Results on security warning enhancement based on users' preferences (classification)

7.4.3.2.1 Questionnaire B

The first question presented to users was similar to that presented in Questionnaire A. It was expected that users would choose warning messages rather than other available options. With regard to the security warning enhancement 41/50 correctly identified the nature of the security dialogue as a warning message, whilst nine others claimed it was an information message. Again, two participants decided to choose two options (warning and information) for the message. However, after being told that they had to choose only one, both of them decided to go for the warning message. In terms of comprehensibility with regard to the type of problems from the security dialogue presented to them (i.e. security warning will be varied based on users' preferences) the

full results of users' decision were compiled in Table 7.20 (i.e. the results in this table were based on combination of users' decision. Thus, the total will not equal 50).

Type of problems	Users decisions (Combination)
Unable to download the software due to an error	2
Potentially became a victim of malware (e.g. virus, worms and Trojans).	29
Trying to download.docx document	1
Downloads from unauthorized publishers	41
Does not facing any risk to proceed with the decision	1
Unable to view what other people do with regard to security message	4
Having difficulties to use guidance or help functions	3
Facing potential problem with regard to his/her action to download software	11

Table 7.20: Users decision with regard to the type of problems based on security warning enhancement (preferences)

Based on the type of problems that users have to choose, it was expected that their selection of answers would focus on options 2, 4 and 8 (Questionnaire B – Question 2 in Appendix D). Again only six users correctly made their choices (i.e. similar with Questionnaire A). From these results, there was a slight increase in choosing option 2 (i.e. from 25 in questionnaire A to 29 in questionnaire B) whilst with option 4 and 8, there was a slightly decrease (i.e. from 44 to 41 and 13 to 11). This happened because some of the security warning enhancements that they received (i.e. security warning group D, G and H) offered limited information that was able to answer the current warnings context that users faced. Even though some of these results were not really convincing, the next ten questionnaire questions gave a different indication of the results.

The results presented in Table 7.21 were based on the questionnaire questions presented to them. The majority of users 26/50 selected “strongly disagree” and “mostly disagree” based on the median given. In terms of information contexts (i.e. easy to understand

and help to complete task), the majority selected “mostly agree”. These high percentage proportions indicated that with the security warning enhancement, the information was much more comprehensible and they even demonstrated that they had enough time to view the details. With this warning, the majority claimed it was easy to find the information presented. In addition, they also selected “strongly agree” to state that the interface of security dialogue was understandable.

Based on these results, the information provided in the security warning enhancement was seen to be more presentable and easy to be understood (i.e. new features or function). In terms of the help function, the majority selected “mostly agree” to indicate that it increased their knowledge and awareness with regard to the contents and features available. The final question revealed that the majority agreed that the security warning enhancement based on users’ preferences had all functions and capabilities that they expected to have (i.e. mode/median = 5).

Statements	Most frequent answer (n = 50)	Mode	Median
1. The security dialogue was too complex for me to understand	26 Strongly disagree	1	1
2. I spent enough time to view the information provided	16 Mostly agree	6	6
3. It was easy to understand the information provided	18 Mostly agree	6	6
4. The way information was presented helped me to complete the tasks	18 Mostly agree	6	6
5. I could effectively complete my task using the information presented	16 Somewhat agree	5	6
6. It was easy to find the information I needed	20 Mostly agree	6	6
7. The interface of security dialogue was understandable	19 Strongly agree	7	6
8. The security dialogue helped me to fix the problem in the way that I understood	15 Somewhat agree	5	5

Statements	Most frequent answer (n = 50)	Mode	Median
9. The available help increased my knowledge and awareness about the contents and features of the dialogue.	18 Mostly agree	6	6
10. This dialogue had all the functionality and capability I expected it to have	15 Somewhat agree	5	5

Table 7.21: Statistics on users’ decision with regard to security warning enhancement

Based on the overall findings, a significant number of users accepted the security warning enhancement better than the standard version of warning. Based on the line graph depicted in Figure 7.18, it can be seen that the security warning enhancement pattern (i.e. median (E)) was better than the standard security warning (i.e. median (S)). The median value had been used as the main comparison to indicate where the main results fluctuated around based on the overall 50 participants. In terms of the positive connotation group of questions in the enhanced version (i.e. question 2 to question 10), almost all of the depicted results performed better when compared to the standard warnings. Meanwhile, for the negative connotation group (i.e. question 1 - the security dialogue was too complex for me to understand), the security warning enhancement based on users’ preferences were better as most users claimed that they “strongly disagree”.

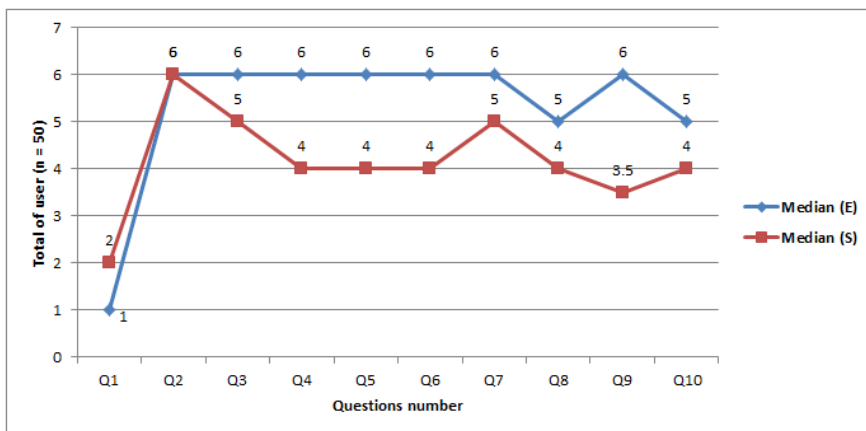


Figure 7.18: Comparison between standard vs. security warning enhancement (i.e. users’ preferences)

Therefore, when probing users with specific questions with regard to users' knowledge about the nature of security dialogues, the types of problem that occurred and some other related questions regarding usability issues, the majority demonstrated greater understanding of the enhanced version of the warning. The interview in section B probed this in further detail.

7.4.3.2.2 Interview B

After users had filled in the questionnaire, they were interviewed to obtain further details about the security warning enhancement that they received. Thus, the results of this section portrayed mixed answers as users were interviewed in relation to the security warning enhancement based on preferences that they had chosen in the first place (i.e. Table 7.19). In each of the questions, users' feedback referred to their main preference (i.e. Most of users gave more than one answer but the focus were given to their main decision). The following section highlights the interview findings in further detail.

Users' decision	Total responses (n = 50)
Concise risk level bar	11
New help options that are informative /relevant/ presentable	23
Simple language	3
Useful icon/symbol/questions	4
Unsure/Uncertain	5
About this file	2
View decision – Others people view	2

Table 7.22: What do you think of the feature(s) that are available to help you make a decision in this security warning?

Based on the results presented on Table 7.22, in general most users were happy with the new option features provided in the security warning enhancement (i.e. Guidance area, risk level, questions and answers link, signal icon and words and tooltips information). They demonstrated that more functions were helpful within this context of warning, when compared to the standard version.

Users' decision	Total responses (n = 50)
No. It is understandable	41
Guidance style box	1
File type	2
Source of publisher	2
Not sure	1
The presented link	1
What is the summary	1
What else should I know	1

Table 7.23: Were there any aspects of the warning that you found hard to understand or interpret?

When probing the elements that users found difficult to understand, the vast majority 41/50 selected “No. It is understandable” as shown in Table 7.23. However, nine other users were still confused about some of the available elements presented (i.e. guidance style box, file type, source of publisher, what is the summary and what else should I know). Some of them further clarified that the functions were pretty new to them. Therefore, it was quite difficult to understand the usage of such functions in the available time. With regard to the other users, most of them claimed that the risk level bar and the guidance area details were informative and helped with their decision making.

Users' decision	Total responses (n = 50)
Yes with technical jargon understood	43
No	2
I just ignored both	4
Not sure	1

Table 7.24: Do you understand the usage of signal icon/signal words in this security warning?

In terms of the usage of signal icons and signal words (the principal investigator gave an example to make them aware about the meaning/concept of signal cues), the vast majority demonstrated that they were understood, as shown in Table 7.24. Surprisingly, four respondents claimed that they ignored both elements. When further probed, they mentioned that it never affected them when making a decision because it was just an

image and word. One of them claimed that it always looked similar in all security warning, so he/she would not bother to pay attention. On the other hand, three respondents claimed “no” and “not sure” respectively.

Users' decision	Total responses (n = 50)
Yes/ Understandable/Straight forward/easier/better	45
No	5

Table 7.25: Do you understand the way information was presented, especially technical wording?

With regard to the way information was presented especially technical wordings on Table 7.25, again the majority claimed that it was understandable, straightforward, easier and even better when compared with the standard security warning. With the new guidance area, the majority of users claimed that the information provided within that frame helped to explain more appropriate details. Some of the respondents also claimed that the usage of tooltips was helpful in explaining quick information about the meaning of most of the features available in the security warning.

Users' decision	Total responses (n = 50)
Yes with enough options	33
Yes with limited options but can be improved	9
Not much options	8

Table 7.26: Do you feel that this security warning was presented with enough options to guide you?

When asked about their feeling as to whether enough options were presented to guide them, 33/50 claimed that they had enough options, 9 claimed they had limited options but could be improved and the remainder did not have many options, as shown in Table 7.26. For example one of the users suggested that there should be an option (e.g. button or link) for users to click to get the list of trusted and untrusted publisher names. Hence, it would be much easier to verify whom he/she should trust.

Users' decision	Total responses (n = 50)
Yes with fully satisfaction	40
Partially satisfied	7
Not satisfied	3

Table 7.27: Do you feel satisfied with help available for this warning?

The final set of question asked about users' satisfaction with the help function available within the security warning enhancement context. 40/50 respondents were fully satisfied, whilst the remainder were partially satisfied or not satisfied, as presented in Table 7.27. Three respondents claimed that the security warning enhancement they received were rather complex to understand. There were more links to click (i.e. more actions to be taken) and this led to time constraints.

Based on the overall results, it can be summarised that end-users were satisfied with the security warning enhancement based on users' preferences, when compared to the standard security warning. They had demonstrated positive results in most of the questions presented. More useful features were available in the security warning enhancement that helped them to make a decision. In terms of the way information was delivered (i.e. technical wordings), the vast majority were clearly satisfied. On the other hand, users agreed that the security warning enhancements had enough options and they were satisfied with the options available. Therefore, this gave a clear indication that users were happy to receive security warning enhancements based on their preferences. In the next section, a detailed comparison was made to compare users' experienced between usage of the standard security warning and the adapted warning version.

7.4.4 Comparison of the standard security warning and the adapted warning

Comparisons can be made between users' performance after being presented with the standard security warning and the adapted warning version. In order to make a useful comparison, this thesis focused on 30 respondents that had experienced the same security warning enhancement as depicted in Table 7.19. This meant that 30 users who had chosen preferences that produced a complete security warning enhancement/adapted warning became the focal point of this section. As these users had common ground in terms of experiencing similar standard and enhanced security warnings, it is

fair to make a comparison of each of the ten presented questionnaire questions in the next section.

7.4.4.1 Demographic detail comparison

In terms of general users' demographic background (n = 30), comparisons were made based on age and computing skills as presented in Figure 7.19 and age and education background in Figure 7.20.

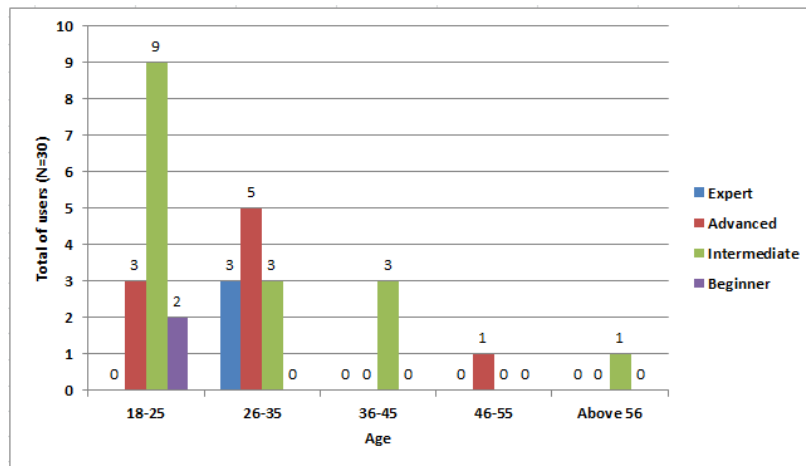


Figure 7.19: Demographic comparison age and computing skills.

It can be revealed that the majority of users classified themselves as intermediate 16/30, advanced 9, expert 3 and beginner 2 respectively. In terms of age classification, the majority were from the age range of 18-25 years old. Interestingly, these results also presented at least one representative from each age group.

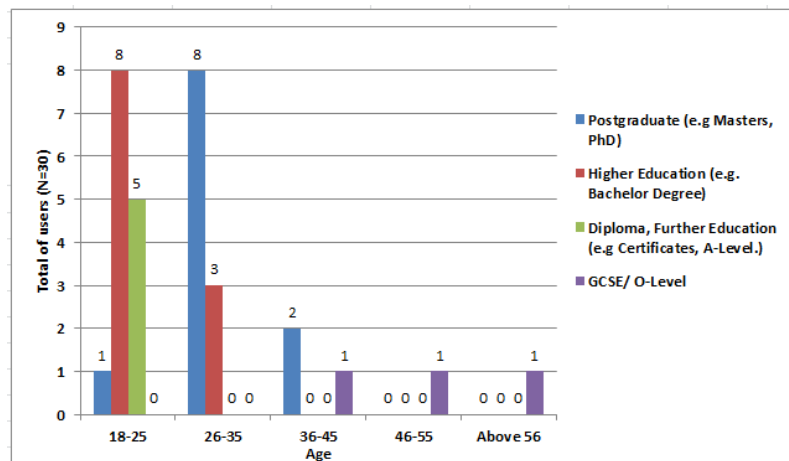


Figure 7.20: Demographic comparison age and education background (n = 30).

In terms of education background from these 30 participants, there was an equal split between postgraduate and higher education from two age groups (i.e. 18-25 and 26-35), whilst the remainder had a diploma or further education and/or at least GCSE/O-level education. From this demographic data, the sample study was derived from all age group ranges from various educational backgrounds, which is very useful in terms of data segregation. As this study was well promoted in the university environment, respondents were generally derived from a postgraduate and undergraduate background which indicates that the majority of them were students or members of staff. Overall, most of the respondents can be considered to have familiarity with computing technology based on their computing skills capabilities and also good education background (i.e. education from college or university).

7.4.4.2 Pre-warning (standard) and Post-warning (adapted)

The comparison was made by looking at pre-warning and post-warning user performance in terms of the ten questions presented in the questionnaire section in Table 7.28. Pre-warning referred to standard security warnings whilst post-warning referred to the adapted warning. Pre-warning had a particular look at users' experienced with standard security warning that they had encountered in task 7 (i.e. it will be repeated again in section 3 of the user study). Post-warning was related to users experience with security warning enhancement based on user preferences (i.e. the adapted warning). Therefore, users experienced both warnings and were able to assess, evaluate and later compare warnings.

From Table 7.28, it shows the comparison between the pre-warning (standard) and post-warning (adapted) based on the likert-scale values with ten questions. In addition, this table utilises a comparison using mode and median values which was based on descriptive statistical analysis. The mode values represent the preference action by users whilst the median values constituted the central tendency from the overall 30 respondents. Having identified the mode and median, indication was given as to where the users' preferences on the likert-scale scoring lay. Therefore, the degree of thought on their part could be gathered as the main outcome of this study.

CHAPTER 7: EVALUATION AND VALIDATION OF THE AUTOMATED SECURITY INTERFACE ADAPTATION (ASIA)

Statements	Standard							Adapted							Standard		Adapted	
	1	2	3	4	5	6	7	1	2	3	4	5	6	7	Mode	Median	Mode	Median
1. The security dialogue was too complex for me to understand	10	7	6	4	3	0	0	15	9	3	0	1	0	2	1	2	1	1.5
2. I spent enough time to view the information provided	0	3	2	2	6	11	6	1	3	2	5	6	6	7	6	6	7	5
3. It was easy to understand the information provided	0	2	5	3	9	6	5	0	1	2	0	4	11	12	5	5	7	6
4. The way information was presented helped me to complete the tasks	0	6	5	8	4	6	1	0	1	0	1	7	12	9	4	4	6	6
5. I could effectively complete my task using the information presented	0	6	3	9	3	7	2	0	1	1	0	9	10	9	4	4	6	6
6. It was easy to find the information I needed	1	7	9	5	4	3	1	0	1	1	1	3	16	8	3	3	6	6
7. The interface of security dialogue was understandable	1	3	6	4	5	6	5	1	0	2	2	4	10	11	3,6	5	7	6
8. The security dialogue helped me to fix the problem in the way that I understood	2	8	4	5	4	5	2	0	1	1	4	7	9	8	2	4	6	6
9. The available help increased my knowledge and awareness about the contents and features of the dialogue.	2	7	6	4	4	5	2	1	1	0	1	8	10	9	2	3.5	6	6
10. This dialogue had all the functionality and capability I expected it to have	1	6	5	8	3	4	3	0	0	3	5	9	7	6	4	4	5	5

Table 7.28: Comparison table between pre-warning (standard) and post-warning (adapted)

From the results, in general, neither of the security warnings was complicated for users to understand, as both mode and median values were in the range of one to two. In terms of enough time spent to view information provided, users demonstrated that they spent their time better in standard security warning. One possible reason was that the size of the warning was smaller, and contained less information compared to the adapted version. Thus, users might easily read the available information. However, with regard to the other questions, the security warning enhancement performed better based on the mode and median values. The details of the comparison are explained on the next section.

In terms of the detailed comparison, both performances were plotted by line graph as shown in Figure 7.21 and Figure 7.22. From the results, there was a pattern demonstrated by the users. In the standard security warning, the plotted line results were distributed almost evenly compared to the adapted warning results. With the adapted warning, the distribution was mostly scattered to the right (i.e. somewhat agree, mostly agree and strongly agree). It can be noted that if the distribution is scattered

more to the right it indicates a better user acceptance and vice versa for the distribution on the left.

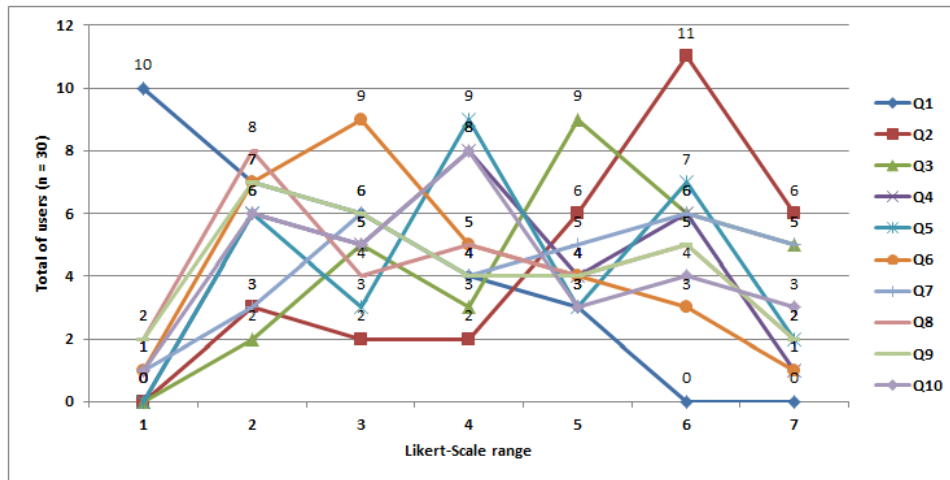


Figure 7.21: Users' performance score on 10 questions with regard to the standard security warning

Based on this observation, the majority of users demonstrated their acceptance of the adapted warning version with more positive attributes (i.e. values more than four in the likert-scale). However, with regard to the standard security warning, users generally demonstrated that they were almost equally split between the likert-scale values (one to three) and (four to seven). Based on the trend from the questions, respondents still struggled with the current usage of standard security warning, albeit they were more familiar with this version of the warning compared to the adapted warning.

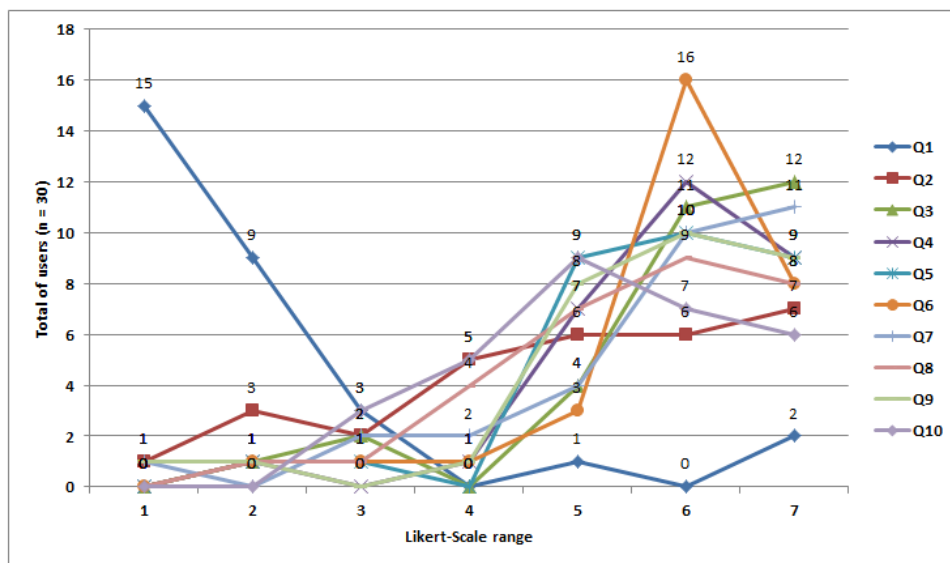


Figure 7.22: Users' performance score on 10 questions with regard to the adapted warning

Having understood this comparison, the next section presenting detailed comparison focused on the evaluation of one-to-one questions (i.e. one to ten).

7.4.4.3 Detailed comparison of one-to-one questions

This section presented a more specific comparison of user performances on each of the presented ten questions. The comparison was presented by a line-graph, on a one-to-one basis ($n = 30$). By looking at these one-to-one comparisons, the evaluation and validation process may be explained with clarity and sufficient empirical evidence may be provided to support the findings and the proposed architecture. In addition, based on these comparisons, a Chi-square test is presented to examine the difference between having the standard and the security warning enhancement (adapted warning). According to McCrum-Gardner (2007), Chi-square test is used as a comparison of more than two groups. Key (1997) further explained that the differences are related to the actual sample and another hypothetical or previously established distribution. Therefore, from the results that had been gathered, this section compares each of the ten available questionnaire questions using a Chi-square test. Having said this, the seven likert-scale values (Figure 7.17) were grouped into three classifications, as follows:

- i. Likert scale range from 1-3 is equal to **No**
- ii. Likert scale value four is equal to **Neutral**
- iii. Likert scale range from 5-7 is equal to **Yes**

The rationale for this classification was that these likert-scale ranges were to ensure that the analysis could be presented in a better focus because the collected sample size ($n = 30$) can be considered small (refer to Appendix D for the full test results of Chi-Square (X^2) Test).

It may be noted from Figure 7.23 that users demonstrated almost a similar fluctuated pattern from both warnings. Half of the overall responses 15/30 (adapted warning) chose “strongly disagree” with regards to the complexity of warning dialogue, compared with 10/30 for the standard security warning. This indicated that a significant number of users had experienced a more user-friendly dialogue with the adapted warning. One surprising finding can be noted with two users who claimed “strongly

agree” with the complexity of the adapted version of warning. A possible reason that contributed to this was that the users did not have exposure or familiarity with the usage of this security warning before. In addition, with the adapted warning more information was depicted (i.e. guidance area) and more features were introduced. Therefore, with lack of experience in terms of its usage (i.e. temporarily used in the prototype software), this might contribute to the reasons why users experienced difficulty with the adapted warning. With regard to Chi-Square test result (i.e. $X^2 < 5.991$ where $X^2 = 4.32$), there is no significant difference between the standard and adapted warnings that users encountered. Thus, it can be suggested that most of the respondents considered that both warnings were not too complex for them to understand.

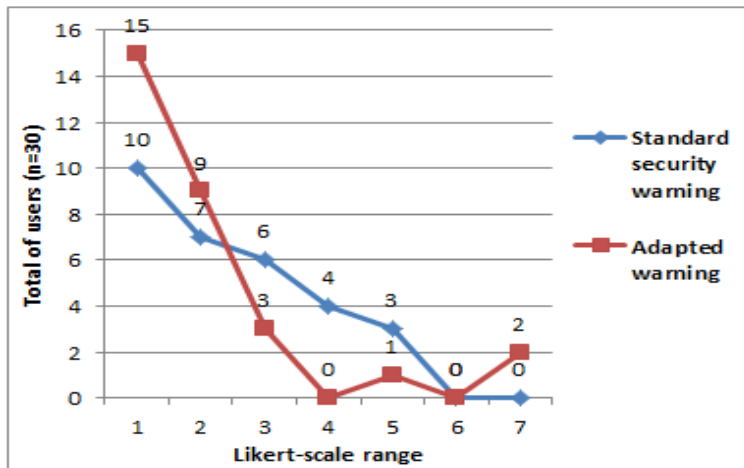


Figure 7.23: Comparison of “The security dialogue was too complex for me to understand”.

In terms of viewing the information provided users spent enough time with the standard security warning compared to the adapted warning based on Figure 7.24. The comparison was made based on the assessment with positive likert-scales (i.e. 5-7 range). 23/30 had chosen the 5-7 range with the standard warning compared to 19/30 with the adapted warning. One observations can made from this finding, namely that users need to spent more time on the adapted warning as it involved clicking few hyperlinks (to navigate to sections within the same dialogue). As this prototype software was conducted within a time constraint (i.e. users might feel not sufficient time to view). It may have significantly impacted on the findings. With regard to the Chi-square test result (i.e. $X^2 < 5.991$ where $X^2 = 1.76$), there is no significant difference between the warnings. This is interesting because the layout of both warning was

totally different especially in the adapted warning version (i.e. as it provided more function and information) but surprisingly was not significant statistically.

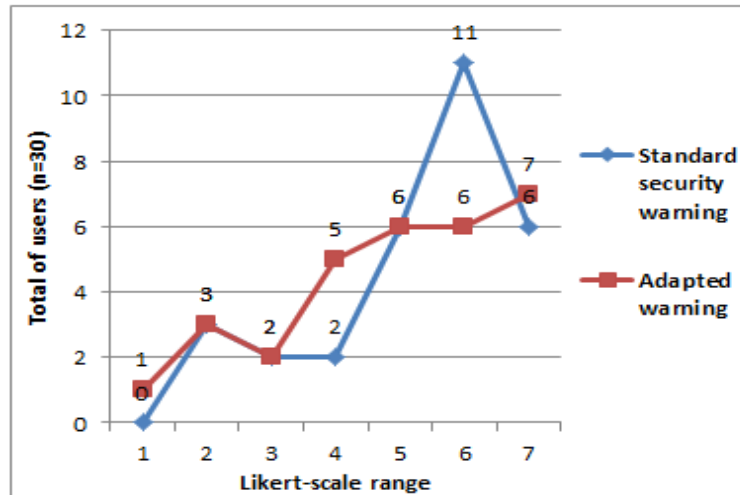


Figure 7.24: Comparison of “I spent enough time to view the information provided”

In terms of the simplicity of understanding the information provided, users demonstrated better understanding of the adapted warning compared to the standard version as depicted in Figure 7.25. 23/30 respondents selected “mostly agree” and “strongly agree” with the information provided by the adapted warning. This indicated that the information provided was significantly improved and worked better for end-users, especially with the guidance area. By introducing the questions and answers (i.e. via hyperlink), users were presented with information within the same page. To a certain extent, users were able to see others’ peoples decisions based on the provided link. With regard to the standard security warning, only 11/30 indicated the ease to comprehend the information provided. One observation that can be made was that users were required to click the link in the footnote area in order to get more information (i.e. in order to receive the help dialogue box). Even if they had viewed the available help, too much information was depicted at the same time. With this help of the dialogue box (i.e. context sensitive help), users were brought to the specific information that dealt with the current state of the application. In Windows XP the information provided on the help dialogue was not sufficient compared to Windows 7 (i.e. far more comprehensive) as shown in Figure 7.26. With regard to Chi-square test result (i.e. $X^2 < 5.991$ where $X^2 = 5.64$), there was no significant difference between both warnings. However, more users regarded the adapted warning as easier.

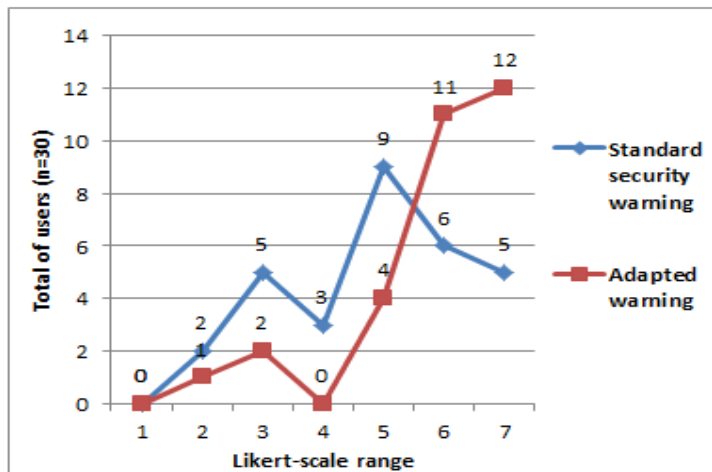


Figure 7.25: Comparison of “It was easy to understand the information provided”

In Windows 7, the approaches to present help were almost similar with the proposed technique in the adapted warning. However, the main differences were based on how the help function was used and the level of information provided. In the proposed method, when the help button was clicked, a new security warning enhancement was generated (i.e. it encourages users to click help by default) and the guidance area was presented. Users were presented with useful information on the summary page. When a link was clicked (i.e. list of questions), users were brought to a specific section within the same dialogue to answer the question that users would like to explore. All the information was embedded together, rather than presented in a new dialogue box.

With the help dialogue box from Windows 7, there were many listed questions and answers presented to users, rather than specific ones. Some of the presented links even provided too much information, rather than providing simple and concise answer (e.g. when users click what are the risks when downloading files?). However, it can also be noted that this version had significantly improved and worked better, compared with the previous version in Windows XP (i.e. the improvement with ask function, survey elements and instant help search function). The approach to question and answer styles was adopted in the proposed framework (i.e. presented with five questions only as noted in guidance area).

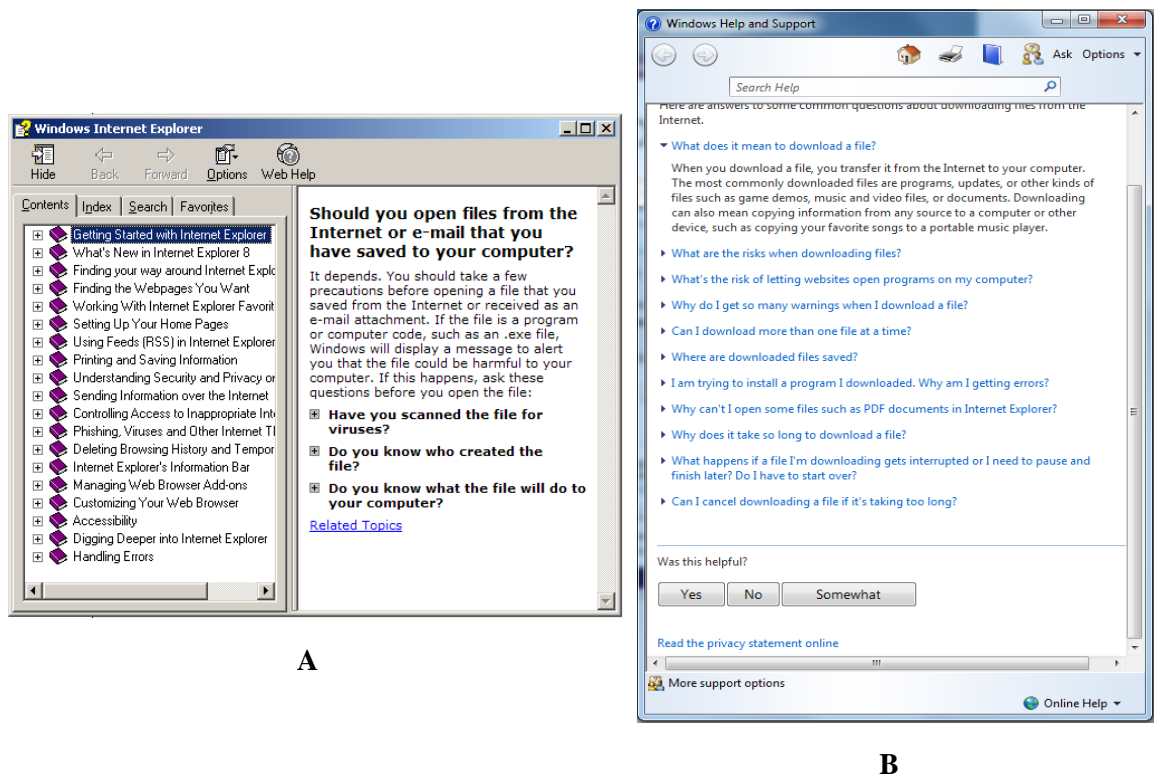


Figure 7.26: Help dialogue box in Windows XP (A) and in Windows 7 (B)

A consistent result was demonstrated by users with regard to the information provided which helped them to complete the tasks as depicted in Figure 7.27. 28/30 respectively chose the positive likert-scale (i.e. 5-7 range) in the adapted warning, this was better than the standard version. From the results, it may be seen that eleven users chose “mostly disagree” and “somewhat disagree” with the standard warnings, whilst only one user in the adapted warning chose “mostly disagree”. This indicated that users were facing more difficulties with the standard warning in relation to the information provided to help them complete the tasks. Based on the Chi-square test result (i.e. $X^2 > 5.991$ where $X^2 = 21.19$), there was a highly significant difference between the standard and the adapted warning with regard to the way information was presented to complete the task.

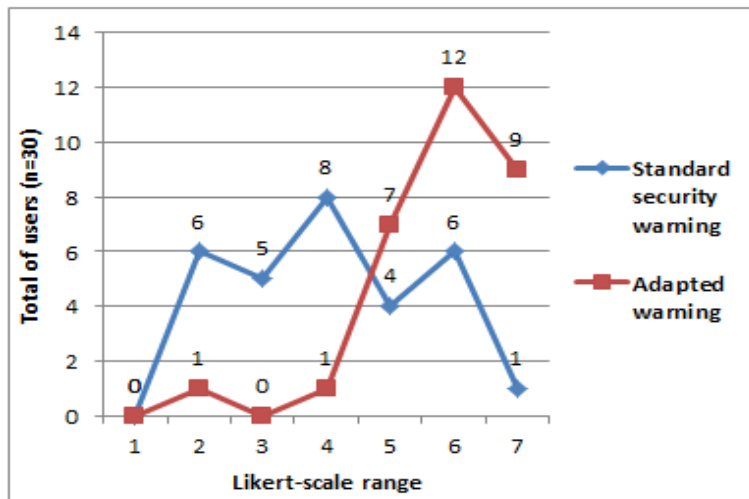


Figure 7.27: Comparison of “The way information was presented helped me to complete the tasks”

Again, a similar pattern of results was portrayed in Figure 7.28, in which 28/30 chose the positive likert-scale (i.e. 5-7 range) claiming they can effectively complete the task by using the information provided in the adapted warning compared with only 12/30 with the standard warning. Only two users selected “mostly disagree” and “somewhat disagree” with the adapted warning, compared with nine users with the standard warning. With regard to the Chi-square test results (i.e. $X^2 > 5.991$ where $X^2 = 19.85$), there is a significant difference between both warnings, where the vast majority of users preferred the adapted warning compared with the standard version.

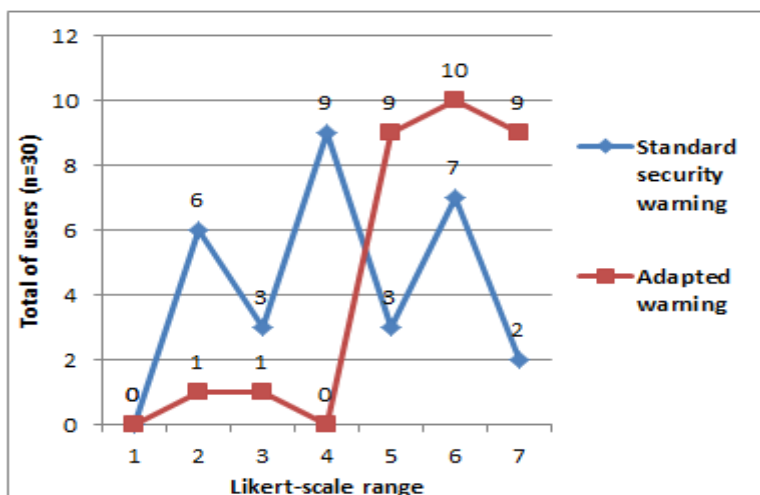


Figure 7.28: Comparison of “I could effectively complete my task using the information presented”

In terms of the ease of finding information, Figure 7.29 shows that 27/30 users positively accepted the adapted warning whilst only 8/30 with the standard warning based on the positive likert-scale (i.e. 5-7 range). As discussed earlier, with the adapted warning, each part of the information provided specifically in the guidance was presented using a question and answer format (i.e. based on Baecker et al. 1995). This technique helped users to get the answers straight away, as the questions listed were based on the question that users normally asked when performing task. On the other hand, Chi-square test results (i.e. $X^2 > 5.991$ where $X^2 = 24.82$) revealed that there was a highly significant difference between both of these warnings in terms of the fact that it was easy to find information that users needed. Therefore, it can be suggested that the vast majority 27/30 of users found it was easier to find information in the adapted warning compared with the standard warning.

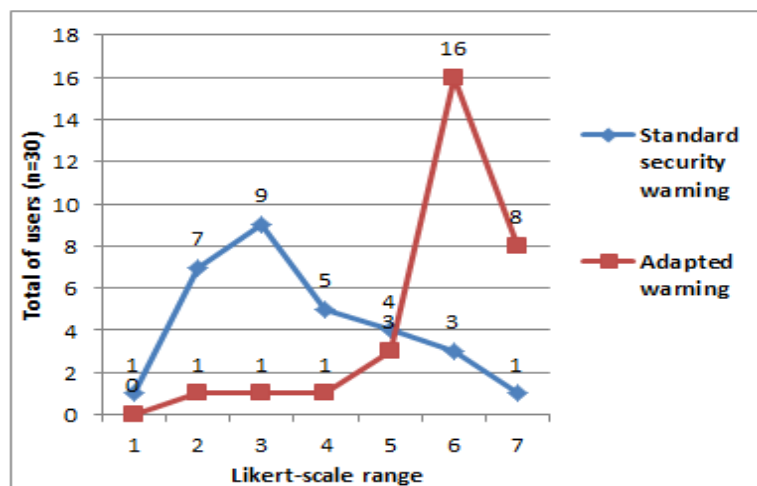


Figure 7.29: Comparison of “It was easy to find the information I needed”

On the other hand, in terms of the comprehensibility of the warning interface, 25/30 respondents chose the positive likert-scale (i.e. 5-7 range) with the adapted warning whilst 16/30 with standard warning as shown in Figure 7.30. Ten users claimed that the standard security warning was difficult for them to understand, whilst only three users with the adapted warning based upon likert-scale (i.e. 1-3 range). With regard to the Chi-square test result (i.e. $X^2 > 5.991$ where $X^2 = 6.41$), there is a significant difference in both warnings in terms of comprehension of the interface of warning dialogue where most respondents decided that the adapted warning was more understandable when compared to the standard warning.

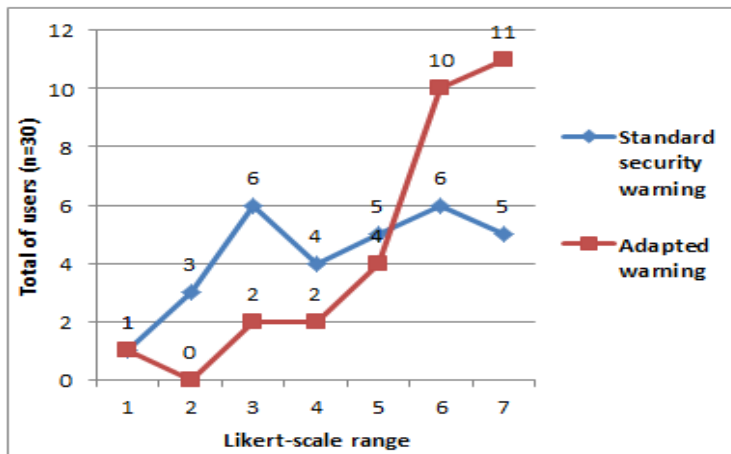


Figure 7.30: Comparison of “The interface of security dialogue was understandable”

Users then demonstrated that the adapted warning helped them to fix the problem in a way they understood, where 24/30 selected “somewhat agree” to “strongly agree” with the adapted warning whilst only 11/30 with the standard warning dialogue as shown in Figure 7.31. With the adapted warning, the flow was increased consistently except for the last part, whilst, with standard warnings, the line graph fluctuated and the top peak was recorded as “mostly disagree” with regards to helping users to fix the problem in a way they understood. On the other hand, with regard to the Chi-square test result (i.e. $X^2 > 5.991$ where $X^2 = 13.94$) it can be revealed that there is highly significant difference between standard and adapted warning in how the security dialogue helped users to fix problems in a way they understood. It can be revealed that 14/30 selected “No” (i.e. likert scale 1-3) on the standard warning whilst only 2/30 with the adapted warning. It can be suggested that users experienced greater difficulties in the standard warning compared to the adapted warning.

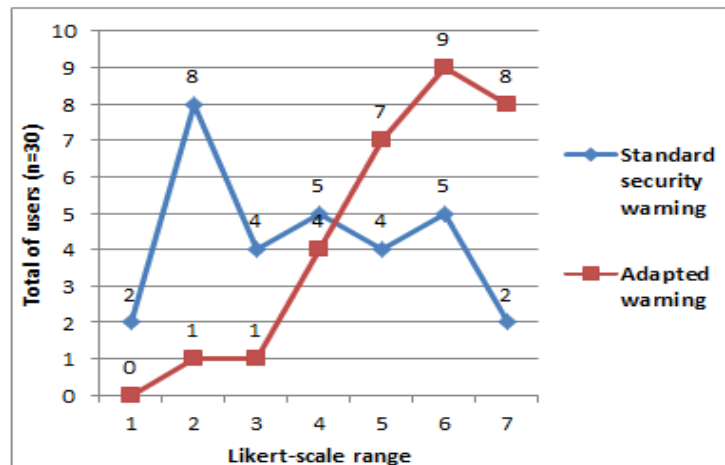


Figure 7.31: Comparison of “The security dialogue helped me to fix the problem in the way that I understood”.

In terms of the help features, 27/30 indicated that the adapted warning was able to increase their knowledge and awareness with regard to the contents and features of the dialogue based on the likert-scale (i.e. 5-7 range) whilst only 11/30 with standard security warning as portrayed on Figure 7.32. Even though the vast majority were generally satisfied with the help available, surprisingly one user still selected “mostly disagree”. With the adapted warning, the overall presentation had been improved in order to communicate the risk effectively and guide users to make a secure decision. Hence, users demonstrated that they accepted the adapted warning far better than the standard warning. Meanwhile, the Chi-square test result (i.e. $X^2 > 5.991$ where $X^2 = 18.48$) revealed that there is highly significant difference between both warnings in terms of has the available help function helped to increase user’s knowledge and awareness of the content and features. With a standard warning, 8 users selected neutral whilst only five users in the adapted warning. Again, the majority agreed with the statement, especially with the adapted warning version.

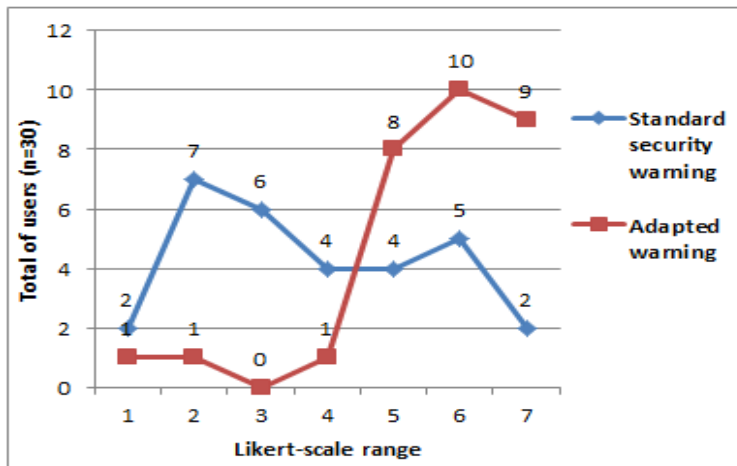


Figure 7.32: Comparison of “The available help increased my knowledge and awareness about the contents and features of the dialogue”.

The final question may be considered as the summary of overall users’ experiences with security warning as shown in Figure 7.33. It can be revealed that 22/30 respondents claimed that the adapted warning based on their preferences had all the functionality and capability they expected to have whilst only 10/30 selected the same for the standard security warning based on the likert-scale (i.e. 5-7 range). The Chi-square test results (i.e. $X^2 > 5.991$ where $X^2 = 10.59$) revealed that there is a significant difference between the standard and the adapted warning in terms of the dialogue having the functionality and capability that users expected it to have. It can be suggested that generally most of the users were able to distinguish the differences from both warnings. Thus, it can be discovered that the adapted warning provided better content and features in order to compare with the standard warning.

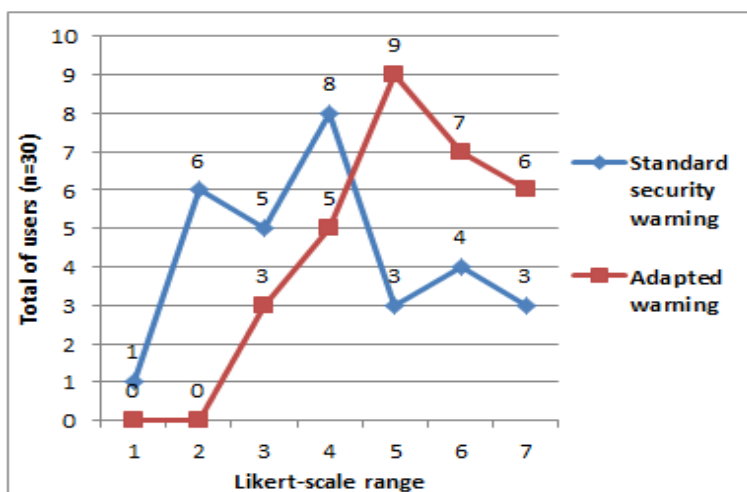


Figure 7.33: Comparison of “This dialogue had all the functionality and capability I expected it to have”

In summary, nine out of ten questions were significantly positive towards the security warning enhancement (adapted warning) based on user preferences (i.e. except on question 2). However, with regard to the Chi-Square results, it can be revealed that (7/10) questions were significantly different statistically in terms of users' decision in comparing the standard and the adapted warning. This evaluation was based on users' experience with the standard security warning and the adapted warning based on their preferences. Even though the experience of each warning can be considered temporary (i.e. via prototype), it gave one clear indication of how security warnings can be improved based on users' need. In addition, this opened a new dimension for integrating help information together with the warning dialogue (i.e. via adaptation). Even though not all users preferred with the full version of the security warning enhancement (adapted warning), all users had a chance to experience it. Therefore, it gave users the opportunity and equal chance to feel and to make a comparison later on. Based on the presented results at this stage, end-users demonstrated that they were positively inclined towards the security warning enhancement (adapted warning) based on the presented question which comprised the end-users satisfaction, perception and understanding of the overall presentation of security warnings. The next section presents further details with regard to the usability aspects which continue the aims of this research study.

7.4.4.4 Usability questions

The final section of this user study was an interview in relation to usability which comprised effectiveness, efficiency and user satisfaction of the usage of security warnings. This technique was derived from Herzog and Shahmehri (2007) who published the comparison analysis of user help techniques based on security and usability criteria. The evaluation of usability was conducted in a general sense, rather than a detailed assessment as the prototype software presented referred to one scenario only. For example, the time that user took using the standard security warning compare with the security warning enhancement (adapted warning) was not measured. However, users had been told to make a comparison in terms of the time involved in the decision making process. The need for usability with this user study was to ensure that the adapted warning (i.e. by the usage of software) could be considered efficient to them.

As usability is closely related to user friendliness (Faulkner 2000), in order to strengthen the outcome of this user study, the author believed that understanding users' assessment on usability aspects is needed. Therefore, a comparison was made for each usability element and specific questions were asked and users were required to justify their reasons as well (i.e. effectiveness, efficiency and user satisfaction).

After assessing usability elements, users were asked their main preference between the standard security warning or the adapted warning and the reasons for their choice. Although only 30 users had chosen the adapted warning, the remaining twenty users were told to make a comparison based on the adapted warning as well. It can be noted with regard to these twenty users, they also had equal opportunities to experience the features and functionality of the adapted warning as well although this warning was generated for them on the first place (i.e. based on users' preferences) (refer to section 7.4.3). This was to ensure that evidence can be gathered from overall views of respondents (i.e. $n = 50$) rather than generalisation from part of the sample. Before ending the session, users were asked whether they had any thoughts on the method to improve the current implementation of security warnings (i.e. based on standard warning and enhancement warning that they had seen). Lastly, they were asked if they wished to give any comments in relation to this study. The lists of questions presented to users are shown in Table 7.29.

Questions (n = 50)	Comparison Elements	Standard Security Warning	Adapted Warning
1. Which of security warnings able to provide effective solutions for you to make a decision? Why?	Effectiveness	2	48
2. Which of security warning able to guide me through to make a safe decision? (i.e. in terms of time involved) Why?	Efficiency	2	48
3. Which of this would be easy for you to use? Why?	User satisfaction	2	48

Table 7.29: Comparison of usability elements and users' preferences

When users were presented with question 1 in relation to effectiveness, 48/50 users claimed the adapted version was more effective compared to the standard version. The reasons for their choices are presented in Table 7.30.

Reasons	Total responses (n = 48/50)
Adequate information for me to understand	20
Suitable for all level of users	4
Estimation of risk levels	11
Statistical details	6
Clearer terminologies and understandable	7

Table 7.30: The reasons on choosing the adapted warning (effectiveness)

The majority of users claimed that the adapted warning dialogue provided adequate information for them to understand. This answer generally covered some other elements that could refer to the “adequate information” such as the risk level, statistical details and simple terminology. Users mentioned specifically how with the adapted warning, the risk level was able to convince them in a better way to understand the problem they encountered (i.e. able to communicate the risk) and the guidance elements in the dialogue guided them thoroughly to make better decisions. Users also realised with the adapted warning that all useful information was depicted in the same dialogue rather than be presented in a new dialogue box. With regard to the two users who preferred standard security warning, they claimed that they were familiar with that version, and thought it was simpler. They simply wanted to make a quick decision and they also ignored warnings most of the time. When probing their decision, they mentioned that with the adapted warning, it was still good, but they suggested it would be more useful to be used for people without technical background.

Reasons	Total responses (n = 48/50)
Informative descriptions/Useful information/Guidance	25
Improved layout	3
Risk level well informed (e.g. colour code bar)	10
More precise and convincing	3
Informed decision	7

Table 7.31: The reasons on choosing the adapted warning (efficiency)

The second question was asked in relation to efficiency (the time involved with regard to making a safe decision). As expected, the majority 48/50 of users preferred the adapted warning with their reasons shown in Table 7.31. From this result, all functionality provided in the warning was able to help them to comprehend the problems and later guided them to make decisions in adequate time. The risk level bar made them pay more attention to the colour coded bar and therefore they could make a quick decision merely by looking at this feature. The guidance area provided questions and answers as a guiding interface for users. In addition, the signal icons or words were used in a reasonable way (i.e. as in Microsoft Guidelines). Therefore, users were able to make better judgements in their decision processed. Users mentioned that they had to use more time with this warning because all information was allocated in one dialogue. Meanwhile, with the standard warning, they would make a quicker decision if they did not click the link at the bottom. However, the vast majority were happy with the adapted warning as this was seen to provide better layout and guidance for users' comprehension and for the sake of security and protection of the users' computer.

2 users claimed that the standard security warning was more efficient highlighting the familiarity issue. As they got used to the previous version, they considered the new security warning as not efficient because the information was too much for them. When further probe, one of the respondents mentioned that they considered themselves immune to security warning (i.e. it was just a warning and they believed nothing bad happened based on their experience receiving warnings on a daily basis). However, they still appreciated the value of the information provided, which might be able to help other people who need it most, such as non-technical people.

Reasons	Total responses (n = 48/50)
Guidance elements that able to help making decision	9
Simplified and informative	19
Better layout and user friendly	5
Risk level options	9
Statistics on users' action	6

Table 7.32: The reasons on choosing enhancement security warning (user satisfaction)

The final part of the usability questions was related to user satisfaction. Effectiveness and efficiency normally will influence user satisfaction. According to Herzog and Shahmehri (2007) an additional factor that influences user satisfaction is empowerment. Empowerment is achieved when users are supported in achieving something that they are unable to handle. Even though this thesis did not ask specifically about empowerment, the author believed that with the proposed method of security warnings (i.e. the adapted warning), empowerment was accomplished. For instance, security warnings were improved with new features such as the risk level bar, matching icon and wording, tooltips information, question and answer style questions. It is expected that this element can be assessed in future research.

The next step was to evaluate user satisfaction. It may be noted that consistent answers were demonstrated by all 50 respondents, as 48/50 were more satisfied with the adapted warning. The reasons for their choices are presented in Table 7.32. The majority agreed that the adapted warning was simplified and more informative. Some suggested that the warning presented enough information (i.e. less to read) because the information had been classified accordingly in the guidance area. The risk was communicated better informing users before they made their decisions. Even though users had not experienced this warning in a live system, it gave a clear indication of how a security warning would be able to satisfy users' need in relation to the presentation of warnings. Overall, users demonstrated a positive preference for the adapted warning. Designing warnings that cater to end-users' requirements are important so that they are able to understand and react accordingly. This also indicated that users were satisfied with the new functions that were used in the proposed warnings, as the vast majority provided reasons by demonstrating the usefulness of the available features to help and guide them.

After the evaluation and the validation of the overall steps within this user study, users were asked about their main preference for the security warnings they received. Based on their experience with the standard security warning and the adapted warning, they were required to make a choice and justify their reasons. The majority 46/50 opted for the adapted warning compared with the standard security warning. Even though users consistently preferred the adapted warning in the usability questions (i.e. effectiveness,

efficiency and user satisfaction) the final verdict was portrayed slightly differently (i.e. from 48 to 46 respondents). Therefore, it is useful to further evaluate this change.

Table 7.33 presents the reasons for user preferences with the adapted warning compared to the standard security warning. The majority claimed that the new warning was simple, informative, visually attractive and contained all necessary information in one place. Some of them even highlighted that it was suitable for all levels of users.

Reasons	Total responses (n = 46/50)
Simple and informative/simplified	17
Visually attractive (e.g. risk level bar)	13
Suitable for all level of users	3
All information in one place	11
Secured	2

Table 7.33: The reasons on choosing enhancement security warning (preference)

The four users who preferred to have the standard security warning were three male and one female user respectively. All of their decisions are presented in Table 7.34

	Effectiveness		Efficiency		User Satisfaction	
	Standard	Adapted	Standard	Adapted	Standard	Adapted
User 1	✓			✓		✓
User 2		✓	✓			✓
User 3		✓		✓		✓
User 4		✓		✓		✓

Table 7.34: 4 users' decisions on usability set of questions

It can be observed that the majority of them still preferred the adapted warning when they were presented with the set of usability questions. Only two of them chose the standard security warning (i.e. with regard to effectiveness and efficiency) whilst the rest selected the adapted version. When further probing this group of users, most of them mentioned that they were happy with the adapted security warning, but they still preferred the standard version. However, users 1 and 2 claimed that the information provided in the warning was too much for them to read. In addition, familiarity became

one of the biggest factors that made this group of users remain with the standard warning. However, it can be noted that all of these users were very satisfied with the adapted warning when they were asked with regard to their satisfactions level (additional questions by principal investigator). 3/4 users suggested that the adapted warning is more suitable for people who are still new users of their computer. They also believed that it was still useful for any level of user to have this warning, as more useful information was provided and it helped users to be more cautious.

Reasons	Total responses (n = 50)
Incorporate the features to antivirus company	3
State the amount of people who proceed with options rather than percentage	3
Explanation on type of file in details	3
More help links	2
Reduce the guidance area size	1
Do not use technical jargon	1
Flashing to indicate high risk	1
Pie chart should provide expert advice rather than general public	2
Improve security warning icon to more meaningful or try to standardise it	8
Using less wordings	1
Computer system should be able to make a decision on behalf of users	2
Enough information provided	23

Table 7.35: Other suggestions to improve security warnings in general

After this, the principal investigator asked users if they would like to suggest other elements that might be needed to improve security warnings. Therefore, Table 7.35 lists some suggestions from end-users with regard to their suggestions to improve security warnings. The majority of users claimed that an essential element that should be presented in one particular warning was an adequate level of information. Therefore, information should be able to inform end-users and able to convince them to make a good judgment before proceeding with any possible action. One interesting finding

from this was that one user suggested that a flashing indicator should be used to highlight the severity of risk, so that they would know straight away something needs to be done.

Viewing others' decision feature was also highlighted by users as it helped them to see what others did. However some users claimed that the statistical information was still not very clear and suggested instead that showing the percentages of how many people had executed the file and cancelled the operation, would be useful if statistics sharing decisions made by expert users and the decision based on the successful rate of the execution of the file (i.e. without any malware detection) which some of them claimed would be more convincing. In addition, three respondents even suggested that this function could be integrated with an antivirus company to gain more trust from end-users. Two users suggested that the pie chart should be provided with expert advice only rather than the general public. They believed that following an expert path would be much more useful and more trusted. The final part of the interview asked if users wished to give some opinions or comments about this study. Most of them were satisfied and happy with the way the user study had been conducted.

7.5 Final observations

In Chapter 2, the author made use of the two recommended strategies by Cranor (2008) to build a secure system so that human beings could use it as follows:

- i. To build systems that are intuitive and find methods to make it easy to use
- ii. To teach humans how to perform the security critical task

Therefore, the author believed that ASIA accomplished both of these strategies based on the presented results within this chapter where it can be revealed that end-users significantly preferred to use the adapted warning compared with the standard security warning. The prototype was developed to evaluate and to validate the architecture proposed in Chapter 6. The next two sections describe the two observations that can be made with regard to the aims of ASIA and the "combined approach" that was proposed in ASIA.

7.5.1 Automated Security Interface Adaptation aims – Validation

As discussed in Chapter 6, ASIA proposed the aims presented in Table 7.36. Therefore, based on the results presented within this Chapter 8, the table describes the level of achievement based on the listed aims.

Aims	Supporting evidence	Descriptions
To adapt the presentation of security warnings based on user preferences	Chapter 3, 4 and 5 highlighted problems with regard to security warnings. This chapter provided an evaluation and validation based on a user study utilising a software prototype.	Evidence suggested that the majority of users (46/50) prefer to have the adapted warning rather than standard security warning.
To improve the usability (i.e. effectiveness, efficiency and satisfaction) of security interactions	Section 7.4.4.4 provided the evaluation and validation process with regards to the usability aspects.	Evidence suggested that 48/50 respondents consistently opted for the adapted warning with regard to the usability features.
To increase users' comprehension of security warning dialogues before making a decision by enhancing the available help	Section 7.4.3 for described the assessment of the adapted warning.	Evidence suggested that in most cases, users chose the positive likert-scale range as compared to the standard warning.

Table 7.36: Aims of ASIA validation

Based on the results presented in this whole thesis, and specifically in Table 7.36, it is clear that all the aims presented were achieved and validated. Even though the final aim of promoting a secure decision making process by enhancing the help feature was not encouraging (i.e. 16/50 clicked help), users were asked to try the new function embedded in the help button. After users had experienced this, it can be revealed that the vast majority preferred the adapted warning. Therefore, they now realised the new concept of help (i.e. the main questions and useful information embedded together in

one dialogue) that had been presented to them (i.e. results as presented in sections 7.4.3 and 7.4.4). In the next section, the validation process is presented, so as to compare various help techniques and the technique that were embedded in ASIA.

7.5.2 Usable help technique – Validation

In Chapter 2, a table of comparison was presented with a “combined approach” column, with the “maybe” justification on each question (i.e. pending upon evaluation and validation) as depicted in Table 2.5. This section provides the results of the validation process based on the presented evidence. ASIA made use of the combination approach from other users help techniques. Based on the comparison in Table 7.37, it may be noted that one of the common and useful help techniques is the online help. This can be considered as an online documentation comprising various types of information related to the current state of the application. However, the information was too detailed. Sometimes, it integrated with other usable help techniques such as context-sensitive help and light-weight help. The information provided was normally very case specific, and was explained in long narratives.

ASIA proposed the usage of a “combined approach” which sought to make use of ten questions to be integrated into the adapted warning. Not all questions were directly asked, however the outcome of the questions was expected to be answered in the warnings (i.e. via new features introduced such as tooltips information, risk level bar, Guidance area (Q & A), less technical terminology words, match signal icon and word). Therefore, Table 7.37 presents the assessment results based on the user study that had been conducted.

CHAPTER 7: EVALUATION AND VALIDATION OF THE AUTOMATED SECURITY INTERFACE ADAPTATION (ASIA)

	Online Help	Context sensitive help	Light-weight help	Sophisticated tutorial	Wizard	Safe staging	Social Navigation	Built in security	Combined approach
Informational What can I do with this application?	Yes	Maybe, upon start-up	No	Yes	No	Maybe	No	No	Yes with guidance
Descriptive What is this? What does this do?	Yes, after searching	Yes immediately	Yes, on a simple level	No	No	Yes	No		Yes with guidance
Procedural How do I do this?		Chances are good	No	Yes	Yes, the wizards shows/guide how to do it	Yes	No		Yes with Q & A format
Interpretive What is happening? Why did this happen? What does it mean?		Maybe	No	Maybe	No	Maybe	No		Yes with the risk level bar and Guidance
Navigational Where am I? Where have I come from and gone to?		Maybe	No	Maybe	Yes by numbering the stages of the	Chances are good	Maybe		Yes with the tooltips information
Choice What can I do now?		Chances are good	No	Yes	Yes by showing the next step		Maybe		Yes with guidance
Guidance What can I do now?					Yes if shown how previous user have progressed and where the current user came from		Yes with Q & A format		
History What have I done?	No	No	No	Maybe	Yes by making previous steps accessible		No		Yes by showing what others did
Motivational Why should I use this program?	Yes	Maybe, upon start-up	No	Maybe	No	No	Yes upon receive risk level bar		
Investigative What else should I know?	Yes, after searching	Maybe	No	Maybe	Maybe	Yes show other available stages	Yes shows other possible path		Yes with Q & A format

Table 7.37: Comparison of which user questions can be answered by which user help technique (adapted from Herzog and Shahmehri (2007))

Based on the previous comparison between the user help technique, online help may be considered as the best approach. However, from the author’s observation, it is lacking the historical information and involved user search activity (i.e. effort) to seek solutions to some questions (i.e. descriptive, procedural, interpretive, navigational, choice, guidance and investigative). To resolve this problem, a “combined approach” was introduced in ASIA framework to bridge the gap and improve the overall function of help. Based on the results presented within this chapter, Table 7.38 further described the evaluation and validation process on the combined approach that has been used in ASIA. This evaluation and validation process was based on the results presented earlier within this chapter. Therefore, the outcome from this user study and detailed explanation in Table 7.38 elucidated the results on Table 7.37 (i.e. blue background).

Users’ questions	Combine approach results	Evaluation and validation
Informational	Yes with guidance	ASIA presented users with Guidance elements that consisted of questions and answers. The information provided was informative to explain

CHAPTER 7: EVALUATION AND VALIDATION OF THE AUTOMATED SECURITY INTERFACE ADAPTATION (ASIA)

Users' questions	Combine approach results	Evaluation and validation
		what user can do with this security warning. "What is the summary" link provided a context to explain what users can do with this application.
Descriptive	Yes with guidance	ASIA presented users with Guidance elements that consisted of questions and answers. The information provided was informative to describe what a user can do with this security warning. "What is the summary" link provided a summary on what is happening. It's available straight away once users clicked help (i.e. no further search required).
Procedural	Yes with Q & A format	ASIA presented users with Guidance elements that consisted of questions and answers. At the main Guidance area, users had been presented with simple instructions on how to use the guidance (i.e. no further search required).
Interpretive	Yes with the risk level bar and Guidance	ASIA presented users with Guidance elements that consisted of questions and answers. "What is the risk" explained the severity level of problems that users encountered. Simultaneously, the risk level bar with colour coding communicated the risk in a better way for users to understand. The tooltips functions explained the definition of the texts (i.e. no further search required).
Navigational	Yes with tooltips information	ASIA presented users with features which embedded the tooltips information. It explained simple and useful information for users. For instance, when users hover over "location" they were presented with "This indicates the location of the file on your system". In addition, "what is the summary" also explained the current context

CHAPTER 7: EVALUATION AND VALIDATION OF THE AUTOMATED
SECURITY INTERFACE ADAPTATION (ASIA)


Users' questions	Combine approach results	Evaluation and validation
		of the warning (i.e. no further search required).
Choice	Yes with guidance	ASIA presented users with Guidance elements that consisted of questions and answers. It provided users with some choices presented in the guidance area. Users would be able to get more information from one page to another page (i.e. but still remain in one dialogue box) (i.e. no further search required).
Guidance	Yes with Q & A format	ASIA presented users with Guidance elements that consisted of questions and answers. "What should I do" presented the recommended action for users to take (i.e. no further search required).
History	Yes by showing what others did	This was the missing element in other user help techniques. ASIA provided this information via "what did others do" to view social navigation elements. One value added element in ASIA.
Motivational	Yes upon receive risk level bar	The risk level bar provided quick information on the severity of warning message. Tooltips provided quick and useful information for users to apprehend. Therefore, it gave early motivation to users.
Investigative	Yes with Q & A format	ASIA presented users with Guidance elements that consisted of questions and answers. By clicking "what else should I know" gave users some other suggestion that can considered before a decision is made (i.e. no further search required).

Table 7.38: Details of evaluation and validation

Having evaluated and validated the results from Table 7.38, it may be noted that with the "combined approach", as proposed in ASIA, security warnings were improved and this approach is feasible. Another comparison was made between the standard security

CHAPTER 7: EVALUATION AND VALIDATION OF THE AUTOMATED SECURITY INTERFACE ADAPTATION (ASIA)

warning and the adapted warning as depicted in Table 7.39. It may be revealed that the standard security warning only covered (i.e. using “✓”) five contexts of (Q & A) whilst the adapted warning covered all of the available contexts. Even though this result was not representative, but was based on the focal point of study (i.e. task 7) it was proved that the “combined approach” embedded in ASIA was workable. One main difference that can be revealed in this comparison is that ASIA improved warnings to incorporate all questions and answer elements, especially with regards to historical information (which cannot be done in online help).

Security Warning Image	Informational	Descriptive	Procedural	Interpretive	Navigational	Choice	Guidance	History	Motivational	Investigative
 <p>Standard security warning</p>	✓	✓	✓	✓		✓				

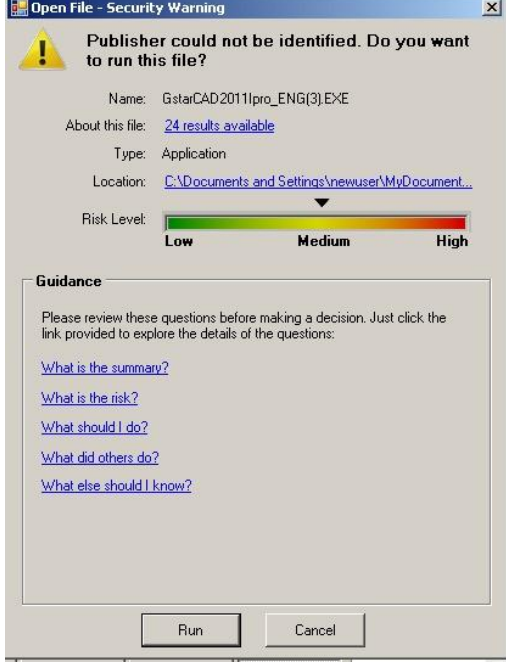
Security Warning Image	Informational	Descriptive	Procedural	Interpretive	Navigational	Choice	Guidance	History	Motivational	Investigative
 <p data-bbox="427 1189 746 1223">Enhanced security warning</p>	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

Table 7.39: Comparison of security warnings based on the availability of 10 questions.

Therefore, based on the overall empirical evidence presented in the earlier chapters, this thesis has been able to achieve its goal by fulfilling all the objectives as presented in Chapter 2. This proves that ASIA was achievable and that security warnings were improved.

7.6 Discussions

Based on the evidence presented within this chapter, it can be noted that the final study utilised 50 respondents to experience the standard security warning and the adapted warning. Thus, participants had experienced the look and feel of both warning styles and then made their own judgement on which became their preference. In the early stage of the experiment, 54% of respondents clicked “run”, 32% used the help button whilst 14% opted for cancel upon receiving the simplified security warning (Table 8.1). Participants were shown the security warning enhancement based on their preferences

only if they selected help. After all participants had experienced the adapted warning, the vast majority (46/50) opted for the adapted warning.

These results indicated that the changes which had been made to the security warnings layout are feasible and accepted by the end-users. The additional features that were introduced such as about this file, the main question, location, risk level, help button and warning icon (Tables 7.2 and 7.3), became the factors that contributed to the successful implementation of the adapted warning. The majority of respondents (i.e. results derived from questionnaire and interviews) demonstrated that they found these new features were able to assist them in comprehending more easily the information provided in one particular warning when compared with the standard version of warnings. For example, in terms of signal cues, icons and technical jargon. With the adapted warnings, end-users were given some useful information to be assessed (i.e. written information or mouse hover) so that they were able to comprehend current risk and situation before making any decision. In contrast, the standard security warning were unable to provide sufficient information and the layout of the warning remained similar to one and another. From an end-users perspective, they found some significant difficulties in making their decisions and expected more in order to help them to comprehend the meaning of the warning. In addition, they also demonstrated that not enough options existed to guide them and a lack of satisfaction with the availability of help functions in the standard security warning. With the adapted warnings, more useful help functions and the availability of various options made users more aware and understand the current context of warnings and able to comprehend them.

Based on the discussion in Chapter 2, a lack of focus had been given to design a meaningful solution as a new method of interaction to provide effective security warnings. Most of the literature that had been discussed highlighted how security warnings can be improved using various methods especially to improve the layout of warnings. On the other hand, there is a lack of research in the adaptation of security warnings (i.e. presenting security warning based on end-users' need). Therefore the ASIA architecture is introduced to counter these problems by presenting more useful information and available features. This new concept makes this research direction significantly different and unique. It meant that security warnings can be improved and

presented with suitable information that would be able to suit their understanding rather than giving general information as portrayed in standard security warnings.

As mentioned in the previous section, this user study implemented a “combined approach” that had been introduced in Chapter 2. This approach worked to bridge the gaps that currently exist in implementations of security warnings by providing more information that is desired by end-users when they encountered security warnings. One similar underlying research that matches the author intention to improve warnings is proposed by Keukelaere et al. (2009) with Adaptive Security Dialogs (ASD). ASD’s worked adapted the risk that users had been exposed to (i.e. security warnings for opening text file and pdf file will be different). On the other hand, the author’s work adapted the warnings based on users’ preference on what level of information is needed in the security warning. Given the useful and suitable information depicted in the adapted warning, users are able to understand the current context of warning and to help them to make secure manner decision. In ASD, the security warning presentation is fixed based based on the five classes of dialogs. Each different file extension had a fixed version of dialogue box. Whilst in ASIA, the security warnings presentation will be presented to end-users based on types of information that they wanted to have in the warning (i.e. warnings icons, web search, risk level bar, location hyperlink and guidance information (help)). Thus, ASIA improves the security warnings by introducing more user-friendly layout, more useful information and more interactive interaction with end-users which had not been done in ASD.

From the perspective of the standard security warning, the information provided was in a generic context. It generally lacked guidance and history information on what end-users should do and refer to before making a decision. Therefore, ASIA framework via this user study significantly improved the current implementation of security warnings and it worked better in relation to usability (i.e. effectiveness, efficiency and user satisfaction) than the standard security warning as demonstrated by the majority of respondents within this user study. The prototype of ASIA highlighted significant novelty by presenting security warnings based on end-users needs. The vast majority of respondents opted for adapted warnings based on a series of interviews and questionnaire sessions. Even though this user study was presented as a prototype, it

gave an early indication of the effectiveness of end-users' interaction with the security warnings. Thus, it can be suggested that adapted security warnings work better than the conventional security warnings which satisfied the aims of the overall study. In addition, this research was able to highlight a novel way of interaction or presenting security warnings that caters to end-users needs on the level of information that should be presented in a particular warning. The proposed idea of security warning adaptation is still new and it would need more time to be conducted in real-life. However, given that the ASIA concept had been tested, validated and evaluated, it gives a positive outcome to conduct more research within these areas of study.

7.7 Constraints

The following were the constraints of this user study:

- i. This evaluation and validation process was conducted as a prototype software (i.e. role-based in order to provide context of warnings) rather than offering real-time experience for end-users. Therefore, end-users were unable to have real interactions with the new security warning they experienced.
- ii. The security warning enhancement was based on only one task (i.e. task 7). Therefore, it did not provide a wide range of flexibility in terms of experiencing with many security warnings.
- iii. The experiment was conducted personally by the principal investigator, to minimise bias the interview scripts were coded by two external individuals.
- iv. The focus of these warnings was only based on dialogue box contexts rather than other type of warnings (i.e. balloon, notification, in place and banners).
- v. The user study did not cover the element of habituation effects, which was normally correlated with security warnings.

7.8 Conclusions

In conclusion, the evaluation and validation of this user study may be considered as successful. Even though the implementation did not involve real-time user interaction, using prototype software gave an early indication that security warnings can be improved based on user preferences. The “Automated Security Interface Adaptation (ASIA)” prototype was developed to evaluate and to validate the effectiveness of the proposed framework in Chapter 6. Users are routinely presented with standard security warnings from various web browsers, these web browsers have different methods of presenting warnings especially with regard to their functionality and approach. Microsoft as one of the major developers produced their own guidelines to ensure that all of the functionality was presented within their design concept. However, based on a series of user studies presented in Chapters 3 to 5, these guidelines are not implemented (e.g. Microsoft). This signals that there is also a need to take a particular look at the creation of the guidelines from the end-users and developers’ perspective, so that it clarifies how to create and use it effectively.

In general, end-users still experience significant problems with regard to the security warnings that they encounter. In order to ensure that users are able to use the warnings correctly and in a secure manner, usability plays a vital role. A significant area in which usability plays a key role is when users have to make a decision. And of course, the significant type of decision that users have to make is when the system issues them with computer warnings, because their impact on the decision could be significantly greater on security and protection of the system and information. Having conducted a number of trials, it may be concluded that end-users are significantly satisfied with the adapted warning presented to them. Based on the presented results from the earlier sections, end-users indicated that they were able to comprehend the warnings better compared to the standard version. Even though these evaluation and validation processes were presented as prototype software, it gave a clear indication that security warning should be presented in a way that suits end-user needs. For instance, the Chi-Square test revealed the significant difference on both presented warnings. Therefore, this supports the findings on how each warning was presented differently (i.e. by rejected null hypothesis).

Based on the author's knowledge, there are no similar adaptation concepts available and as such this proposed method can be considered as a new concept. In addition, ASIA utilised the help function which embedded all useful information in a similar dialogue of warnings rather than having different dialogue boxes. The prototype software tried to imitate real scenarios and it was conducted with deliberate considerations (i.e. role-based scenarios and order of warnings). Based on the empirical evidence presented within this chapter, it can be considered that the ASIA framework is feasible and achievable. Users demonstrated significant satisfaction, specifically with the new proposed security warning enhancement.

CHAPTER 8

Conclusion and Future Work

8 Conclusion and Future Work

This chapter presents a summary of the thesis by reviewing the achievements that have been made, and later presents the limitation of the study. The chapter then goes on to highlight future directions for research.

8.1 Achievements of research

Based on the overall findings in this thesis, it may be noted that all of the objectives which were set out in Chapter 1 have been addressed by the series of user studies and the prototype of the Automated Security Interface Adaptation (ASIA) architecture. The achievements of the research are highlighted as follows:

- i. A detailed understanding of the current state of the art in the use of security dialogues and warnings. The research illustrated the need to improve security warnings by highlighting the fundamental concept, approaches and weaknesses in the way that security warnings are currently implemented (i.e. Chapter 2).
- ii. A comprehensive assessment of security dialogues and warnings through a series of experimental studies. The evidence obtained through these trials proved that in most scenarios, end-users face significant difficulties understanding and interacting with security warnings and thus it can be demonstrated that security warnings should be improved accordingly (i.e. Chapters 3, 4 and 5).
- iii. Proposal of the Automated Security Interface Adaptation (ASIA) architecture to improve security warnings. This architecture provides a novel approach to adapt security dialogues and warnings based on end-users' need or preferences (i.e. Chapter 6).
- iv. Implementation of a prototype to evaluate and to validate the ASIA architecture. The results proved that, in the vast majority of cases, the adaptation warnings were the preferred choice when compared to the standard warnings in terms of usability (i.e. effectiveness, efficiency and availability) and the overall

implementation that include usable help technique table comparison (i.e. Chapter 7).

Two papers relating to the research programme have been presented at refereed conferences, with favourable comments being received from delegates. As such, it is believed that the research has made valid and useful contributions to the body of knowledge of information security, in regards to security warnings (see Appendix E).

8.2 Limitations of the research

Despite the aims of this research having been met, there are a number of limitations that can be identified. The limitations may be summarised as follows:

- i. The evaluation and validation user study was conducted as a prototype system rather than having a real-time context where end-users were able to experience the look and feel of security warnings through genuine interactions. It was difficult to conduct a real-time study, due to privacy and ethical issues. Also, only one task has been presented (i.e. task 7) in order to generate a security warning enhancement, rather than having all tasks. This was done to elicit the learning effect and to ensure that users remained focused through a long period of user study. It may be noted, for the user study as described in Chapter 7, that each session was approximately 40 minutes.
- ii. The focal point of this research was specifically on dialogue box warnings as suggested by the previous user studies (Chapters 4 and 5). It did not cover other types of interaction such as notifications, in-place, balloons and banners. As a result, warning dialogues that provided at least two options (e.g. Yes and No) and were associated with security and protection (i.e. upon detection of warning class, header name and application name) were chosen.
- iii. The 7 tasks that were used were derived from 3 main web browsers (i.e. Internet Explorer, Mozilla Firefox and Google Chrome) rather than providing flexibility with all browsers. A series of user studies conducted in Chapters 3, 4 and 5

revealed that these three browsers were among the most popular to be chosen by end-users.

- iv. A study of “habituation effects”, as suggested in warning studies, has not been covered. A habituation effect considers in particular the effect of repeated exposure to warnings. At present, the aims of this research are limited to how warnings can be presented based on user preferences.
- v. With regard to the participants involved (i.e. ranging from 30 to 50 participants in Chapters 3, 4 and 5), the majority were experienced in using a computer and the Internet for more than six years, and had good computing skills. The segregation of the data sets (i.e. participant group in terms of age) was not sufficiently diverse with the majority aged from twenty to early 30s and had a high level of familiarity with technology. It would be useful if the data set can be varied to different age groups (e.g. older participants). In addition, participants from the general public (i.e. not within the university) would provide a more diverse sample distribution, as they might come from different backgrounds.
- vi. The interview sessions were recorded by the principal investigator, with most of the participants involved being predominantly Plymouth University students or staff. As a consequence of the interviews being recorded, participants might have provided biased answers (i.e. to satisfy the listener or examiner).
- vii. Most of the outcomes of the user studies in this thesis were evaluated using a descriptive method (i.e. frequency and cross tabulation analysis). It would be useful to consider other statistical analysis techniques.

Despite these limitations, the overall findings are still valid and useful, based on the evidence that has been gathered. The presented contributions have highlighted how this research can fit into the domain of warning research study and significantly improve the current state of the art.

8.3 Suggestions for future work

This research has sought to improve the domain of computer security, specifically in terms of computer security warnings. The issues of usability and users' experience of the usage of security dialogues and warnings were highlighted in which future work may be carried out to advance upon what has been achieved with this particular research. Details of proposed future work are presented below:

- i. An application (i.e. automated security warnings adaptation software) could be designed that would interact with any context or type of security warning from different web browsers in a computer, in real-time, and therefore enable a wider range of assessments to be conducted to evaluate the effectiveness of how security warning presentation can be improved.
- ii. The habituation effects study could be conducted in relation to this warning study. It could consider how security warning enhancements can be accepted by end-users after being used for a certain period of time (i.e. whether habituation effects still exist or can be minimised). Hence, it will gather more empirical evidence in terms of how security warnings can be improved.
- iii. Once a full, real-time application has been developed, a repeated study with regards to the questionnaire and interview may be conducted again. This will provide more useful insights from end-users based on the results of using the security warning enhancement over a prolonged period of time. In addition, a usability study may be conducted again (i.e. in a real-time context) and all of these results may then be compared with the results presented in Chapter 7.
- iv. It would be useful to obtain involvement from a range of participant groups to provide more evidence as to how each group of people understand and make use of the warnings. Therefore, it might be useful to suggest that warnings can be presented to cater for needs based on these different groups (e.g. based on age or technical ability or experience).
- v. For more comprehensive analysis, various statistical analysis techniques can be used, such as significance and reliability tests, to further validate the findings.

- vi. Further research should also focus on how warnings can be effectively used to warn the user and simultaneously minimise the level of interruption whilst users are focussed on the respective task. As it has been proposed that warnings should only be presented when needed (i.e. based on the criticality of the warnings), it is useful to assess the effectiveness of warning implementations in various application usage contexts (e.g. from different operating systems, web browsers and Internet security packages).

8.4 The future of security warnings

The future of this research offers considerable scope for future work, since end-users deal with computer warnings on a daily basis, whilst using their computer at home or at work. The interdependencies of human and computer cannot be neglected as warnings will continue to be used to warn and to inform the user about possible problems. However, more research and development is needed to find methods that ensure that warnings are presented in a meaningful manner, at the time they are needed, with sufficient information to make an informed decision, but, in a way that users do not disregard the main purpose of the warning. To this end, this research has proposed and developed the ASIA architecture that provides improved security warnings and reacts to users' needs.

The problems or difficulties based on end-user experience with computer warnings have been clearly established in this thesis. These facts then led to a series of experimental studies to explore alternative approaches to provide warnings in a desirable context that suited the users' needs. Thus, security warnings become the means to provide transparent security and protection with regards to the decision making process that a user has to make which greatly affects the fundamental goal of computer security.

The research has shown that, as far as security warnings are concerned, a 'one size fits all' approach is not viable, and users need targeted support in order to understand and thereby make more informed decisions. ASIA evidences the potential to contribute here by tailoring security interactions far more closely to individual needs. Through doing so, security technology will be better positioned to serve and protect a much wider proportion of the online community than is currently being achieved.

List of References

References

- American National Standards Institute (ANSI) (2012) 'Introduction to ANSI'. [Online]. Available at: http://www.ansi.org/about_ansi/introduction/introduction.aspx?menuid=1#UJqDJuTZzfQ (Accessed: 20/12/2012).
- Amer, T. S. & Maris, J. B. (2007) 'Signal Words and Signal Icons in Application Control and Information Technology Exception Messages - Hazard Matching and Habituation Effects', *Journal of Information Systems*, vol.21, 2, pp. 1-22.
- Apple (2012) 'iOS Human Interface Guidelines'. [Online]. Available at: <http://developer.apple.com/library/ios/documentation/userexperience/conceptual/mobilehig/MobileHIG.pdf> (Accessed: 18/02/2013).
- Baecker, R. M., Small, I. & Mander, R. (1991) Bringing Icons to Life. In Baecker, R.M., Grudin, J., Buxton, W.A.S. and Greenberg, S. (eds.) *Readings in Human-computer Interaction: Toward the Year 2000*. San Francisco, California, Morgan Kaufmann, pp. 444-449. ISBN 1558602461.
- Baecker, R. M., Grudin, J., Buxton, W. A. S. & Greenberg, S. (1995) Designing to Fit Human Capabilities. In Baecker, R.M., Grudin, J., Buxton, W. A. S. and Greenberg, S. (eds.) *Human-Computer Interaction: Toward the Year 2000*. San Francisco, California, Morgan Kaufmann Publishers, Inc. pp. 667-680. ISBN 1558602461.
- Baecker, R.M., Grudin, J., Buxton, W. A. S. and Greenberg, S. (1995b) A Historical and Intellectual Perspective. In Baecker, R.M., Grudin, J., Buxton, W. A. S. and Greenberg, S (eds.) *Human-Computer Interaction: Toward the Year 2000*. San Francisco, California, Morgan Kaufmann Publishers, Inc. pp. 35-47. ISBN 1558602461.
- Bahr, G.S. and Ford, R.A. (2010) 'How and Why Pop-Ups Don't Work: Pop-up Prompted Eye Movements, User Affect and Decision Making', *Computers in Human Behaviors*, vol.27, 2, pp. 776-783.
- BBC (2010) 'Illegal music downloads are 'on the rise''. [Online]. Available at: <http://www.bbc.co.uk/news/entertainment-arts-12003499> (Accessed: 6 /11/2012).
- Balfanz, D., Durfee, G., Smetters, D. K. & Grinter, R. E. (2004) 'In search of usable security: five lessons from the field'. *Security & Privacy, IEEE*, 2 (5), pp. 19-24.
- Balnaves, M. & Caputi, P. (2001) *Introduction To Quantitative Research Methods - An Investigative Approach*. London: Sage Publications. ISBN 0761968032.
- Bellissimo, A., Burgess, J. & Fu, K. (2006) 'Secure software updates: disappointments and new challenges', *Proceedings of the 1st USENIX Workshop on Hot Topics in Security*. Vancouver, B.C., Canada USENIX Association, pp. 37-43.
- Belloti, V. & Edwards, W.K. (2001) 'Intelligibility and Accountability: Human Considerations in Contexts Aware Systems', *Journal of Human-Computer Interaction*, Vol. 16, 2-4, pp. 193-212.

-
- Ben-Asher, N., Meyer, J., Moller, S. & Englert, R. (2009) 'An Experimental System for Studying the Tradeoff between Usability and Security', *International Conference on Availability, Reliability and Security, 2009. ARES '09*. 16-19 March 2009. pp. 882-887.
- Berners-Lee, T., Cailliau, R., Luotonen, A., Nielsen, H. F. & Secret, A. (1994) 'The World-Wide Web', *Communications of the ACM*, vol.37, 8, pp. 76-82.
- Bertram, D. (2006) 'Likert Scales'. [Online]. Available at: <http://poincare.matf.bg.ac.rs/~kristina//topic-dane-likert.pdf> (Accessed: 11/01/2013).
- Besnard, D. & Arief, B. (2004) 'Computer security impaired by legitimate users'. *Computers & Security*, 23 (3). pp 253-264.
- Bétrancourt, M. & Bisseret, A. (1998) 'Integrating textual and pictorial information via pop-up windows: An experimental study', *Behaviour & Information Technology*, vol.17, 5, pp. 263-273.
- Bishop, M. (2003) *Computer Security Art and Science*. Addison-Wesley. ISBN 0201440997.
- Bødker, S. (2006) 'When second wave HCI meets third wave challenges', *Proceedings of the 4th Nordic conference on Human-computer interaction: changing roles*. Oslo, Norway ACM, pp. 1-8.
- Boone, H., N. and Boone, H., A. (2012) 'Analyzing Likert Data'. [Online]. Available at: <http://www.joe.org/joe/2012april/tt2.php> (Accessed: 10/01/2013).
- Böhme, R. & Köpsell, S. (2010) 'Trained to accept?: a field experiment on consent dialogs', *Proceedings of the 28th international conference on Human factors in computing systems*. Atlanta, Georgia, USA, ACM, pp. 2403-2406.
- Böhme, R. & Köpsell, S. (2011) 'The security cost of cheap user interaction', *Proceedings of the 2011 workshop on New security paradigms workshop*. Marin County, California, USA, ACM, pp. 67-82.
- Brustoloni, J. C & Villamarín-Salomón, R. (2007) 'Improving Security Decisions with Polymorphic and Audited Dialogs', *Proceedings of the 3rd symposium on Usable privacy and security*, Pittsburg, USA, ACM, pp. 76-85.
- Bravo-Lillo, C., Cranor, L., Downs, J., Komanduri, S., Sleeper, M., Campos, P., Graham, N., Jorge, J., Nunes, N., Palanque, P. & Winckler, M. (2011) 'Improving Computer Security Dialogs Human-Computer Interaction – INTERACT 2011'. Springer Berlin / Heidelberg, pp. 18-35.
- Bravo-Lillo, C., Cranor, L. F., Downs, J. S. & Komanduri, S. (2011b) 'Bridging the Gap in Computer Security Warnings: A Mental Model Approach', *Security & Privacy, IEEE*, vol.9, 2, pp. 18-26.

-
- Brignano, M. & McCullough, H. (1981) *The search for safety: A history of railroad signals and the people who made them*, Union Switch & Signal Division, American Standard, New York. ISBN 0960620206.
- Brinck, T., Gergle, D. & Wood, S. D. (2002) *Designing web sites that work Usability for The Web*. United States of America: Morgan Kaufmann. ISBN 1558606580.
- Camp, L. J. (2009) 'Mental Models of Privacy and Security,' *Technology and Society Magazine*, Vol. 28, 3, pp.37-46.
- Carrol, J. M. (2003) *HCI Models, Theories and Frameworks: Toward a Multidisciplinary Science*. Morgan Kaufmann. ISBN 1558608087.
- Cockton, G. & Lavery, D. (1999) 'A Framework for Usability Problem Extraction'. In Sasse, M. A. and Johnson, C. (eds.) *Human-Computer Interaction – INTERACT '99 Proceedings of the Seventh IFIP Conference on Human-Computer Interaction*, IOS Press, London, pp. 344-352.
- Coffee, P. (2006) 'Security Onus Is on Developers'. [Online]. Available at: <http://www.eweek.com/c/a/Application-Development/Security-Onus-Is-on-Developers/> (Accessed: 02/02/13).
- Computing Research Association (2003) 'Grand Research Challenges in Information Systems'. [Online]. Available at: <http://archive.cra.org/reports/gc.systems.pdf> (Accessed: 02/02/2013).
- Cranor, L. F. & Garfinkel, S. (eds.) (2005) *Security and Usability. Designing Secure Systems that People Can Use*. USA: O'Reilly. ISBN 0596008279.
- Cranor, L. F. (2008) 'A framework for Reasoning About the Human in the Loop', *USENIX : Usability, Psychology and Security (UPSEC) 2008*. San Francisco, USA, pp. 1-15.
- Daily Mail (2012) 'UK's obsession with Facebook, iPlayer and downloading music means we spend more time on mobiles than the rest of the world'. [Online]. Available at: <http://www.dailymail.co.uk/news/article-2247309/UKs-obsession-Facebook-iPlayer-downloading-music-means-spend-time-mobiles-rest-world.html> (Accessed: 13/12/2012).
- De Paula, R., Ding, X., Dourish, P., Nies, K., Pillet, B., Redmiles, D. F., Rien, J., Rode, J. A. & Filbo, R. S. (2005) 'In the eye of the beholder: A visualization-based approach to information system security', *International Journal of Human-Computer Studies*, vol.63, 1-2, pp. 5-24.
- DeWitt, A. J. & Kuljis, J. (2006) 'Aligning usability and security: a usability study of Polaris', *Proceedings of the second symposium on Usable privacy and security (SOUPS) 2006*. Pittsburgh, Pennsylvania, ACM, pp. 1-7.
- Dhamija, R., Tygar, J. D. & Hearst, M. (2006) 'Why phishing works', *Proceedings of the SIGCHI conference on Human Factors in computing systems*. Montreal, Quebec, Canada, pp. 581-590.

-
- Dickinson, A., Eisma, R. & Gregor, P. (2003) 'Challenging interfaces/redesigning users', *Proceedings of the 2003 conference on Universal usability*. Vancouver, British Columbia, Canada ACM, pp. 61-68.
- Dourish, P. & Anderson, K. (2006) 'Collective information practice: exploring privacy and security as social and cultural phenomena'. *Human Computer Interaction*, 21 (3). pp. 319-342.
- Downs, J. S., Holbrook, M. B. & Cranor, L. F. (2006) 'Decision strategies and susceptibility to phishing', *Proceedings of the second symposium on Usable privacy and security*. Pittsburgh, Pennsylvania, ACM, pp. 79-90.
- Edwards, W. K. & Grinter, R. (2001) At Home with Ubiquitous Computing: Seven Challenges. In Abowd, G., Brumitt, B. and Shafer, S. (eds.) *UbiComp 2001: Ubiquitous Computing*. Springer Berlin Heidelberg, 2201, pp. 256-272. ISBN 9783540426141.
- Edwards, W. K., Poole, E. S. & Stoll, J. (2007) 'Security Automation Considered Harmful', *Proceedings of the 2007 Workshop on New Security Paradigms*. North Conway, USA, ACM, pp. 33-42.
- Egelman, S., King, J., Miller, R. C., Ragouzis, N. & Shehan, E. (2007) 'Security user studies: methodologies and best practices', *CHI '07 Extended Abstracts on Human Factors in Computing Systems*. San Jose, CA, USA, ACM, pp. 2833-2836.
- Egelman, S., Cranor, L. F. & Hong, J. (2008) 'You've been warned: an empirical study of the effectiveness of web browser phishing warnings', *Proceeding of the twenty-sixth annual SIGCHI conference on Human factors in computing systems*. Florence, Italy ACM, pp. 1065-1074.
- Egilman, D. & Bö hme, S. R. (2006) A brief History of Warnings. In Wogalter, M.S. (ed.) *Handbook of Warnings*. USA: Lawrence Erlbaum Associate, pp. 11-20. ISBN 0805847243.
- Farago, P. (2010) 'Record 2010 iOS, Android Black Friday New Device and App Downloads'. [Online]. Available at: <http://blog.flurry.com/?Tag=Usage%20Statistics> (Accessed: 4/12/2012).
- Faulkner, C. (1998) *The Essence of Human-Computer Interaction*. Great Britain, Prentice Hall. ISBN 0137519753.
- Faulkner, X. (2000) *Usability Engineering*. New York: Palgrave. ISBN 0333773217.
- Folmer, E. & Bosch, J. (2004) 'Architecting for usability: a survey'. *Journal of Systems and Software*, 70 (1-2). pp. 61-78.
- Fowler, J. F. J. (1993) *Survey Research Methods*. United States of America: Sage Publications Inc. ISBN 0803950497.
- Friedman, B., Hurley, D., Howe, D. C., Felten, E. & Nissenbaum, H. (2002) 'Users' conceptions of web security: a comparative study', *CHI '02 extended abstracts on*

Human factors in computing systems. Minneapolis, Minnesota, USA, ACM, pp. 746-747.

Furnell, S. M. (2004) 'Using security: Easier said than done?', *Computer Fraud & Security*, vol.2004, 4, pp. 6-10.

Furnell, S. M. (2005) 'Why users cannot use security', *Computers & Security*, vol.24, 4, pp. 274-279.

Furnell, S. M. (2005b) 'Considering the security challenges in consumer-oriented eCommerce', *Proceedings of the Fifth IEEE International Symposium on Signal Processing and Information Technology*, 2005. pp. 534-539.

Furnell, S. M., Jusoh, A. & Katsabas, D. (2006) 'The challenges of understanding and using security: A survey of end-users', *Computers & Security*, vol.25, 1, pp. 27-35.

Furnell, S. M., Jusoh, A., Katsabas, D. & Dowland, P. S. (2006b) 'Considering the Usability of End-User Security Software', *Proceedings of 21st IFIP International Information Security Conference (IFIP SEC 2006)*. Karlstad, Sweden. Springer Boston, pp. 307-316.

Furnell, S. M., Tsaganidi, V. & Phippen, A. (2008) 'Security beliefs and barriers for novice Internet users', *Computers & Security*, vol.27, 7-8, pp. 235-240.

GoCSI.com (2010) 'Computer Crime and Security Survey'. [Online]. Available at: <http://gocsi.com/survey/> (Accessed: 08/01/2013).

Good, N. S. & Krekelberg, A. (2005) 'Usability and Privacy: A study of KazaA P2P File Sharing'. In Cranor, L.F. and Garfinkel, S. (eds.) *Security and Usability Designing Secure Systems That People Can Use*. O'Reilly, pp. 651-667. ISBN 0596008279.

Hadden, S. (1986) *Read the Label: Reducing Risk by Providing Information*. Westview P. ISBN 0813302447.

Hardee, J. B., West, R. & Mayhorn, C. B. (2006) 'To Download or Not to Download: An Examination of Computer Security Decision Making', *Interactions*, vol.13, 3, pp. 32-37.

Hasan, B. & Ahmed, M. U. (2007) 'Effects of interface style on user perceptions and behavioral intention to use computer systems'. *Computers in Human Behavior*, 23 (6). pp. 3025-3037.

Havana, T. & Roning, J. (2004) 'Attitudes and Perceptions Related to Information Security - Case: Rotuaari', *Proceedings of the 30th EUROMICRO Conference*. pp. 534-543.

Herley, C. (2009) 'So long, and no thanks for the externalities: the rational rejection of security advice by users', *Proceedings of the 2009 workshop on New security paradigms workshop*. Oxford, United Kingdom, ACM, pp. 133-144.

-
- Herzog, A. & Shahmehri, N. (2007) 'User help techniques for usable security', *Proceedings of the 2007 symposium on Computer human interaction for the management of information technology*. Cambridge, Massachusetts, ACM, pp. 37-48.
- Hewett, T. T., Baecker, R. M., Card, S., Carrey, T., Gasen, J., Mantei, M., Perlman, G., Strong, G. and Verplank, W. (1996) 'Curricula for Human-Computer Interaction'. [Online]. Available at: <http://old.sigchi.org/cdg/cdg2.html> (Accessed: 05/02/2013).
- Hoegh, R. T. (2006) 'Usability problems: do software developers already know?' *Proceedings of the 18th Australia conference on Computer-Human Interaction: Design: Activities, Artefacts and Environments*, Sydney, Australia, ACM, pp. 425-428.
- Irani, D., Webb, S., Giffin, J. & Pu, C. (2008) 'Evolutionary study of phishing', *eCrime Researchers Summit, 2008*. 15-16 Oct. 2008. pp. 1-10.
- Isbell, C. & Pierce, J. (2005) 'Using an IP Continuum for Adaptive Interface Design', proceedings of the 11th International Conference on Human Computer-Interaction, ACM, New York.
- ISO (1998) 'ISO 9241 Part 11: Guidance on usability'. [Online]. Available at: <http://www.userfocus.co.uk/resources/iso9241/part11.html> (Accessed: 02/03/2013).
- Jagatic, T. N., Johnson, N. A., Jakobsson, M. & Menczer, F. (2007) 'Social phishing', *Communications of the ACM*, vol.50, 1, pp. 94-100.
- Johnston, J., Eloff, J. H. P. & Labuschagne, L. (2003) 'Security and human computer interfaces', *Computers & Security*, vol.22, 8, pp. 675-684.
- Jones, L. A., Anton, A. I. & Earp, J. B. (2007) 'Towards understanding user perceptions of authentication technologies'. *Proceedings of the 2007 ACM workshop on Privacy in electronic society*. Alexandria, Virginia, USA, ACM, pp. 91-98.
- Kauer, M., Pfeiffer, T., Volkamer, M., Theuerling, H. & Bruder, R. (2012) It is not about the design - it is about the content! Making warnings more efficient by communicating risks appropriately. In Neeraj, S. and Waidner, M. (eds.). *Lecture Notes in Informatics (LNI)*. Darmstadt Bonner Köllen Publishing, pp. 187-198. ISBN 978-88579-289-5.
- Keukelaere D. F., Yoshihama, S., Trent, S., Zhang, Y., Luo, L. & Zurko, M. (2009) 'Adaptive Security Dialogs for Improved Security Behavior of Users Human-Computer Interaction – INTERACT 2009'. Springer Berlin / Heidelberg, pp. 510-523.
- Key, J. P. (1997) 'Module S7- CHI SQUARE'. [Online]. Available at: <http://www.okstate.edu/ag/agedcm4h/academic/aged5980a/5980/newpage28.htm> (Accessed: 19/02/2013).
- Koziol, J. (2003) *Intrusion Detection with Snort*. SAMS Publications. ISBN 157870281X.

-
- Lacohee, H., Phippen, A. D. & Furnell, S. M. (2006) 'Risk and restitution: Assessing how users establish online trust', *Computers & Security*. pp. 486-493.
- Lampson, B. (2009) 'Privacy and security: Usable security: how to get it', *Communication of ACM*, vol.52, 11, pp. 25-27.
- Lehto, M. R. (1991) 'A proposed conceptual model of human behavior and its implication for design of warnings', *Perceptual and Motor Skills*, vol.73, 2, pp.595-611.
- Linfo (2004) 'GUI Definition'. [Online]. Available at: <http://www.linfo.org/gui.html> (Accessed: 20/01/2013).
- Macaulay, C., Sloan, D., Xinyi, J., Forbes, P., Loynton, S., Swedlow, J. R. & Gregor, P. (2009) 'Usability and User-Centered Design in Scientific Software Development', *Software, IEEE*, vol.26, 1, pp. 96-102.
- Mannan, M. & Van Oorschot, P. C. (2008) 'Security and usability: the gap in real-world online banking', *Proceedings of the 2007 Workshop on New Security Paradigms*. New Hampshire, ACM, pp. 1-14.
- Maurer, M-E. Luca, A. D & Kempe, Sylvia. (2011) 'Using Data Type Based Security alert Dialogs to Raise Online Security Awareness', *Proceedings of the 7th Symposium on Usable Privacy and Security*, Washington USA, ACM, pp. 1-13.
- McCrum-Gardner, E. (2008) 'Which is the correct statistical test to use?', *British Journal of Oral and Maxillofacial Surgery*, vol.46, 1. pp. 38-41.
- McDougald, B. R. & Wogalter M.S. (2011) 'Increased Comprehension of Warning Pictorials with Color Highlighting', *Proceedings of the Human Factors and Ergonomics Society 55th Annual Meeting*, Sage Journals, pp. 1769-1772.
- Meier, J. D. (2006) 'Web application security engineering', *Security & Privacy, IEEE*, vol.4, 4, pp. 16-24.
- Microsoft (2010) 'Windows User Experience Interaction Guidelines'. [Online]. Available at: <http://msdn.microsoft.com/en-us/library/aa511440.aspx> (Accessed: 18/02/2013).
- Molich, R. & Nielsen, J. (1990), 'Improving a human-computer dialogue', *Communication of the ACM*, vol.33, 3, pp. 338-348.
- Montesino, R & Fenz, S. (2011), 'Information Security Automation: How far can we go', *Sixth International Conference on Availability, Realibility and Security*, pp. 280-285.
- Morris, M. G. & Dillon, A. (1997) 'How user perceptions influence software use', *Software, IEEE*, vol.14, 4, pp. 58-65.
- Mouratidis, H., Giorgini, P. & Manson, G. (2004) 'When security meets software engineering: a case of modelling secure information systems', *Information Systems*, vol.30, 8, pp. 609-629.

-
- Murayama, Y., Fujihara, Y., Nishioka, D., Hauser, C. & Inoue, A. (2009) 'Anshin as Emotional Trust: A Comparison Study between U.S. and Japanese Non-computer-science Students', *Ninth Annual International Symposium on Applications and the Internet, 2009. SAINT '09*, pp. 161-164.
- Nielsen, J. (2003) 'Usability 101: Introduction to Usability'. [Online]. Available at: <http://www.useit.com/alertbox/20030825.html> (Accessed: 06/03/2013).
- Nielsen, J. (2003) 'User education is not the Answer to Security Problems'. [Online]. Available at: <http://www.nngroup.com/articles/security-and-user-education> (Accessed: 02/03/2014).
- Nodder, C. (2005) 'Users and Trust: A Microsoft Case Study'. In Cranor, L.F. and Garfinkel, S. (eds.) *Security and usability. Designing Secure Systems That People Can Use*. O'Reilly, pp. 589-605. ISBN 0596008279.
- Noreen, S., Murtaza, S., Shafiq, M. Z. & Farooq, M. (2009) 'Evolvable malware', *Proceedings of the 11th Annual conference on Genetic and evolutionary computation*. Montreal, Quebec, Canada, pp. 1569-1576.
- Norman, D. A. (2009) 'When Security Gets in the Way'. *interactions*. [Online]. Available at: <http://interactions.acm.org/archive/view/november-december-2009/when-security-gets-in-the-way> (Accessed: 02/02/2013).
- Nowack, M. (1997), 'The Impact of the Internet on Statistical Organisations', *Statistical Journal of the UN Economic Commission for Europe*, vol.14, 4, pp. 345-355.
- Oltedal, S., Moen, B.-E., Klempe, H. & Rundmo, T. (2004) 'Explaining risk perception. An evaluation of cultural theory'. [Online]. Available at: http://www.svt.ntnu.no/psy/Torbjorn.Rundmo/Cultural_theory.pdf (Accessed: 03/02/2013).
- Oppenheim, A. N. (1996) *Questionnaire Design, Interviewing and Attitude Measurement*. London: Pinter Publishers. ISBN 1855670445.
- Pc.Net (2012) 'GUI'. [Online]. Available at: <http://pc.net/glossary/definition/gui> (Accessed: 20/01/2013).
- Pfleeger, C. P. & Pfleeger, S. L. (2003) *Security in Computing*. Prentice Hall. ISBN 0130355488.
- Phippen, A. & Furnell, S. M. (2007) 'Taking responsibility for online protection - why citizens have their part to play', *Computer Fraud & Security*, vol.2007, 11, pp. 8-13.
- Potter, C. & Beard, A. (2010) 'Information Security Breaches Survey Technical Report'. [Online]. Available at: <http://www.pwc.co.uk/audit-assurance/publications/isbs-survey-2010.jhtml> (Accessed: 08/01/2012).

-
- Potter, C. & Warterfall, G. (2012) 'Information Security Breaches Survey Technical Report'. [Online]. Available at: http://www.pwc.co.uk/en_UK/uk/assets/pdf/olpapp/uk-information-security-breaches-survey-technical-report.pdf (Accessed: 06/03/2013).
- Proctor, R. W., Lien, M.-C., Salvendy, G. & Schultz, E. E. (2000) 'A Task Analysis of Usability in Third-Party Authentication', *Information Security Bulletin*, 5, (W3schools), 49-56.
- PWC (2008) 2008 *Information Security Breaches Survey*. <http://www.bis.gov.uk/files/file45713.pdf> (Accessed: 06/03/2013).
- Radle, K. & Young, S. (2001) 'Partnering usability with development: how three organizations succeeded', *Software, IEEE*, vol.18, 1, pp. 38-45.
- Raffetseder, T., Kirda, E. & Kruegel, C. (2007) 'Building Anti-Phishing Browser Plug-Ins: An Experience Report', *ICSE Workshops, Third International Workshop on Software Engineering for Secure Systems, 2007. SESS '07* 20-26 May 2007. pp. 6-6.
- Raja, F., Hawkey, K. & Beznosov, K. (2009) 'Revealing hidden context: improving mental models of personal firewall users', *Proceedings of the 5th Symposium on Usable Privacy and Security*. Mountain View, California ACM, pp. 1-12.
- Raja, F., Hawkey, K., Jaferian, P., Beznosov, K. & Booth, K. S. (2010) 'It's Too Complicated, So I Turned It Off! Expectations, Perceptions, and Misconceptions of Personal Firewall', *Proceedings of the 3rd ACM Workshop on Assurable & USABLE Security Configuration (SafeConfig)*, pp. 53-62.
- Raja, F., Hawkey, K., Hsu, S., Wang, K. L. C. & Beznosov, K. (2011) 'A brick Wall, a Locked Door, and a Bandit: A physical Security Metaphor For Firewall Warnings', *Proceedings of the Seventh Symposium on Usable Privacy and Security*. Pittsburgh, USA, ACM, pp. 1-20.
- Ratnasingham, P. (1998) 'The importance of trust in electronic commerce', *Internet Research: Electronic Networking Applications and Policy*, vol.8, 4, pp. 313-321.
- Reeder, R., Karat, C.M., Karat, J., Brodie, C., Baranauskas, C., Palanque, P., Abascal, J. & Barbosa, S. (2007) 'Usability Challenges in Security and Privacy Policy-Authoring Interfaces Human-Computer Interaction – INTERACT 2007'. Springer Berlin / Heidelberg, pp. 141-155.
- Richardson, R. (2008) 'CSI Computer Crime & Security Survey'. [Online]. Available at: <http://i.cmpnet.com/v2.gocsi.com/pdf/CSISurvey2008.pdf> (Accessed: 05/01/2013).
- Rogers, W. A., Rousseau, G. K. & Lampson, B. (1999) Maximizing the effectiveness of the warning process: Understanding the variables that interact with age. In Park, D.C., Morrel, R.W. and Shifren, K. (eds.) *Processing of medical information in aging patients: Cognitive and human factors perspectives*. NJ: Erlbaum, pp. 267-290. ISBN 0805828893.

-
- Rogers, W. A., Lamson, N. & Rousseau, G. K. (2000) 'Warning Research: An Integrative Perspective', *Human Factors: The Journal of the Human Factors and Ergonomics Society*, vol.42, 1, pp. 102-139.
- Saltzer, J. H. & Schroeder, M. D. (1975) 'The protection of information in computer systems', *Proceedings of the IEEE*, vol.63, 9, pp. 1278-1308.
- Sanders, M. S. & McCormick, E. J. (1993) *Human factors in engineering and design*, McGraw Hill, New York. ISBN 7302054835.
- Schechter, S. E., Dhamija, R., Ozment, A. & Fischer, I. (2007) 'The Emperor's New Security Indicators', *IEEE Symposium on Security and Privacy (SP '07)*, pp. 51-65.
- Schonfeld, E. (2010) 'Pew Shows 65% of People Pay For Digital Content; Mostly Music, Software, And Mobile Apps'. [Online]. Available at: <http://techcrunch.com/2010/12/30/pew-65-percent-pay-digital-content/> (Accessed: 13/12/2012).
- Schultz, E. E. (2007) 'Research on usability in information security', *Computer Fraud & Security*, vol.2007, 6, pp. 8-10.
- Seifert, C., Welch, I. & Komisarczuk, P. (2006) 'Effectiveness of security by admonition: a case study security warnings in a web browser setting', *secure Magazine*, pp. 1-9.
- Shackel, B., & Richardson, S. (1991) Human Factors For Informatics Usability-Background and Overview. In B. Shackel & S. Richardson (Eds.), *Human Factors for Informatics Usability*. Cambridge: Cambridge University Press. ISBN 0521365708.
- Sharek, D., Swofford, C. & Wogalter, M. (2008) 'Failure to Recognize Fake Internet Popup Warning Messages', *Proceedings of the Human Factors and Ergonomics Society 52nd Annual Meeting*, pp. 557-580.
- Shneiderman, B. (2000) 'Designing trust into online experiences', *Communications of the ACM*, vol.43, 12, pp. 57-59.
- Smetters, D. K. & Grinter, R. E. (2002) 'Moving from the design of usable security technologies to the design of useful secure applications', *Proceedings of the 2002 workshop on New security paradigms*. Virginia Beach, Virginia: ACM, pp. 82-89.
- Stanton, J. M. (1998) 'An Empirical Assessment of Data Collection Using The Internet', *Personnel Psychology*, vol.51, 3, pp. 709-725.
- Stanton, J. M., Caldera, C., Guzman, I., Isaac, A., Lin, P., Mathur, M., Seymour, J., Spitzmueller, C., Stam, K., Yamodo, I. & Zakaria, N. (2003) 'Behavioral Information Security: An Overview, Research Agenda and Preliminary Results', *The Security Conference Las Vegas, Nevada*. April 23-24.
- Stanton, J. M., Stam, K. R., Mastrangelo, P. & Jolton, J. (2005) 'Analysis of end user security behaviors', *Computers & Security*, vol.24, 2, pp. 124-133.

-
- Stoll, J., Tashman, C. S., Edwards, W. K. & Spafford, K. (2008) 'Sesame: informing user security decisions with system visualization', *Proceeding of the twenty-sixth annual SIGCHI conference on Human factors in computing systems*. Florence, Italy, ACM, pp. 1045-1054.
- Stone-Gross, B., Abman, R., Kemmerer, R., Kruegel, C., Steigerwald, D. & Vigna, G. (2013) The Underground Economy of Fake Antivirus Software. In Schneier, B. (ed.) *Economics of Information Security and Privacy III*. Springer New York, pp. 55-78. ISBN 1461419808.
- Sunshine, J., Egelman, S., Almuhiemedi, H., Atri, N. & Cranor, L. F. (2009) 'Crying wolf: an empirical study of SSL warning effectiveness', *Proceedings of the 18th conference on USENIX security symposium*. Montreal, Canada USENIX Association, pp. 399-416.
- Symantec (2009) '2009 NCSA / Symantec Home User Study'. [Online]. Available at: <http://www.symantec.com/theme.jsp?themeid=ncsa> (Accessed: 06/03/2013).
- Symantec (2012) 'Internet Security Threat Report'. [Online]. Available at: <http://www.symantec.com/threatreport/> (Accessed: 30 July 2012).
- Thomas, R. M. (2003) *Blending Qualitative & Quantitative Research Methods in These and Dissertations*. United States of America: Corwin Press, Inc. ISBN 0761939326.
- Tognazzini, B. (2005) Design for Usability. In Cranor, L.F. and Garfinkel, S. (eds.) *Security and Usability Designing Secure Systems That People Can Use*. United States of America: O'reilly, pp. 31-46. ISBN 0596008279.
- Tondel, I. A., Jaatun, M. G. & Meland, P. H. (2008) 'Security Requirements for the Rest of Us: A Survey', *Software, IEEE*, vol.25, 1, pp. 20-27.
- Tryfonas, T., Kiountouzis, E. & Poulymenakou, A. (2001) 'Embedding security practices in contemporary information systems development approaches', *Information Management & Computer Security*, Vol. 9, 4, pp. 183 – 197.
- Tuchscheerer, S., Dittmann, J., Hoppe, T. & Krems, J. F. (2010) 'Theoretical analysis of security warnings in vehicles and design challenges for the evaluation of security warnings in virtual environments', *Proceedings of the First International Workshop on Digital Engineering*. Magdeburg, Germany, ACM, pp. 33-37.
- Villamarín-Salomón, R & Brustoloni, J. C. (2010) 'Using Reinforcement to Strengthen Users' Secure Behaviors', *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, Atlanta USA, ACM, pp. 363-372.
- W3schools (2010) 'Browser Statistics'. [Online]. Available at: http://www.w3schools.com/browsers/browsers_stats.asp (Accessed: 18/01/2010).
- W3schools (2012) 'Browser Statistics'. [Online]. Available at: http://www.w3schools.com/browsers/browsers_os.asp (Accessed: 09/01/2013).

- Weible, R. & Wallace, J. (1998) 'Cyber research: the impact of the Internet on data collection', *Marketing Research*, vol.10, 3, pp. 19-25.
- Weir, C. S., Douglas, G., Carruthers, M. & Jack, M. (2009) 'User perceptions of security, convenience and usability for ebanking authentication tokens', *Computers & Security*, vol.28, 1-2, pp. 47-62.
- West, R. (2008) 'The psychology of security', *Communications of the ACM*, vol.51, 4, pp. 34-40.
- Whalen, T. & Inkpen, K. M. (2005) 'Gathering evidence: use of visual security cues in web browsers', *Proceedings of Graphics Interface 2005*. Victoria, British Columbia Canadian Human-Computer Communications Society, ACM, pp. 137-144.
- Whitten, A. & Tygar, J. D. (1999) 'Why Johnny can't encrypt: a usability evaluation of PGP 5.0', *Proceedings of the 8th USENIX Security Symposium*. Washington D.C, pp. 169-184.
- Whitten, A. & Tygar, J. D. (2003) 'Safe Staging for Computer Security', *Proceedings of the 2003 Workshop on Human-Computer Interaction and Security Systems*. Fort Lauderdale, Florida.
- Wogalter, M. S., Dejoy, D. M. & Laughrey, K. R. (1999) Organizing Theoretical Framework: A Consolidated Communication-Human Information Processing (C-HIP) Model. In Wogalter, M.S., Dejoy, D.M. and Laughrey, K.R. (eds.) *Warning and Risk Communication*. Taylor & Francis, pp. 13-21. ISBN 0748402667.
- Wogalter, M. S., Conzola, V. C. & Smith-Jackson, T. L. (2002) 'Research-based guidelines for warning design and evaluation'. *Applied Ergonomics*, 33 (3). pp. 219-230.
- Wogalter, M.S. (2006) Purposes and Scope of Warnings. In Wogalter, M.S. (ed.) *Handbook of Warnings*. USA: Lawrence Erlbaum Associate, pp. 3-9. ISBN 0805847243.
- Wool, A. (2004) 'The use and usability of direction-based filtering in firewalls', *Computers & Security*, vol.23, 6, pp. 459-468.
- Wright, P. (1991) Designing and Evaluating Documentation for I.T Users. In Shackel, B. and Richardson, S. (Eds), *Human Factors for Informatics Usability*, Cambridge University Press, pp. 343-358. ISBN 0521365708.
- Wu, M., Miller, R. C. & Garfinkel, S. L. (2006) 'Do security toolbars actually prevent phishing attacks?' *Proceedings of the SIGCHI conference on Human Factors in computing systems*. Montreal, Quebec, Canada ACM, pp. 601-610.
- Yee, K. P. (2004) 'Aligning security and usability', *Security & Privacy, IEEE*, vol.2, 5, pp. 48-55.

Zaaba, Z. F., Furnell, S. M. and Dowland, P. S. (2011) 'End-User Perception and Usability of Information Security', *Proceedings of the Fifth International Symposium on Human Aspects of Information Security & Assurance (HAISA), London*, pp. 97-107.

Zaaba, Z. F., Furnell, S. M., Dowland, P. S. and Stengel, I. (2012) 'Assessing the usability of application-level security warnings', *Proceedings of the 11th Security Conference (Security Assurance & Privacy), Las Vegas, USA*.

Zurko, M. E., Kaufman, C., Spanbauer, K. & Bassett, C. (2002) 'Did you ever have to make up your mind? What Notes users do when faced with a security decision', *Proceedings of the 18th Annual Computer Security Applications Conference*, pp. 371-381.

Appendix A

User Study 1 Documentation

Faculty of Science and Technology



Portland Square A106, Plymouth

To:	Zarul Zaaba	From:	Paula Simson
cc:	Prof Steven Furnell, Dr Paul Dowland		Secretary to Human Ethics Committee
Your Ref:		Our Ref:	scitech:\d:\human ethics:
Date:	18 February 2010	Phone Ext:	84503

Application for Ethical Approval

Thank you for submitting the ethical approval form and details or the amendments concerning your project:

'Perception and usability in information security: A survey of public attitudes'

I am pleased to inform you that this has been approved.

Kind regards

Paula Simson

Survey questions

Perception and usability in information security: A survey of public attitudes



University of Plymouth

Centre for Security, Communications and Network Research (CSCAN)

This survey is being conducted for PhD research on perception and usability in information security at University of Plymouth, United Kingdom. The questionnaire is designed to investigate perception and level of understanding on usage of computer and its application. It consists of 5 sections, namely:

- 1. Background/demographic** - Overview on users' background which consists of gender, education background, occupation, computing skills and perception on security in computing contexts.
- 2. General usage of computer and operating systems** - Analysis of users' experience on using the Internet, operating system and security concerns on computer
- 3. Usability and protection** - Analysis of users' understanding on issues of usability and protection in relation to malware, security applications, security updates and security trust which require respondents to identify features from a depicted diagram in order to determine what they understand about the features.
- 4. Computer scenario study** - Analysis of users' understanding of computer web security issues based on their past experiences and knowledge of dealing with information security

Researcher details:

Zarul Fitri Zaaba

Centre for Security, Communications and Network Research (CSCAN)

School of Computing and Mathematics, PL4 8AA

University of Plymouth

E-mail: zarul.zaaba@plymouth.ac.uk

Project Supervisors:

Prof. Steven M. Furnell

Dr. Paul Dowland

There are 41 questions in this survey

Consent Form



Dear participants,

This survey is designed for adult participation. If you are **NOT 18 YEARS OR OLDER, PLEASE DO NOT ANSWER THIS SURVEY**. Anyone can take part in the survey and you are free to withdraw at any time.

All your answers will be treated confidentially and respondents will be anonymous during the collection, storage and publication of research material. The survey is hosted online within the Centre for Security, Communications and Network Research (CSCAN). Responses are collected online and stored in a secure database. Once the survey has been taken offline participant responses will be extracted, statistically analysed and published into a suitable academic journal. In addition these results may be used and published in a PhD thesis. Your responses will be treated as confidential at all times and data will be presented in such a way that your identity cannot be connected with specific published data. Should you have any questions about the study or you wish to receive a copy of the results, please contact the researcher Zarul Fitri Zaaba via email or address below:

Researcher details:

Zarul Fitri Zaaba Centre for Security, Communications and Network Research
(CSCAN) School of Computing and Mathematics University of Plymouth
Mail to: zarul.zaaba@plymouth.ac.uk

If you have any concerns regarding the way the study has been conducted, please contact the secretary of Faculty of Science and Technology Ethics Committee:

Paula Simson
A106, Portland Square, Drake Circus
Faculty of Science and Technology
University of Plymouth
Phone: +44 (0)1752584503
Mail to: paula.simson@plymouth.ac.uk

1 [QC1] Are you 18 years old and above? *

Please choose only one of the following:

- Yes
- No

Only answer this question if you are 18 years old and above. IF your answer is NO please quit the survey.

2 [QC] I understand that I am free to withdraw at any time and I confirm that I have read and understand the information given and agree to take part in the study? *

Only answer this question if the following conditions are met:

° Answer was 'Yes' at question '1 [QC1]' (Are you 18 years old and above?)

Please choose only one of the following:

- Yes

Section 1

Background and demographic

3 [Q1] Please select your gender *

Please choose only one of the following:

- Female
- Male

4 [Q2] Please select your age *

Please choose only one of the following:

- 18-30
- 31-40
- 41-50
- Above 50

5 [Q3] Educational background *

Please choose only one of the following:

- Postgraduate (e.g Masters, PhD)
- Higher education (e.g Bachelor Degree, HND, Diploma)
- Further Education (e.g Certificates, A-Levels, GNVQ)
- GCSE/O Level
- Other

6 [Q4] How do you rate your computing skills? *

Please choose only one of the following:

- Expert
- Advanced
- Intermediate
- Beginner

7 [Q5] How many years have you been using a computer? *

Please choose only one of the following:

- <1 year

- 1-2 years
- 3-4 years
- 5-6 years
- >6 years

8 [Q6] What kind of problems do you regularly encounter while using your computer? *

Please choose all that apply:

- User interface difficulties
- Complex security features
- Problem in understanding help functions
- Internet connection speed
- Application problems (i.e installation, difficulty on software usage etc)
- Hardware difficulties
- Operating systems
- Malware (i.e Viruses, worms, trojans, rootkits etc)
- None
- Other:

9 [Q7] What is your level of concern regarding the security of your computer? *

Please choose only one of the following:

- I am very concerned
- I am concerned
- I am mildly concerned
- I am not concerned at all
- I don't know

Section 2

General usage of computer and operating systems

10 [Q8] How long you have been using the Internet? *

Please choose only one of the following:

- < 1 year
- 1-2 years
- 3-4 years
- 5-6 years
- > 6 years
- I do not use Internet

11 [Q9] What is your primary operating system (OS) for your computer? *

Please choose only one of the following:

- Windows 7
- Windows Vista

- Windows XP
- Mac OS X
- Linux
- I don't know
- Other

12 [Q10] Do you feel it is important to update the operating system (OS)? *

Please choose only one of the following:

- It is very important
- It is important
- It is mildly important
- It is not important at all
- I don't know

13 [Q11] How do you keep your operating system (OS) up to date by installing online software update/patches? *

Please choose only one of the following:

- Updated automatically
- Updated manually
- Not updated
- I don't know
-

14 [Q11X] Do you use any security software? *

Please choose only one of the following:

- Yes
- No
- I don't know

15 [Q11X1] From which vendor(s) do you use your security products? *

Only answer this question if the following conditions are met:

° Answer was 'Yes' at question '14 [Q11X]' (Do you use any security software?)

Please choose all that apply:

- Avast
- AVG
- AVIRA
- BitDefender
- eScan
- ESET NOD32
- F-Secure
- G DATA

- Kaspersky
- Kingsoft
- McAfee
- Microsoft Live OneCare
- Norman
- Norton
- Sophos
- Symantec
- Trend Micro
- Trustport
- Other:

16 [Q11X2] What type of security software products do you use? *

Only answer this question if the following conditions are met:

° Answer was 'Yes' at question '14 [Q11X]' (Do you use any security software?)

Please choose all that apply:

- Antivirus
- Zone Alarm Firewall
- Mobile Security
- Anti spyware
- Internet Security (i.e Antivirus, Anti spyware, E-mail security etc)
- Other:

17 [Q12X] What is your preferred web browser? *

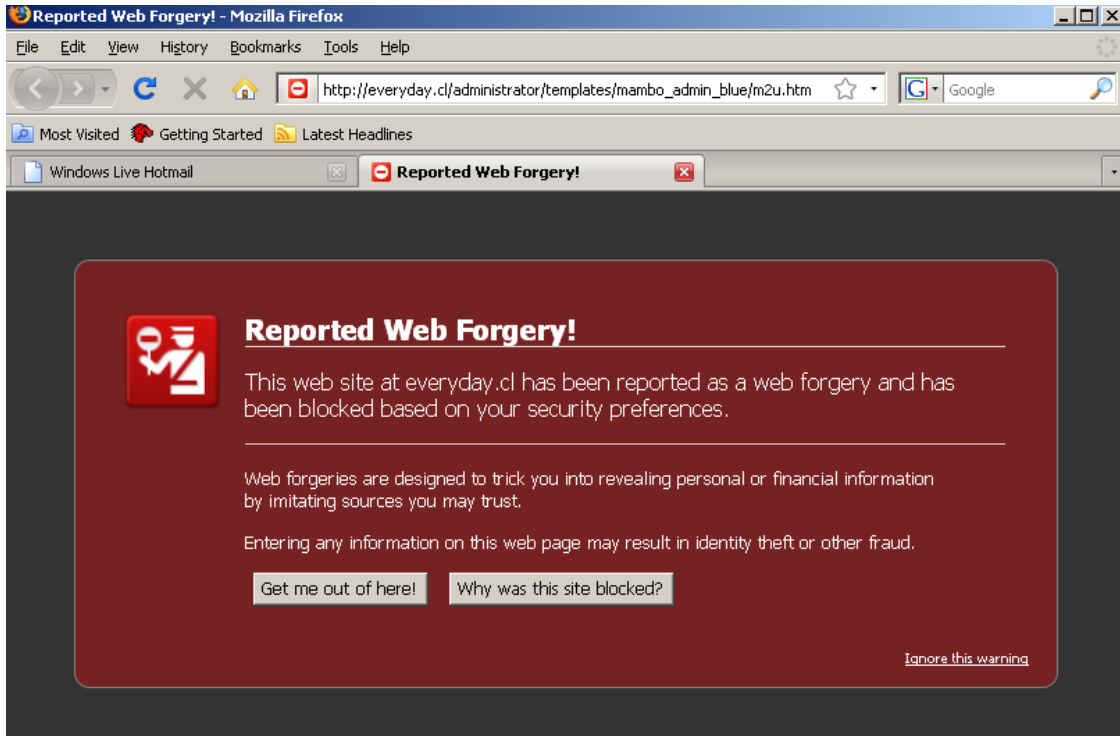
Please choose only one of the following:

- Internet Explorer 8
- Internet Explorer 7
- Mozilla Firefox
- Opera
- Safari
- Chrome
- I don't know
- Other

Section 3

Usability and protection

18 [Q12-a] You received an e-mail from a bank to request for re-activate your online banking account. When you click the hyperlink from the e-mail to respond, you receive the screen below. How would you respond?



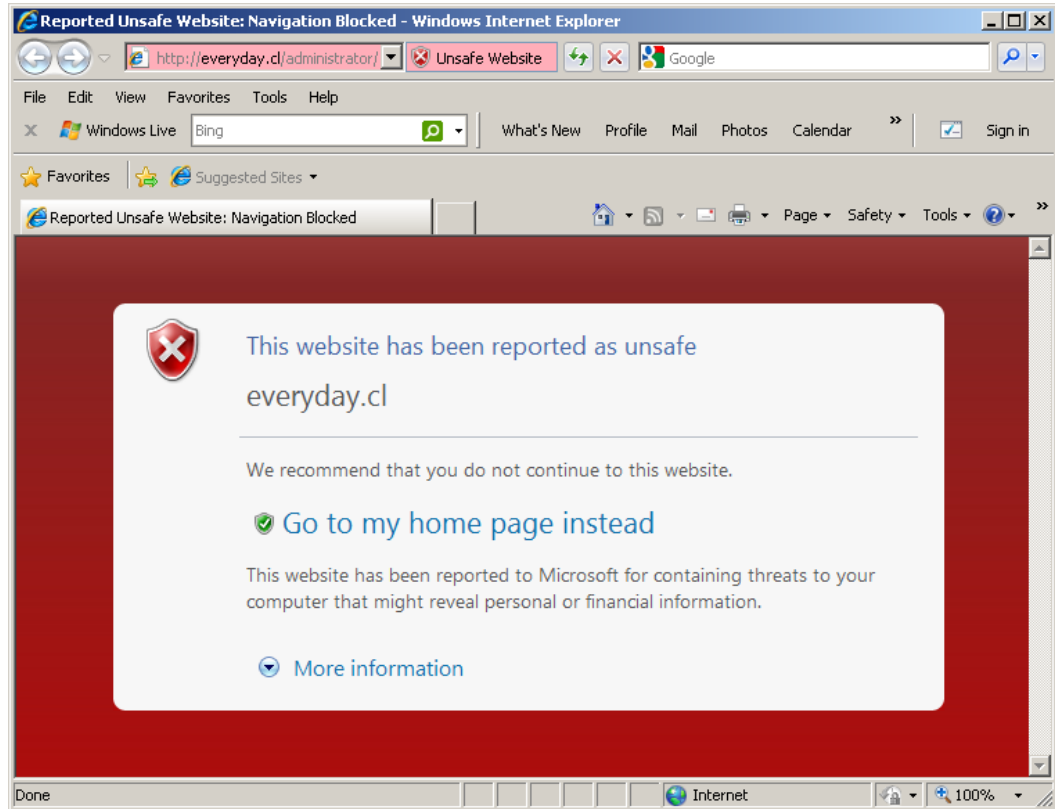
Only answer this question if the following conditions are met:

° Answer was 'Mozilla Firefox' at question '17 [Q12X]' (What is your preferred web browser?)

Please choose only one of the following:

- Try to find more information about the meaning of the message
- Close the browser
- Ignore the warning and proceed with the transaction
- I don't know
- Other

19 [Q12-b] You received an e-mail from a bank to request for re-activate your online banking account. When you click the hyperlink from the e-mail to respond, you receive the screen below. How would you respond?



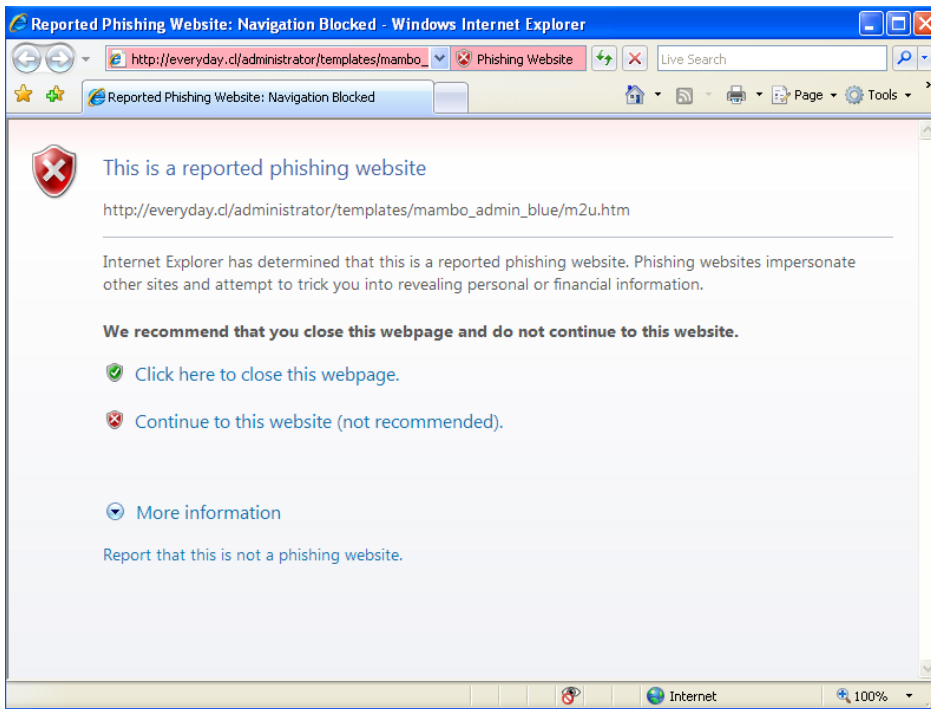
Only answer this question if the following conditions are met:

° Answer was 'Internet Explorer 8' at question '17 [Q12X]' (What is your preferred web browser?)

Please choose only one of the following:

- Try to find more information about the meaning of the message
- Close the browser
- Ignore the warning and proceed with the transaction
- I don't know
- Other

20 [Q12-c] You received an e-mail from a bank to request for re-activate your online banking account. When you click the hyperlink from the e-mail to respond, you receive the screen below. How would you respond?



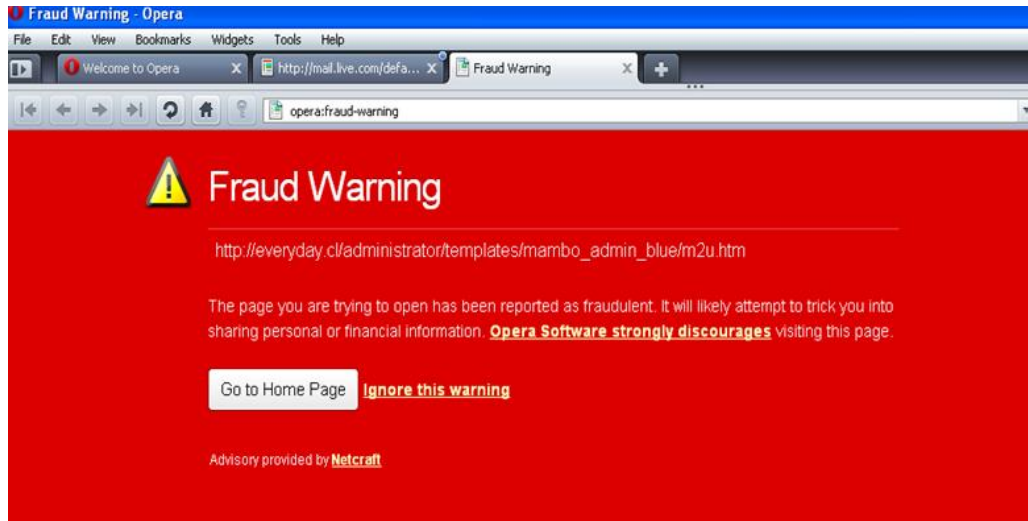
Only answer this question if the following conditions are met:

◦ Answer was 'Internet Explorer 7' at question '17 [Q12X]' (What is your preferred web browser?)

Please choose only one of the following:

- Try to find more information about the meaning of the message
- Close the browser
- Ignore the warning and proceed with the transaction
- I don't know
- Other

21 [Q12-d] You received an e-mail from a bank to request for re-activate your online banking account. When you click the hyperlink from the e-mail to respond, you receive the screen below. How would you respond?



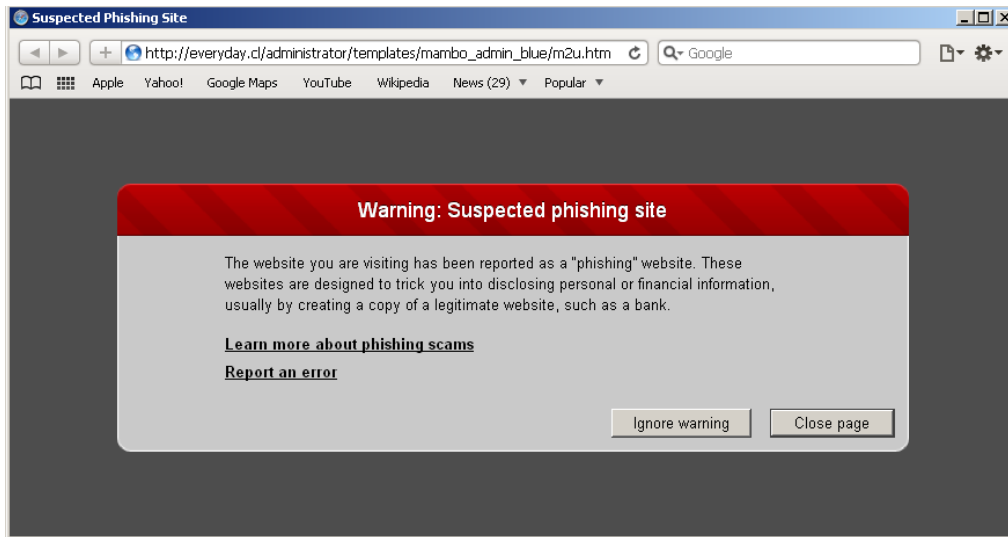
Only answer this question if the following conditions are met:

° Answer was 'Opera' at question '17 [Q12X]' (What is your preferred web browser?)

Please choose only one of the following:

- Try to find more information about the meaning of the message
- Close the browser
- Ignore the warning and proceed with the transaction
- I don't know
- Other

22 [Q12-e] You received an e-mail from a bank to request for re-activate your online banking account. When you click the hyperlink from the e-mail to respond, you receive the screen below. How would you respond?



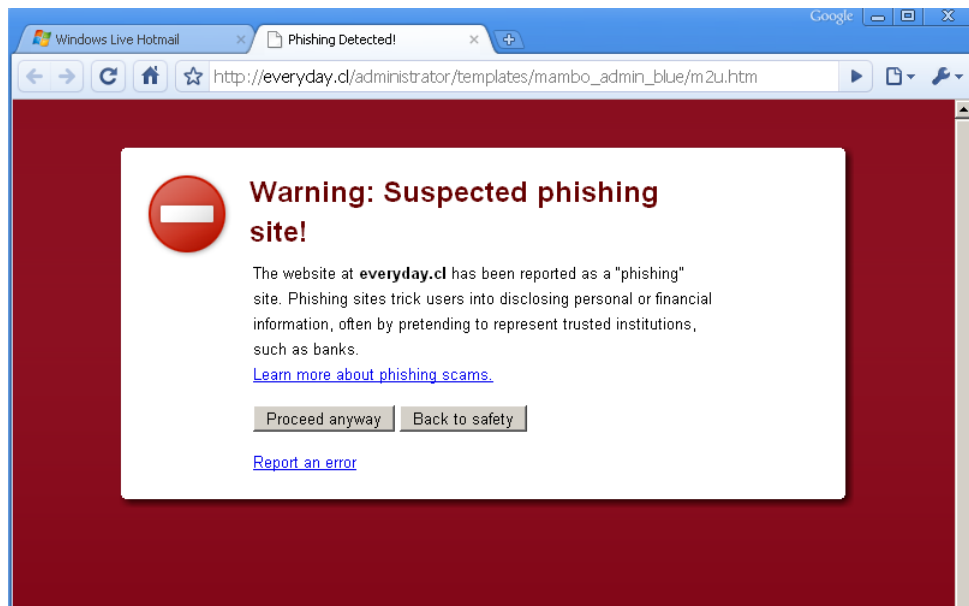
Only answer this question if the following conditions are met:

° Answer was 'Safari' at question '17 [Q12X]' (What is your preferred web browser?)

Please choose only one of the following:

- Try to find more information about the meaning of the message
- Close the browser
- Ignore the warning and proceed with the transaction
- I don't know
- Other

23 [Q12-f] You received an e-mail from a bank to request for re-activate your online banking account. When you click the hyperlink from the e-mail to respond, you receive the screen below. How would you respond?



Only answer this question if the following conditions are met:

◦ Answer was 'Chrome' at question '17 [Q12X]' (What is your preferred web browser?)

Please choose only one of the following:

- Try to find more information about the meaning of the message
- Close the browser
- Ignore this warning and proceed with the transaction
- I don't know
- Other

24 [Qxx-1] Do you feel that you understood the information depicted in the screenshot?

Only answer this question if the following conditions are met:

◦ Answer was 'Internet Explorer 7' or 'Mozilla Firefox' or 'Internet Explorer 8' or 'Opera' or 'Safari' or 'Chrome' at question '17 [Q12X]' (What is your preferred web browser?)

Please choose only one of the following:

- Yes
- No

25 [Qxx-1a] Which of the following did you have difficulty understanding? *

Only answer this question if the following conditions are met:

° Answer was 'No' at question '24 [Qxx-1]' (Do you feel that you understood the information depicted in the screenshot?) Please choose all that apply:

- Technical terminology
- The nature of the event being described
- The choices available
- Other:

26 [Qxx-2] Why do you believe the security message would have appeared? *

Only answer this question if the following conditions are met:

° Answer was 'Safari' or 'Internet Explorer 8' or 'Internet Explorer 7' or 'Mozilla Firefox' or 'Opera' or 'Chrome' at question '17 [Q12X]' (What is your preferred web browser?) Please choose all that apply:

- The website contains inappropriate materials
- The website is linked to fraudulent activity
- The website contains viruses
- It is the security warning which I encounter normally
- I don't know
- Other:

27 [Q14] Have you experienced any of the following? *

Please choose the appropriate response for each item:

	Yes	No	I don't know	Never heard of it
Virus	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Worms	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Trojans	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Phishing	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Spyware	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Spam	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Unauthorized access attempt	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

28 [Q15] How has the possibility of becoming a victim of malicious attack or cybercrime changed your behaviour towards the usage of computer security? *

Please choose all that apply:

- It has not changed my attitude
- I only visit web sites that I am familiar with
- Used Internet security package
- Go online surfing less often
- Other:

29 [Q16] Which of the following security applications do you have installed on your computer? *

Please choose the appropriate response for each item:

	Yes	No	I don't know	Never heard of it
Anti-virus	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Anti-spyware	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Anti-phishing	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Firewall	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Intrusion detection system	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Pop up blocker	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Parental controls	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Spam filters	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

30 [Q17] How do you update your anti-malware tools? *

Please choose the appropriate response for each item:

	Updated manually	Updated automatically	Not updated at all	I don't know
Antivirus	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Anti-spyware	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Anti-phishing	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Firewall	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>
Intrusion detection system (IDS)	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>	<input type="radio"/>

31 [Q18] Which of these statements do you agree, with regarding your use of anti-malware protection tools? *

Please choose only one of the following:

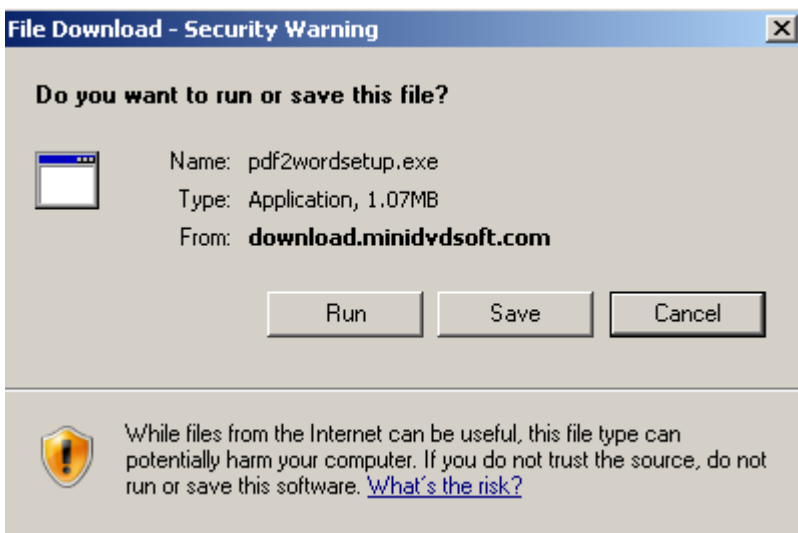
- It is very important to trust anti-malware tools as they provide safeguards for my computer
- It is important to trust anti-malware tools as they provide safeguards for my computer
- It is mildly important to trust anti-malware tools as they provide safeguards for my computer
- It is not important to trust anti-malware tools

- I don't know

Section 4

Scenario study

32 [Q19a] You would like to download a new free application from your web browser. When you click the link to download the file, the following pop up appears. What would you do next?



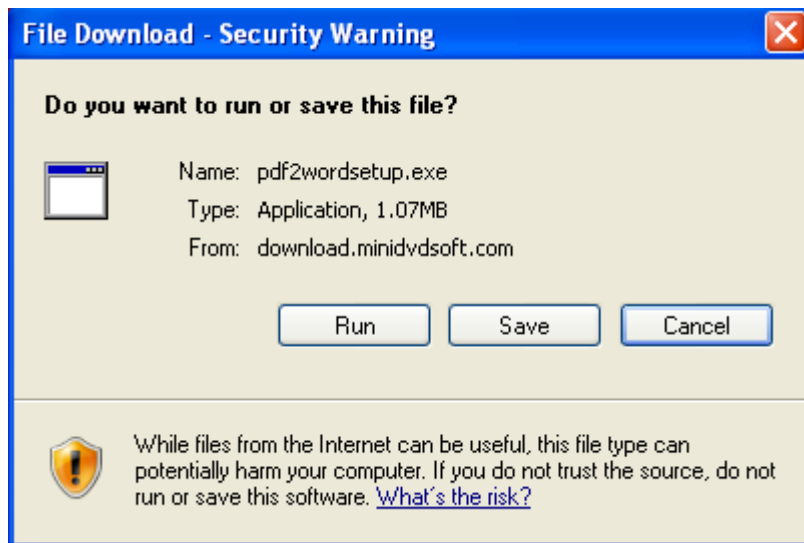
Only answer this question if the following conditions are met:

° Answer was 'Internet Explorer 8' at question '17 [Q12X]' (What is your preferred web browser?)

Please choose only one of the following:

- I get the information about the application from the web
- I save and scan the file for viruses
- I save and run the application
- I cancel or quit from the process
- I run the application
- I don't know
- Other

33 [Q19b] You would like to download a new free application from your web browser. When you click the link to download the file, the following pop up appears. What would you do next?



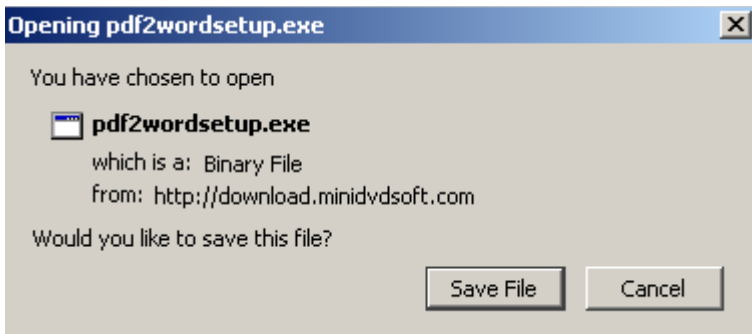
Only answer this question if the following conditions are met:

° Answer was 'Internet Explorer 7' at question '17 [Q12X]' (What is your preferred web browser?)

Please choose only one of the following:

- I get the information about the application from the web
- I save and scan the file for viruses
- I save and run the application
- I cancel or quit from the process
- I run the application
- I don't know
- Other

34 [Q19c] You would like to download a new free application from your web browser. When you click the link to download the file, the following pop up appears. What would you do next?



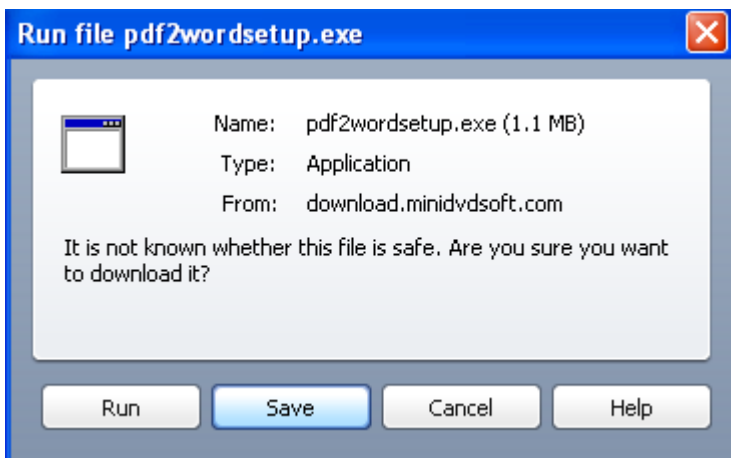
Only answer this question if the following conditions are met:

° Answer was 'Mozilla Firefox ' at question '17 [Q12X]' (What is your preferred web browser?)

Please choose only one of the following:

- I get the information about the application from the web
- I save and scan the file for viruses
- I save and run the application
- I cancel or quit from the process
- I run the application
- I don't know
- Other

35 [Q19d] You would like to download a new free application from your web browser. When you click the link to download the file, the following pop up appears. What would you do next?



Only answer this question if the following conditions are met:

° Answer was 'Opera' at question '17 [Q12X]' (What is your preferred web browser?)

Please choose only one of the following:

- I get the information about the application from the web
- I save and scan the file for viruses
- I save and run the application
- I cancel or quit from the process
- I run the application
- I don't know
- Other

36 [Q19e] You would like to download a new free application from your web browser. When you click the link to download the file, the following pop up appears. What would you do next?



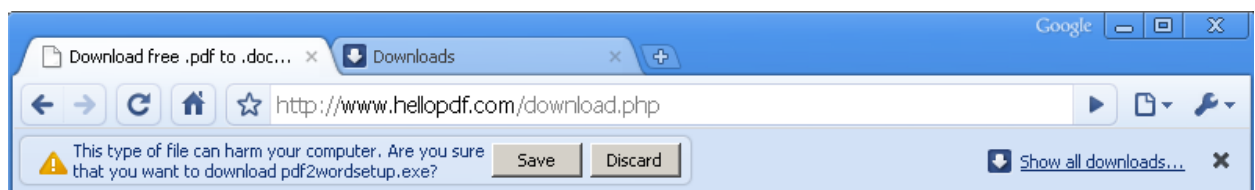
Only answer this question if the following conditions are met:

◦ Answer was 'Safari' at question '17 [Q12X]' (What is your preferred web browser?)

Please choose only one of the following:

- I get the information about the application from the web
- I save and scan the file for viruses
- I save and run the application
- I cancel or quit from the process
- I run the application
- I don't know
- Other

37 [Q19f] You would like to download a new free application from your web browser. When you click the link to download the file, the following pop up appears. What would you do next?



Only answer this question if the following conditions are met:

° Answer was 'Chrome' at question '17 [Q12X]' (What is your preferred web browser?)

Please choose only one of the following:

- I get the information about the application from the web
- I save and scan the file for viruses
- I save and run the application
- I cancel or quit from the process
- I run the application
- I don't know

38 [Q20] Do you feel there is enough information for you to make a decision based on the depicted warning? *

Only answer this question if the following conditions are met:

° Answer was 'Internet Explorer 8' or 'Internet Explorer 7' or 'Mozilla Firefox' or 'Opera' or 'Safari' or 'Chrome' at question '17 [Q12X]' (What is your preferred web browser?)

Please choose only one of the following:

- Yes
- No

39 [Q21] What other information do you think is needed? *

Only answer this question if the following conditions are met:

° Answer was 'No' at question '38 [Q20]' (Do you feel there is enough information for you to make a decision based on the depicted warning?)

Please choose all that apply:

- Details of the consequences if you were to proceed to run the application
- Provision of a proper help function
- Confirmation of legitimate download
- Its free from any kind of malware attack
- Other:

40 [Q23]By completing this online questionnaire, are you more or less concerned about security on your computer? *

Please choose only one of the following:

- I am more concerned
- I am less concerned
- My level of concern has not changed
- I don't know
- Other

41 [Q22]Do you have any comments regarding the given questions or wish to share any information with regards to information security issues. Please feel free to leave your comments in the space provided

Please write your answer here:

**If you have any questions or would like to be notified the findings from this survey, please e-mail zarul.zaaba@plymouth.ac.uk
Thank you for spending your time to fill in this survey**

**Submit your survey.
Thank you for completing this survey.**

Figures from Chapter 3 – Section 3: Usability and Protection

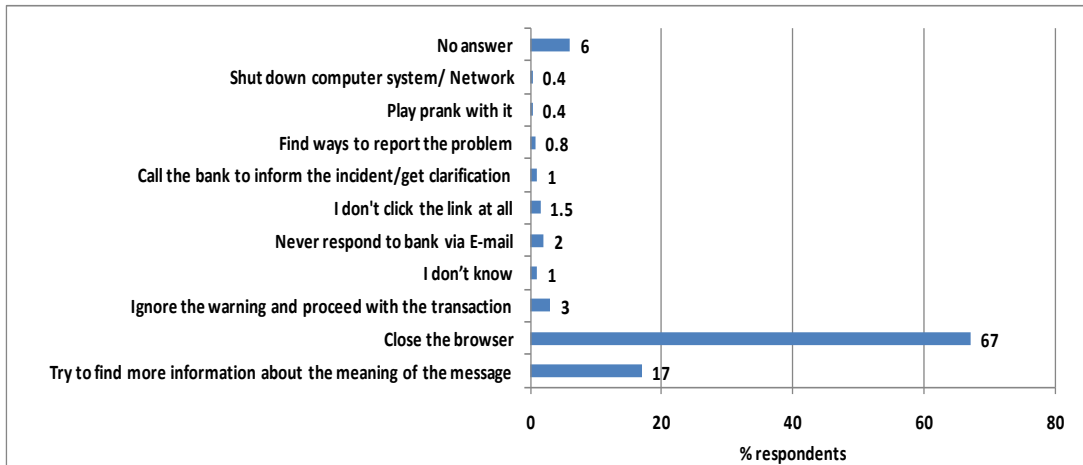


Figure 3-1: Responses to phishing warning – Mozilla Firefox

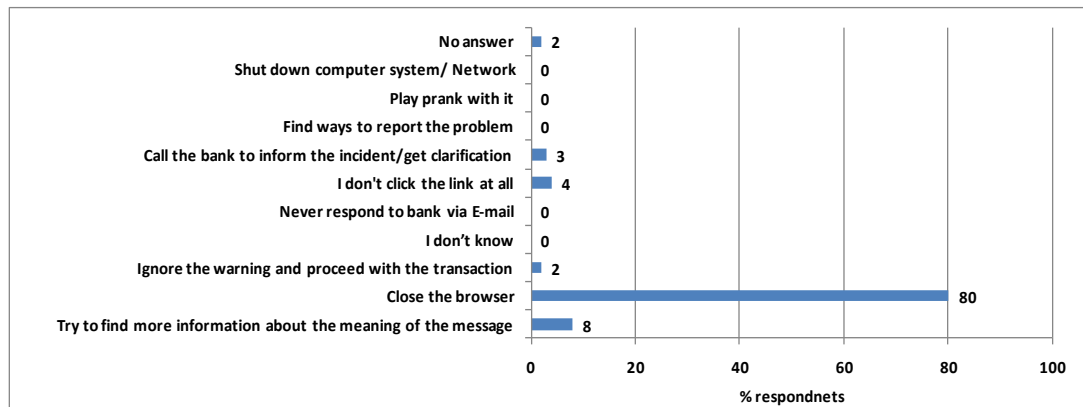


Figure 3-2: Responses to phishing warning – Internet Explorer 8

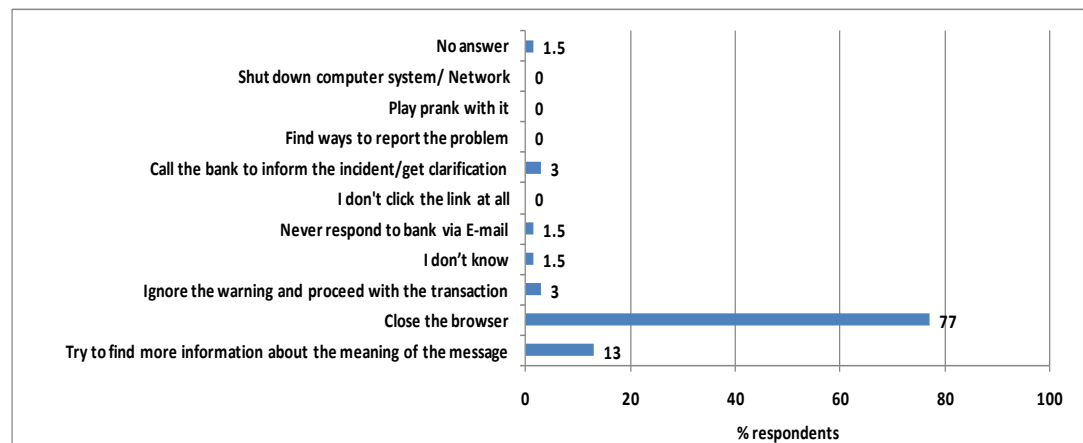


Figure 3-3: Responses to phishing warning – Internet Explorer 7

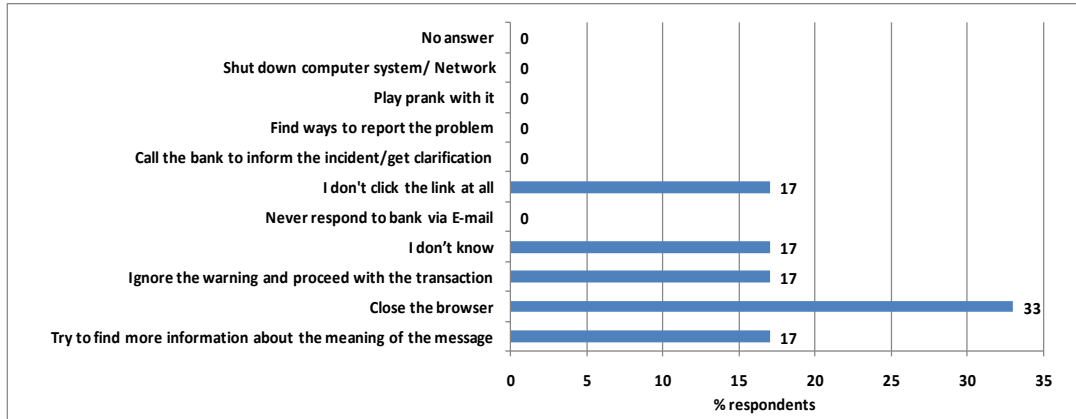


Figure 3-4: Responses to phishing warning – Opera

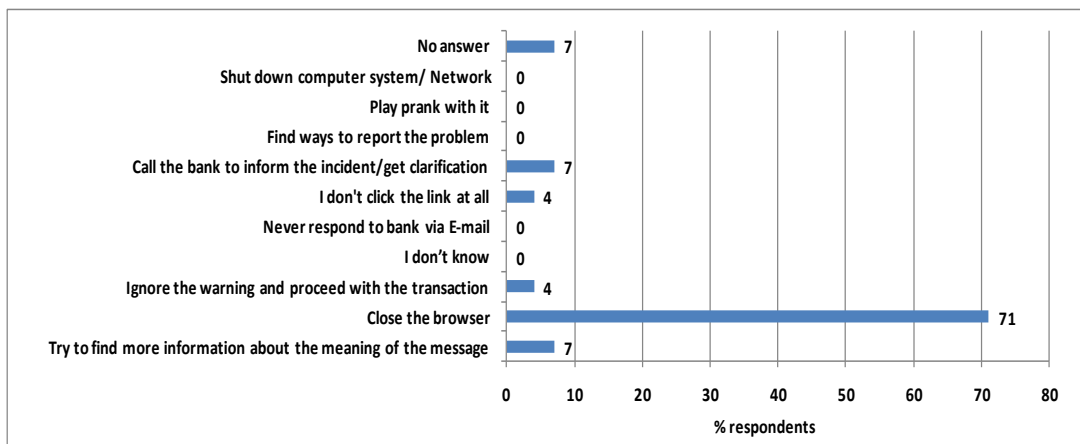


Figure 3-5: Responses to phishing warning – Safari

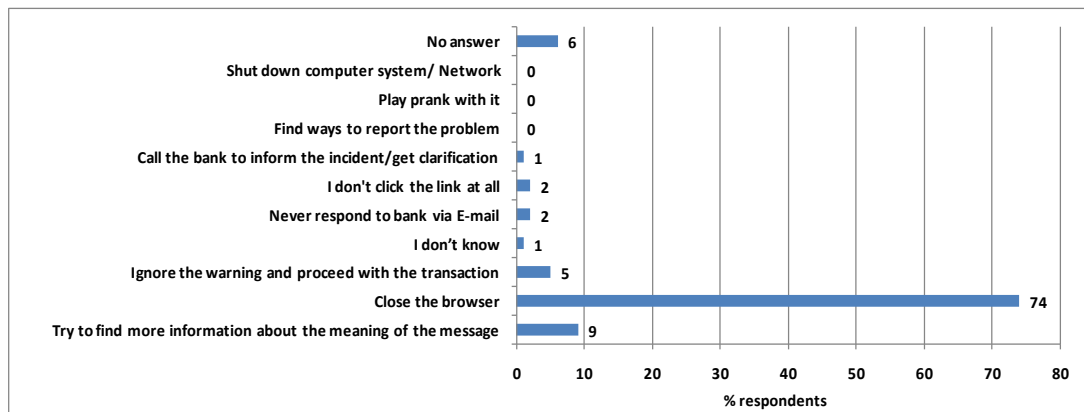


Figure 3-6: Responses to phishing warning – Chrome

Section 4: Computer Scenario Study

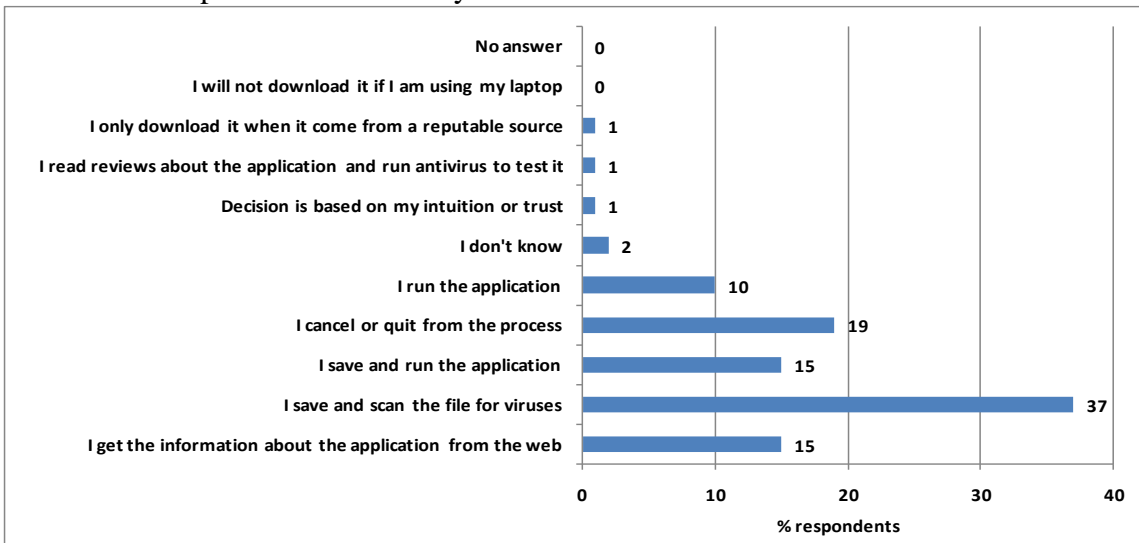


Figure 3-7: Internet Explorer 8 Security pop up respondents' decisions

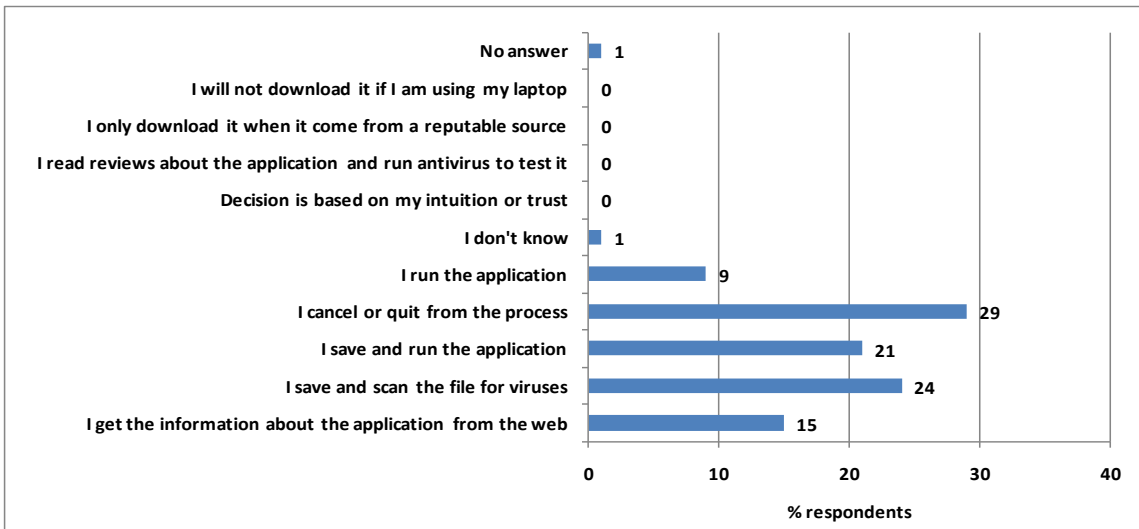


Figure 3-8: Internet Explorer 7 Security pop up respondents' decisions

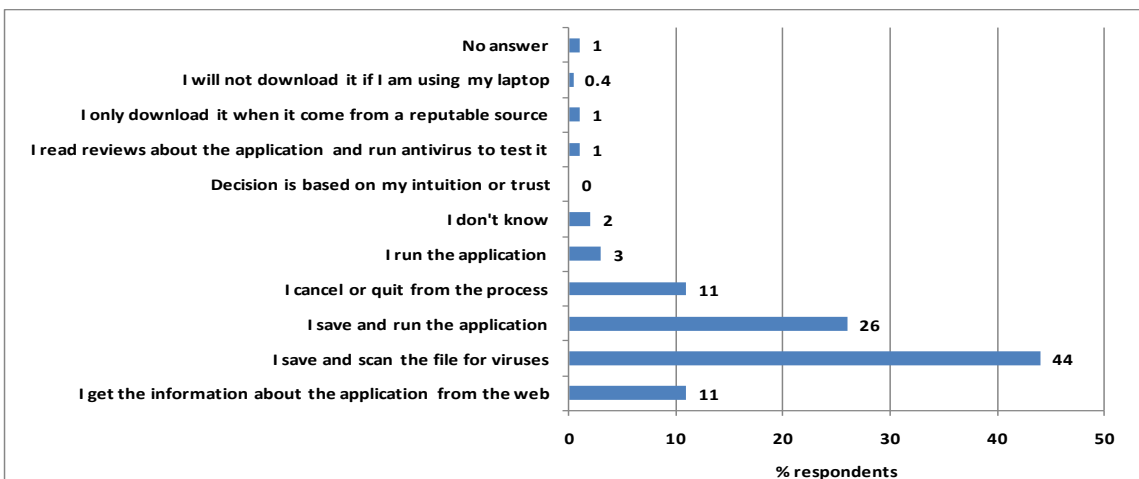


Figure 3-9: Mozilla Firefox Security pop up respondents' decisions

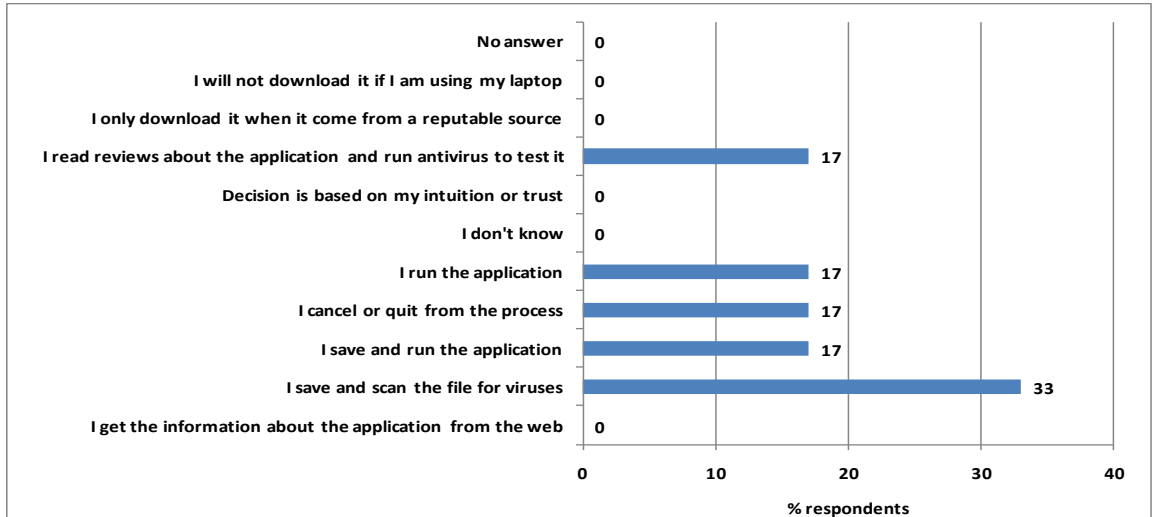


Figure 3-10: Opera Security pop up respondents' decisions

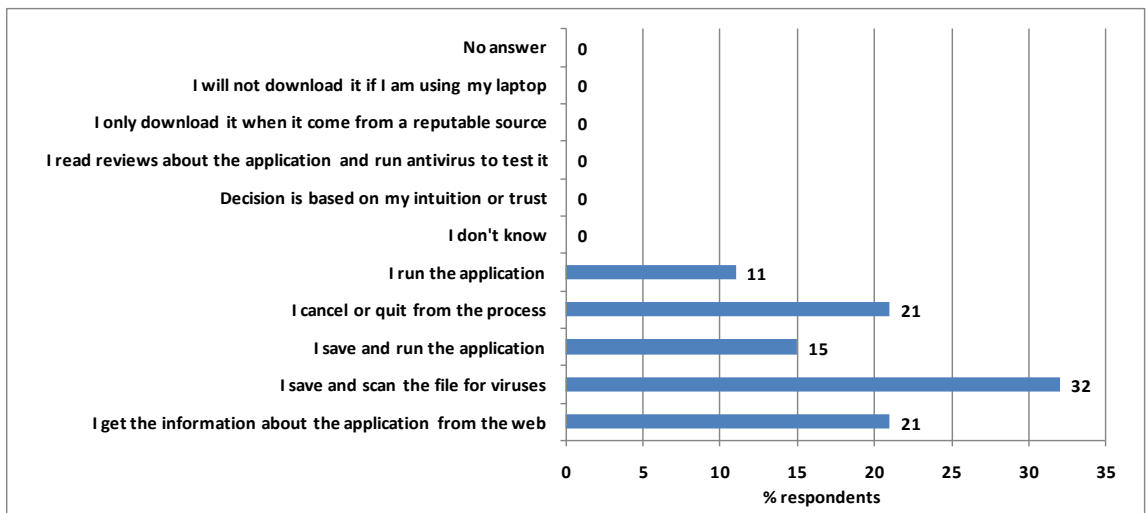


Figure 3-11: Safari Security pop up respondents' decisions

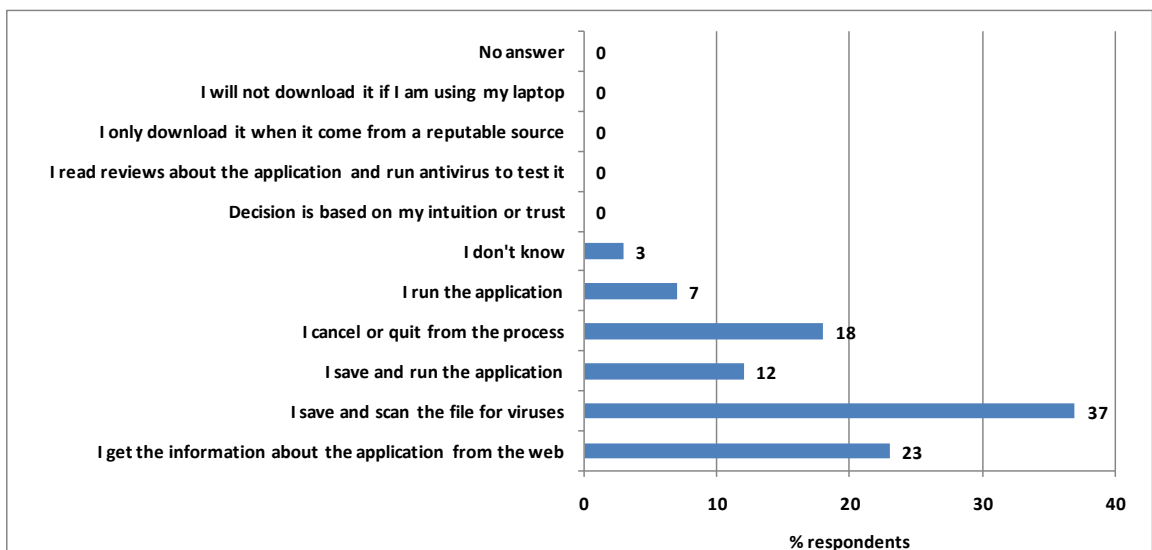


Figure 3-12: Chrome Security pop up respondents' decisions

Appendix B

User Study 2 Documentation

Faculty of Science and Technology



Smeaton 009, Plymouth

To:	Zaru Zaaba	From:	Paula Simson
cc:	Prof Steven Furnell		Secretary to Human Ethics Committee
Your Ref:		Our Ref:	scitech:\d:\human ethics:
Date:	31 March 2011	Phone Ext:	84503

Application for Ethical Approval

Thank you for submitting the ethical approval form and details or the amendments concerning your project:

'Information security: A usability perspective of security features in computer'

I am pleased to inform you that this has been approved.

Kind regards

Paula Simson

UNIVERSITY OF PLYMOUTH
FACULTY OF SCIENCE AND TECHNOLOGY

Human Ethics Committee Sample Consent Form

CONSENT TO PARTICIPATE IN RESEARCH PROJECT / PRACTICAL STUDY

Name of Principal Investigator

Zarul Fitri Zaaba

Title of Research

Information security: A usability perspective of security features in computer

Brief statement of purpose of work

The U-Surf system is being used to conduct a survey as part of the PhD project at the University of Plymouth. The aim of this study are to give users the practical exposure on dealing with security warning/message and to investigate how end users' understand these features with regard to the usage of computer application on daily basis. This finding will help to determine the features that easily to be understood compare to currently tend to cause difficulty. Hence, it will lead to the potential for new approaches to improve the usability of security warning/message in computer respectively. Please note that you are going to use this program only for 14 days.

The objectives of this research have been explained to me.

I understand that I am free to withdraw from the research at any stage, and ask for my data to be destroyed if I wish.

I understand that my anonymity is guaranteed, unless I expressly state otherwise.

I understand that the Principal Investigator of this work will have attempted, as far as possible, to avoid any risks, and that safety and health risks will have been separately assessed by appropriate authorities (e.g. under COSHH regulations). Under these circumstances, I agree to participate in the research.

Name:

Signature:

Date:

UNIVERSITY OF PLYMOUTH**FACULTY OF SCIENCE AND TECHNOLOGY****Research Information Sheet**

Principal Investigator : Zarul Fitri Zaaba

Title of Research : Information security: A usability perspective of security features in computer

Introduction & Aim :

The U-Surf system is being used to conduct a survey as part of the PhD project at the University of Plymouth. The aim of this study is to examine how end users understand and handle security-related events, notifications and warning messages that they may encounter during day-to-day use of their systems. This finding will help to determine the features that are most easily understood and those that tend to cause difficulty. Hence, it will lead to the potential for new approaches to improve the usability of such warnings/messages in future systems. Please note that you are asked to use this program only for 14 days. This study is designed for adults **aged 18 years or older**. Please read the following sections before continuing to ensure that you understand your rights to withdraw, the procedures of the study and issues relating to confidentiality and data protection.

Procedure: A step by step process

Please note that this program will be used for only 14 days for the purpose of experiment.

1. User will be given the consent form with details of research information. They will read and understand the procedure before they proceed with this study. If they agreed, they will give their signature.
2. Researcher will give respondents' guidance sheet and program installer. They will follow step by step procedure as stated in the guidance sheet until the program can be fully used.
3. Complete the capture process and the relevant questionnaire (that requires only few clicks which is less than 5 minutes) each time user encounter security message/ warning event when using computer
4. Finally, after 14 days of using the program, respondents' will send the completed questionnaire data to this e-mail (usurf2011@gmail.com). This will include a (Questionnaire) zip file contains database and folder of image captured.
5. Last step, after using sending the final results (zip files), they will have to uninstall the program from their computer. This process is provided in the guidance sheet section.

After 14 days

After 14 days, you will be required to send back the results. (Follow steps 4 in **Procedure**)

What happen to collected data:

All data from this study will be treated as confidential. Your responses can only be accessed by the principal investigator only for the purpose of this research project. Your responses will **not** contain any identifying information. Novel results may be published into one or more journal/conference articles. Data and references to any participants will be anonymised so that true identities are not revealed.

Description of Risk:

Please note that this study needs you to capture your experience dealing with security warning/message. There is no specific risk identified in this study as none of the results reported from the study will include information that allows identification of named individuals.

Benefits of study:

This study will help researcher to understand users' exposure towards the security warning/message and able to analyse what can be done to improve current security situation. In addition, this study able to give end users' knowledge and experience with regards to various types of security warning that they have day to day basis.

Right to Withdraw:

Respondent are able to quit or withdraw at any time. If they already have installed the program in their computer and decide to withdraw please refer to **Guidance sheet – Section D**. All information regarding the program installed will be deleted from your computer.

If you need further assistance please contact the principal investigator:-

Zarul Fitri Zaaba

Centre for Security Communications and Network Research (CSCAN)
A304 Portland Square
University of Plymouth
Drake Circus
Plymouth
PL4 8AA Telephone: 01752 586287, Email: zarul.zaaba@plymouth.ac.uk

Should you have any concerns about the way in which this study is being conducting please contact the secretary of the Faculty of Science and Technology Ethics Committee:

Paula Simson

Faculty of Science and Technology
Dean's Office
Smeaton 009
University of Plymouth
Drake Circus
Plymouth
PL4 8AA
Telephone: 01752 584503
Email: paula.simson@plymouth.ac.uk

Guidance Sheet

The U-Surf system is being used to conduct a survey as part of the PhD project at the University of Plymouth. The aim of this study is to examine how end users understand and handle security-related events, notifications and warning messages that they may encounter during day-to-day use of their systems. This finding will help to determine the features that are most easily understood and those that tend to cause difficulty. Hence, it will lead to the potential for new approaches to improve the usability of such warnings/messages in future systems. Please note that you are asked to use this program only for 14 days.

Step by step with illustration

A. Installation and registration

You are kindly required to:-

1. You have read, understand and agree to participate in this experiment by signing the consent form. Then you can start to use the program by following step by step actions to use the program.
2. Install this program (U-Surf System) by running the setup from the CD provided/Pen Drive. After the installation, click the notification balloon to complete the registration in **Figure 1**.



Figure 1 : Notification balloon for registration process

Personal details form will pop up. You will first need to read and understand the general information section.(It is a reminder about the program that you are going to use) By clicking the checkbox meaning that you are agree to participate in this study as depicted in **Figure 1.2**.

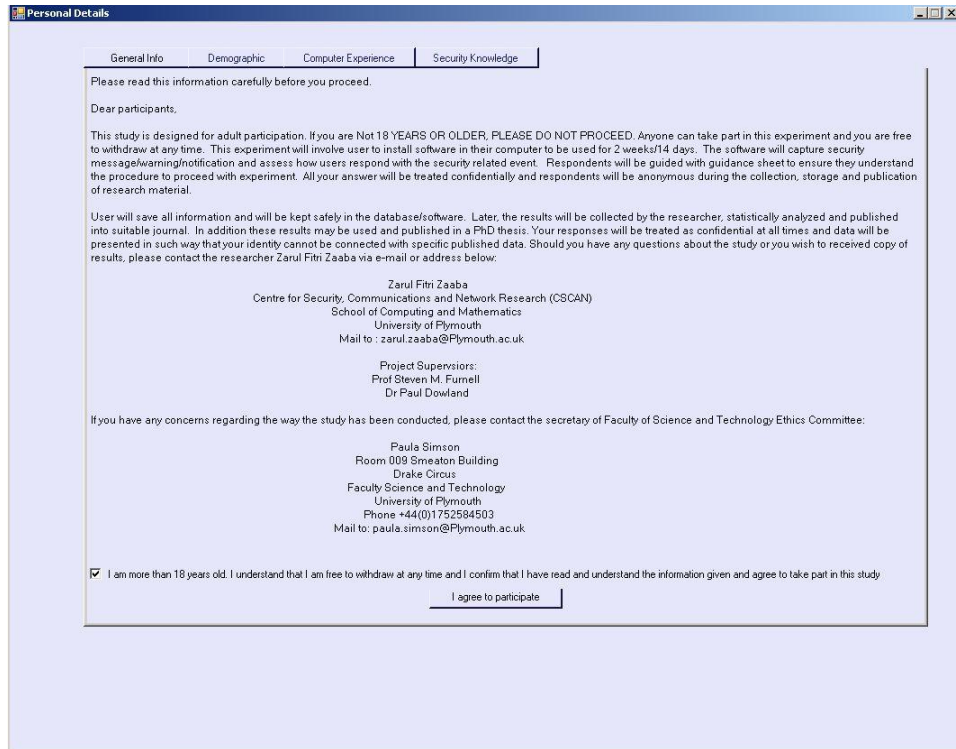


Figure 1.2 : Click the checkbox to proceed

Then you may proceed to next section until everything is saved as shown in **Figure 1.3- Figure 1.5**

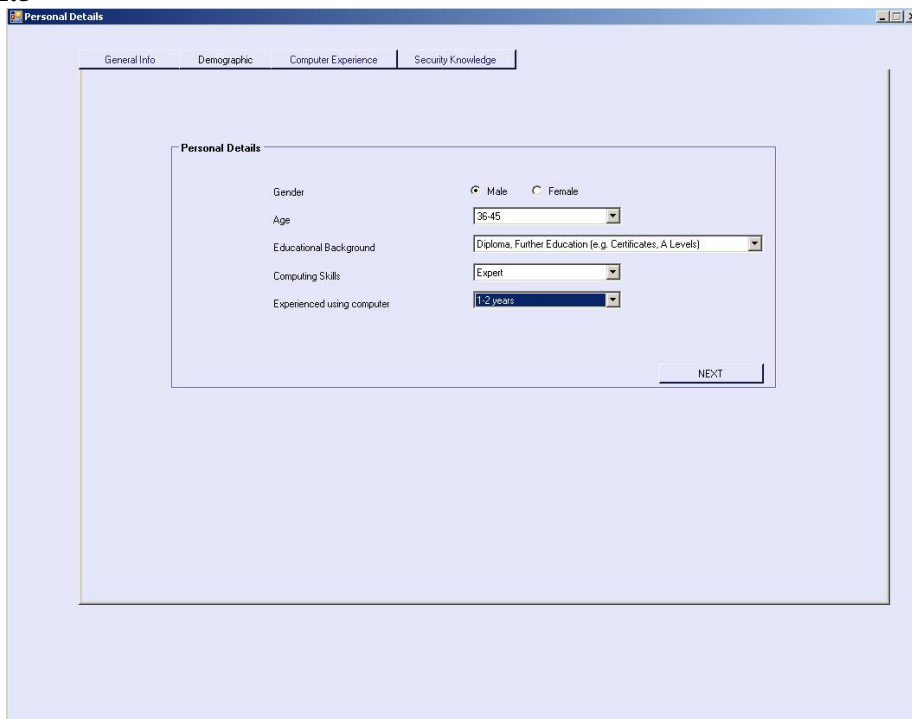


Figure 1.3: Demographic caption

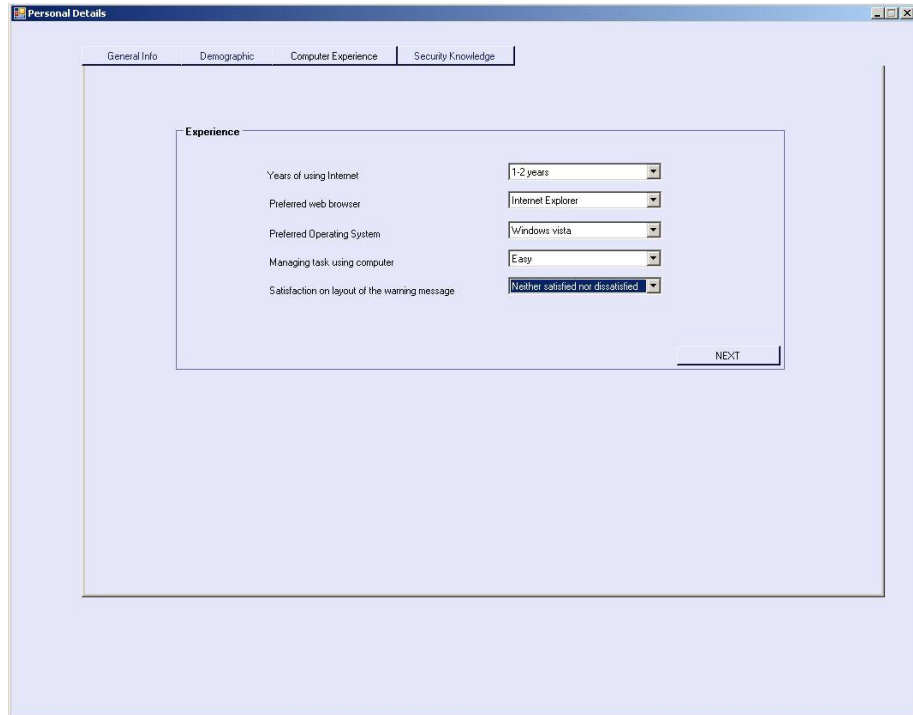


Figure 1.4: Computer Experience caption

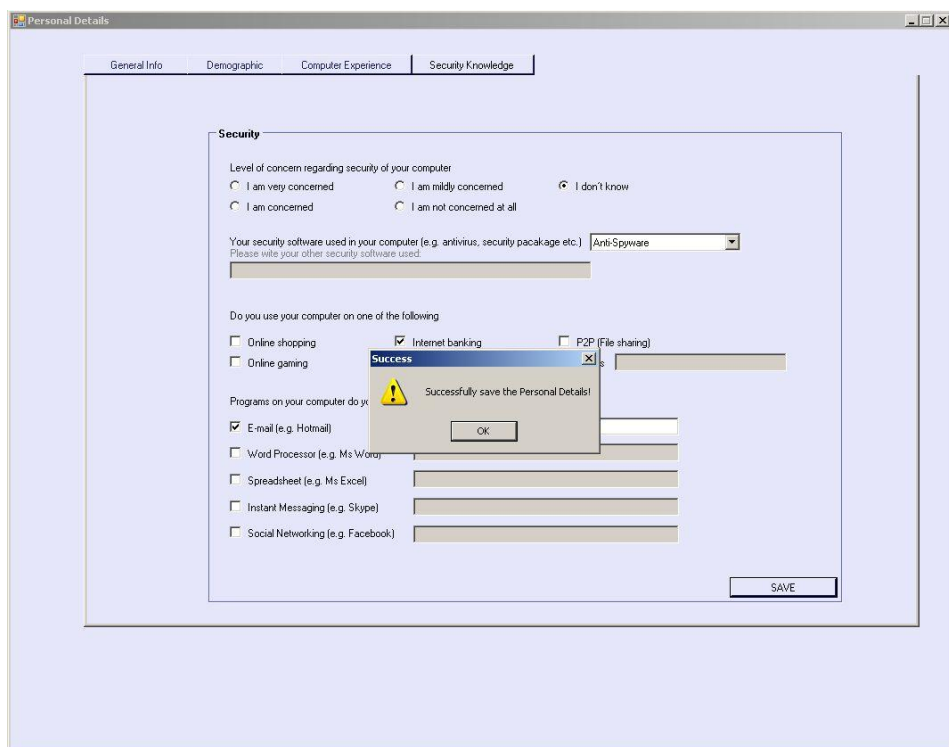


Figure 1.5: Security knowledge caption

(Click Ok when Information message pop up in **Figure 1.5** and program will seat back in your system tray) at this stage, you are not able to change anything in your personal details as it will be locked.

3. After you have saved the information in personal details, you are able to see small **Z** icon on the system tray in **Figure 1.6** . Right click the icon until you see list of menu. Please choose **run at startup** as depicted in **Figure 1.7**.



Figure 1.6: Notify icon in system tray



Figure 1.7: click right on notify icon and select Run at startup

4. Restart your computer. Then, you will see the Z icon in your system tray and you are officially can use the program installed.

B. Capture security warning/message & Answering Questionnaire

1. This program will always seat in your system tray and will not disturb your current task. If you are facing any security warning/message (e.g. security message upon downloading application from website in **Figure 1.8**, press ALT then Z slowly. Please wait until you can see notification balloon from you system tray stated “**You have successfully saved the Screen Capture..... click the notification to proceed**” in **Figure 1.9**.

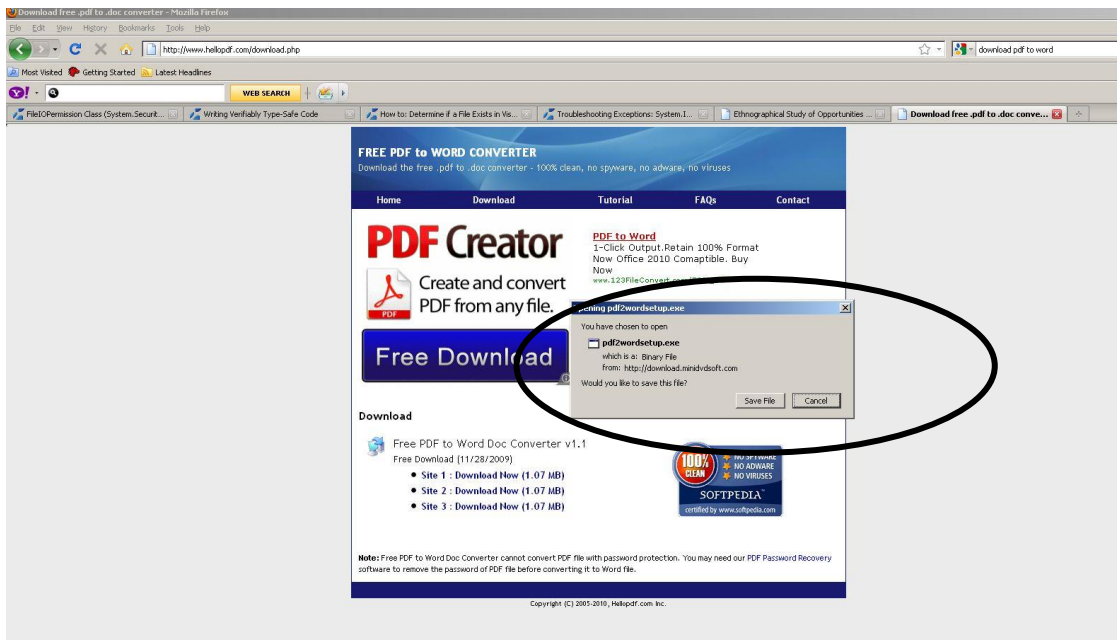


Figure 1.8: Capturing image of security warning (in round shape) when downloading application from Internet.

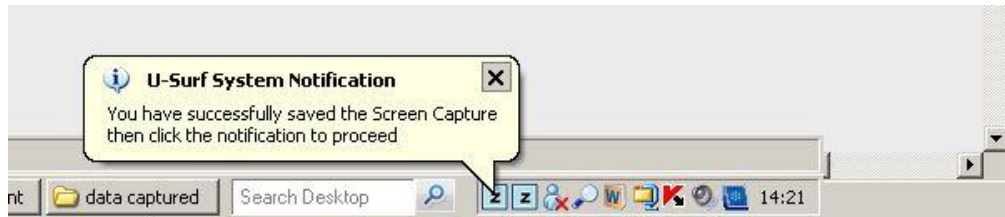


Figure 1.9: Notification successfully captured image

2. You may decide to answer the questionnaire straight away by clicking the balloon notification. Then, form questionnaire will be presented as shown in **Figure 1.10**

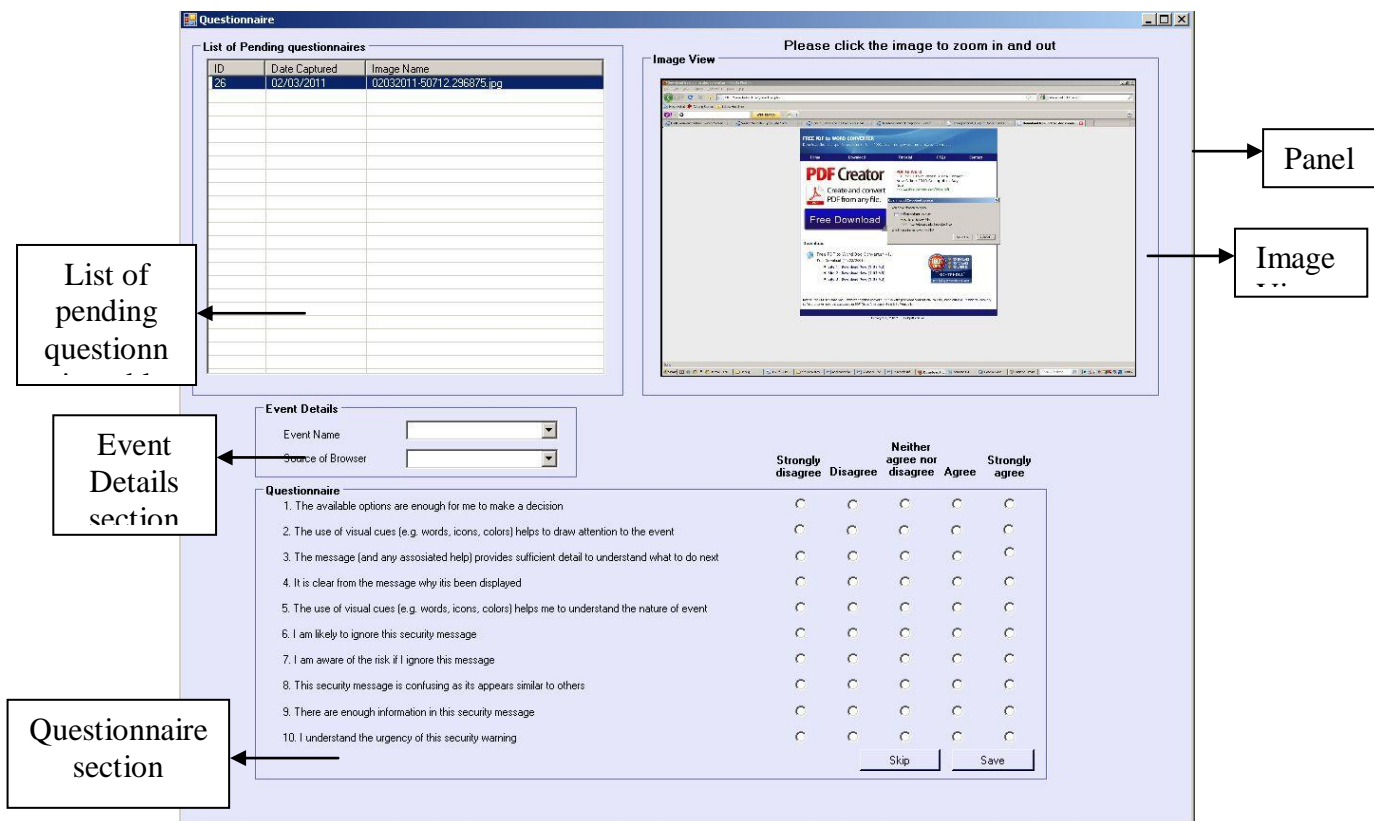


Figure 1.10: Form questionnaire

3. You also may decide to complete it at your convenient time. If you would like to do it at any time, clicks the icon Z from system tray. Then, form questionnaire will be presented again.

4. To complete the questionnaire, firstly, you will click any 1 item in List of pending questionnaire. Then, on right of the **List of pending questionnaire** table, it will preview the image in the **Image View** that you have captured. You can click the image to zoom in and out(Note: once you mouse hover inside the Image View, the border will change to blue color and the mouse change to magnifying glass icon). Then after you have clicked (zoom in) the image, you can control the **panel** movement to see the specific warning/message that you have captured.

5. Later, you will have to answer questions with regards to the image that you viewed. All questions are compulsory to answer. If you decide to do it later, press skip button (It will bring the program back to system tray). If you satisfied with your choices, press save button until you see message saying that it is successfully saved as shown in **Figure 1.11** . Click Ok.

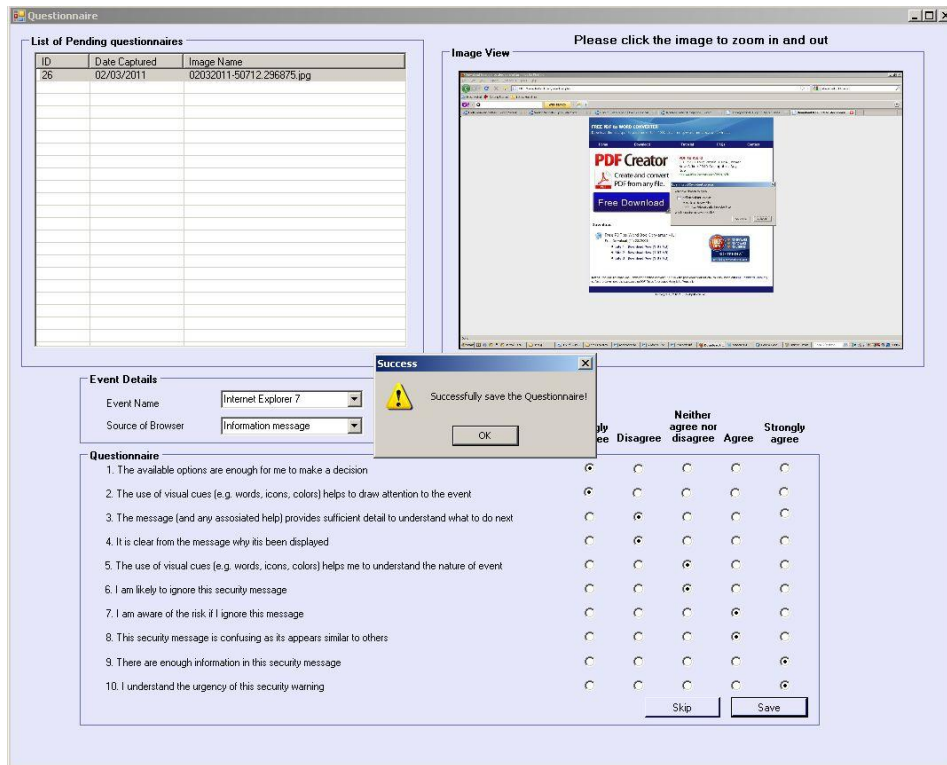


Figure 1.11: Information notification saying the data is saved

C. After completed study (14 days)

You are required to send a zip folder document from your computer by e-mail to (**usurfsupport@gmail.com**) or directly to the researcher Mr Zarul Fitri Zaaba (please refer address in **Help** section). Please note that the folder will be located on your desktop with the name questionnaire data (**ZIP file**).

D. Uninstall Program

Steps to uninstall your program (**Other than Windows 7**)

1. Click start. Go to setting then click control panel
2. Then, click Add/Remove programs. Wait few seconds
3. Find U-Surf System in the currently installed program list.
4. Click once, until you can see Remove button appears.
5. Click remove then yes.

If using **windows 7 only**

1. Click start. Go to setting then click control panel
2. Then, click program and features & you will see U-Surf System program in the list
3. Right click the program or click the program to uninstall
4. Then click ok to uninstall

E. Help

If you need further assistance please contact the principal investigator:-

Zarul Fitri Zaaba

Centre for Security Communications and Network Research (CSCAN)

A304 Portland Square

University of Plymouth

Drake Circus

Plymouth

PL4 8AA

Telephone: 01752586287

Email: zarul.zaaba@plymouth.ac.uk

Should you have any concerns about the way in which this study is being conducting please contact the secretary of the Faculty of Science and Technology Ethics Committee:-

Paula Simson

Faculty of Science and Technology

Dean's Office

Smeaton 009

University of Plymouth

Drake Circus

Plymouth

PL4 8AA

Telephone: 01752 584503

Email: paula.simson@plymouth.ac.uk

Figures from Chapter 4 – Results and findings

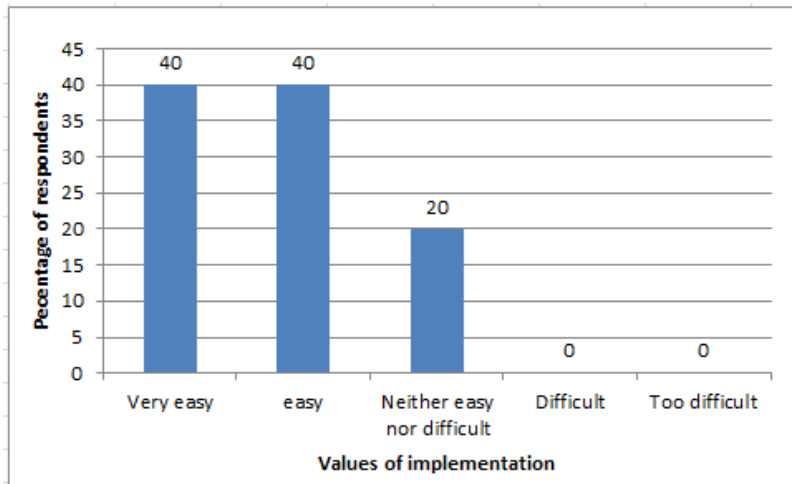


Figure 4-1: Managing tasks using computer

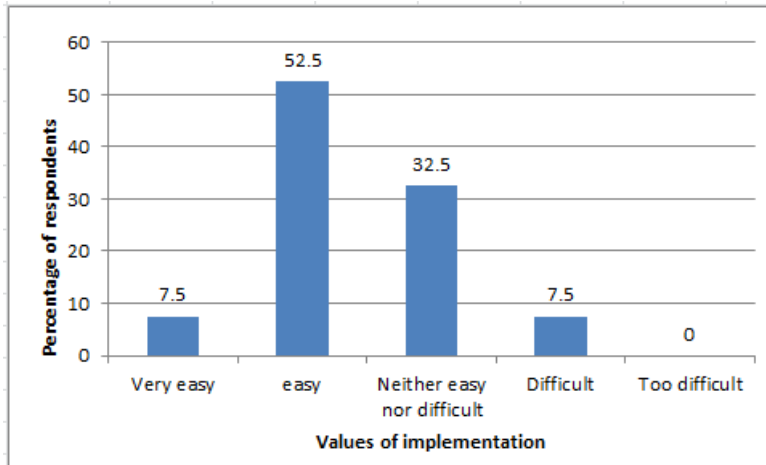


Figure 4-2: Satisfaction on layout of security warning

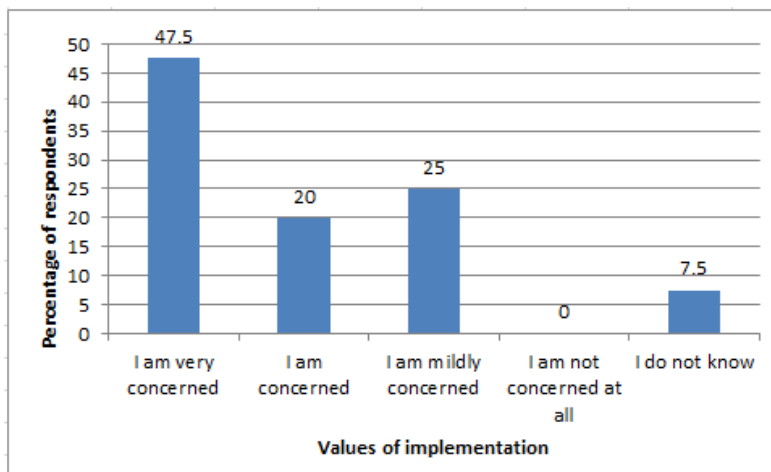


Figure 4-3: Level of concern for computer security.

Appendix C

User Study 3 Documentation

Faculty of Science and Technology

Smeaton 009, Plymouth

To:	Zarul Zaaba	From:	Paula Simson
cc:	Prof Steven Furnell, Dr Paul Dowland		Secretary to Human Ethics Committee
Your Ref:		Our Ref:	scitech:\d:\human ethics:
Date:	21 December 2011	Phone Ext:	84503

Application for Ethical Approval

Thank you for submitting the ethical approval form and details concerning your project:

'Security Usability Survey 2011'

I am pleased to inform you that this has been approved.

Kind regards



Paula Simson

UNIVERSITY OF PLYMOUTH

FACULTY OF SCIENCE AND TECHNOLOGY

Human Ethics Committee Sample Consent Form

CONSENT TO PARTICIPATE IN RESEARCH PROJECT / PRACTICAL STUDY

Name of Principal Investigator

Zarul Fitri Zaaba

Title of Research

Security Usability Survey 2011

Brief statement of purpose of work

The Security Usability Survey 2011 is being used to conduct a survey as part of the PhD project at the Plymouth University. The aim of this study is to examine how end users understand and handle security-related events, notifications and warning messages that they may encounter during day-to-day use of their systems. This finding will help to provide a proof that shows the needs to enhance the implementation of security message. Hence, it will lead to the potential for new approaches to improve the usability of such warnings/messages in future systems. Please note that you are asked to use this program for **5 days** only. This study is designed for adults **aged 18 years or older**. Please read the following sections before continuing to ensure that you understand your rights to withdraw, the procedures of the study and issues relating to confidentiality and data protection.

The objectives of this research have been explained to me. I understand that I am free to withdraw from the research at any stage, and ask for my data to be destroyed if I wish.

I understand that my anonymity is guaranteed, unless I expressly state otherwise.

I understand that the Principal Investigator of this work will have attempted, as far as possible, to avoid any risks, and that safety and health risks will have been separately assessed by appropriate authorities (e.g. under COSSH regulations). Under these circumstances, I agree to participate in the research.

Name:

Signature:

Date:

UNIVERSITY OF PLYMOUTH**FACULTY OF SCIENCE AND TECHNOLOGY****Research Information Sheet**

Principal Investigator : Zarul Fitri Zaaba
Title of Research : Security Usability Survey 2011
Introduction & Aim :

The Security Usability Survey 2011 is being used to conduct a survey as part of the PhD project at the Plymouth University. The aim of this study is to examine how end users understand and handle security-related events, notifications and warning messages that they may encounter during day-to-day use of their systems. This finding will help to provide a proof that shows the needs to enhance the implementation of security message. Hence, it will lead to the potential for new approaches to improve the usability of such warnings/messages in future systems. Please note that you are asked to use this program for **5 days** only. This study is designed for adults **aged 18 years or older**. Please read the following sections before continuing to ensure that you understand your rights to withdraw, the procedures of the study and issues relating to confidentiality and data protection.

Procedure: A step by step process

Please note that this program will be used for only **5 days** for the purpose of experiment.
1. Users will be given the consent form and research information form. If they agree to participate, they will give their signature before proceeding with the study.

2. The researcher will give respondents a guidance sheet and program installer. They will follow the step by step procedure as stated in the guidance sheet in order to prepare the program for use.

3. Firstly, user will fill in the demographic form and then the program will automatically capture images of any security-related dialogues that they encounter while using their system. Whenever any such dialogue is encountered, the user will subsequently be presented with a second dialogue box with questions about security their decision making process. All of their responses will be saved for future analysis in the research.

4. After 5 days of using the program, respondents will be instructed to generate a zip file containing the database and folder of captured images. The respondent will then be instructed to send the data using dropbox (a program that the user will have to install from the specified link) or by giving the file manually to principal investigator using pen drive.

(Note: Dropbox: is an application that allows users to share files up to 2GB online. The Principal Investigator will only be able to access the file after the respondent has e-mailed a link to the principal investigator. Please refer to guidance sheet)

5. Finally, after sending the final results, they will be instructed to uninstall the program from their computer. This process is provided in the guidance sheet section 4.

After 5 days

After 5 days, you will receive e-mail reminder to send the results to researcher. (Follow steps 4 in **Procedure**)

What happen to collected data:

All data from this study will be treated as confidential. Your responses can only be accessed by the principal investigator only for the purpose of this research project. Your responses will **not** contain any identifying information. Novel results may be published into one or more journal/conference articles. Data and references to any participants will be anonymised so that true identities are not revealed.

Description of Risk:

Please note that this study will capture security message in background as it will detect it automatically. There is no specific risk identified in this study as none of the results reported from the study will include information that allows identification of named individuals.

Benefits of study:

This study will help the researcher to understand whether user can make a decision or not based on the security message that they received. In addition, this study able to give end users' knowledge and experience with regards to various types of security warning that they encounter day to day basis.

Right to Withdraw:

Respondent are able to quit or withdraw at any time. If they already have installed the program in their computer and decide to withdraw please refer to **Guidance sheet – Section 4**. All information regarding the program installed will be deleted from your computer.

If you need further assistance please contact the principal investigator:-

Zarul Fitri Zaaba

Centre for Security Communications and Network Research (CSCAN)

A304 Portland Square

University of Plymouth

Drake Circus

Plymouth

PL4 8AA

Telephone: 01752 586287, Email: zarul.zaaba@plymouth.ac.uk

Should you have any concerns about the way in which this study is being conducting please contact the secretary of the Faculty of Science and Technology Ethics Committee:

Paula Simson

Faculty of Science and Technology

Dean's Office

Smeaton 009

University of Plymouth

Drake Circus

Plymouth

PL4 8AA

Telephone: 01752 584503, Email: paula.simson@plymouth.ac.uk

Guidance Sheet

There are 5 sections that you have to deal with:

- 1. Installation**
- 2. User’s main task**
- 3. Sending the results (After the program has been used for 5 days)**
- 4. Uninstall process**
- 5. Help**

Please follow **step by step**:

1. Installation



Figure 1

1. Install the program by choosing setup.exe and you will see Setup-CSCAN Security Survey. Click **Next**.

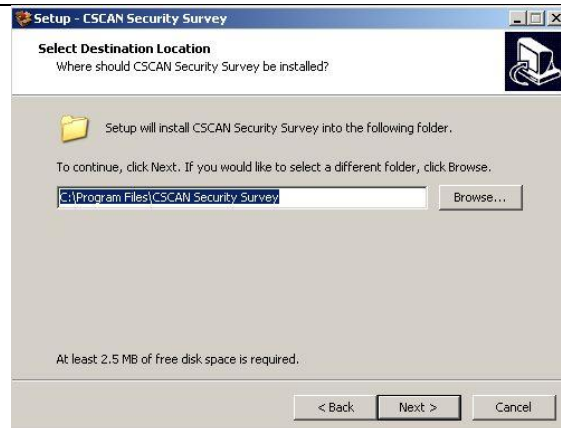


Figure 2

2. Click **Next**

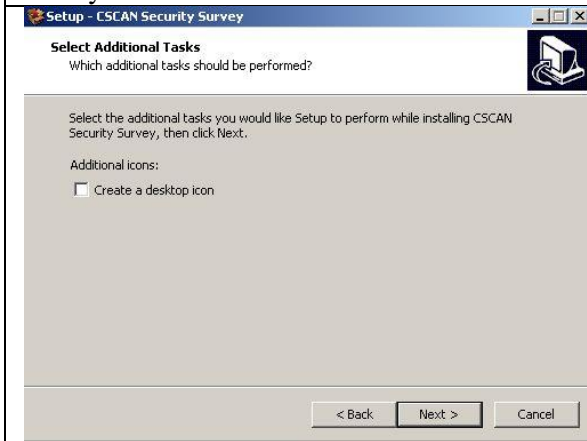


Figure 3

3. Click **Next**

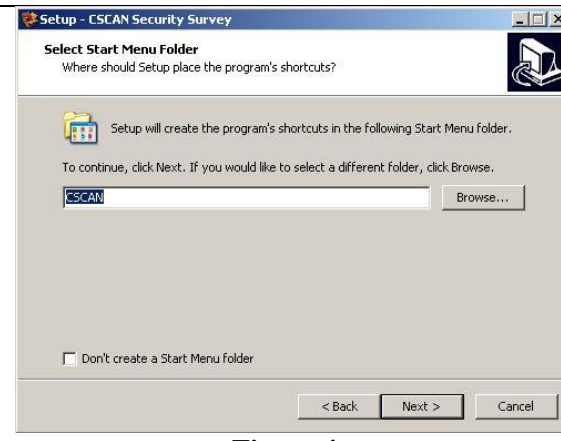


Figure 4

4. Click **Next**

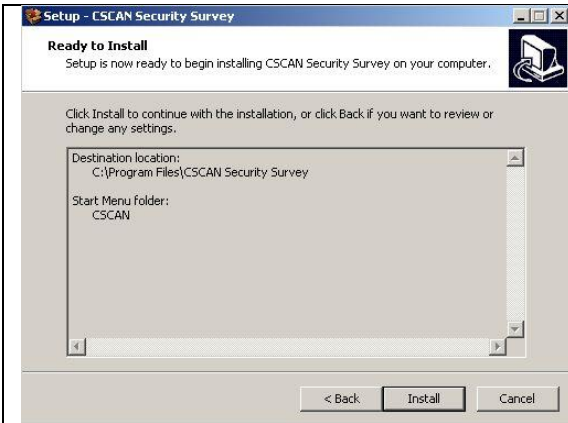


Figure 5

5. Choose **Install**



Figure 6

6. Click **Finish** and leave (Tick) on launch CSCAN security message



Figure 7



Figure 8

7. Shortly after that, you receive demographic form and balloon notification (C icon) as shown in Figure 7 and Figure 8. Please fill in the demographic form (Figure 7). All fields are compulsory. Then click Finish Survey.

2. Users' main task

- i. Use your computer like usual.
- ii. This program will detect security message automatically and you will have to answer as shown in Figure 10
- iii. See Example below:

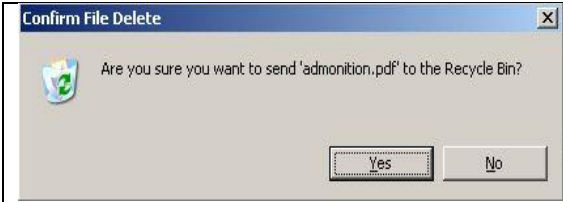


Figure 9

1. Assume that you receive this security message (It will be detected automatically by the program). You need to make a decision on it. Choose any of your preference answer.

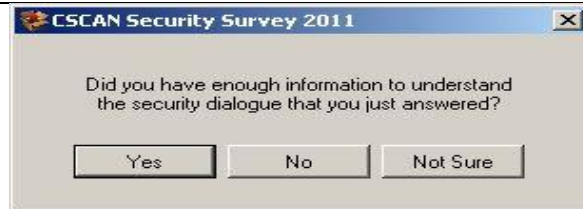


Figure 10

2. After you made a decision (By clicking Yes, No or X on Figure 9), the dialogue box (Figure 10) will be pop up to ask you with a question. Choose your answer accordingly and it will be saved in the database.

Note: The program will automatically detect the security message. Users' responsibility is only to answer the dialogue box pop up as shown in Figure 10.

3. Sending the results (After the program has been used for 5 days)

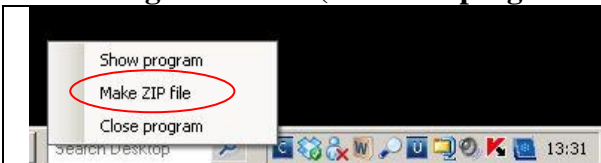


Figure 11

1. **Right click** the C icon and choose **Make Zip file**. This will create a zip file on your desktop (Contains data image capture and database)

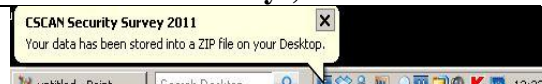


Figure 12

2. You will receive a balloon notification when the creation of zip file is successful.



Figure 13

3. This is the example of zip file created on your desktop.

There are 2 methods to send back the outcome of the study.

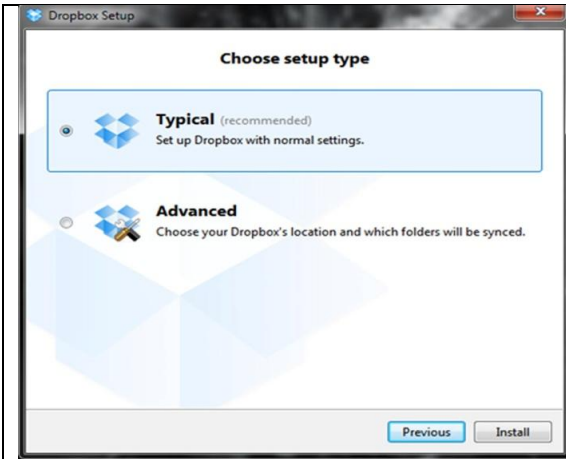
1. Attach the file from your computer (Figure 13) and send directly to usurf2011@gmail.com

Or

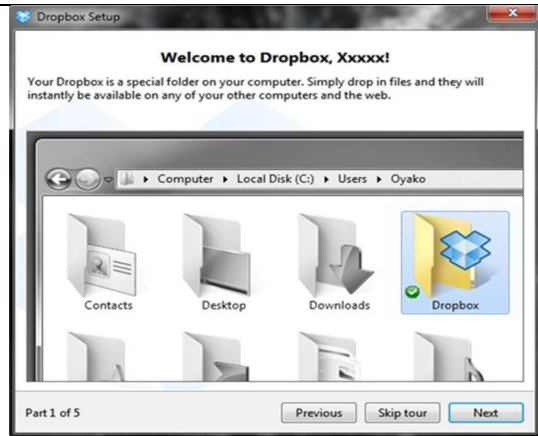
2. If the file attachment is too large, please use **Dropbox** method instead.

In order to proceed with this, you have to download the free **Dropbox** software from this link <http://www.dropbox.com>. Please click download to proceed and follow these instructions accordingly.

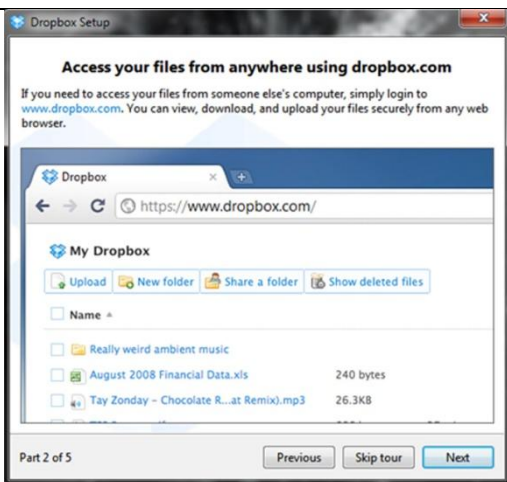
<p>1. You received security warning (it depend on the browser that you use). Click run or save (In other type of browser. Then activate it by double click the saved file)</p>	<p>2. Click Install</p>
<p>3. You receive the progress page</p>	<p>4. Choose I don't have DropBox account (default) and click Next. Choose I already have a drop box account if you had one.</p>
<p>5. If you have chosen I don't have Dropbox account, please fill in the details, tick the box(Terms of Service) and click Next</p>	<p>6. Choose 2GB (Free) instead and click Next</p>



7. Choose **Typical** and **Install**



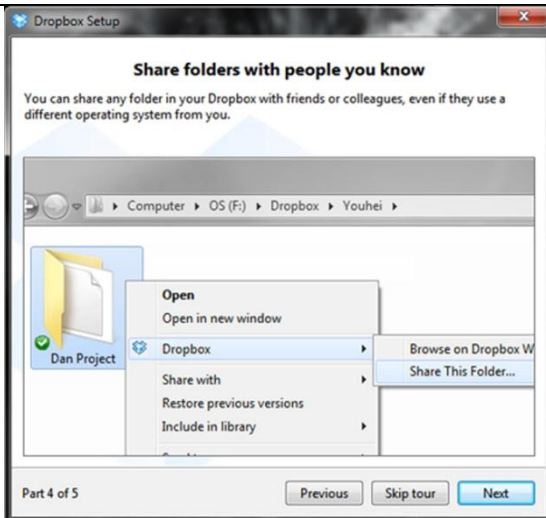
8. You will receive “Welcome to Dropbox, <Your name>” and click **Next**



9. Click **Next**



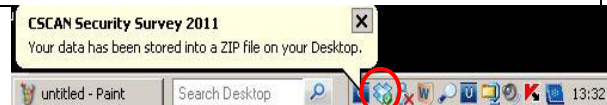
10. Click **Next**



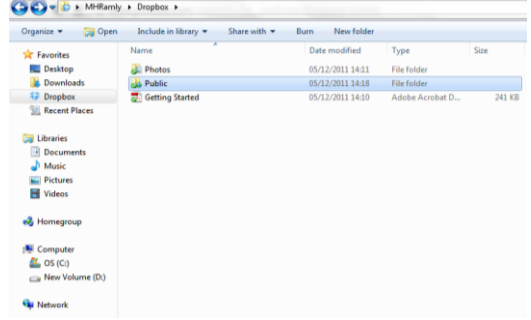
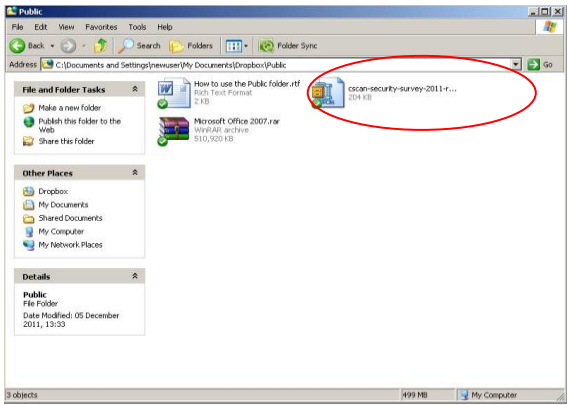
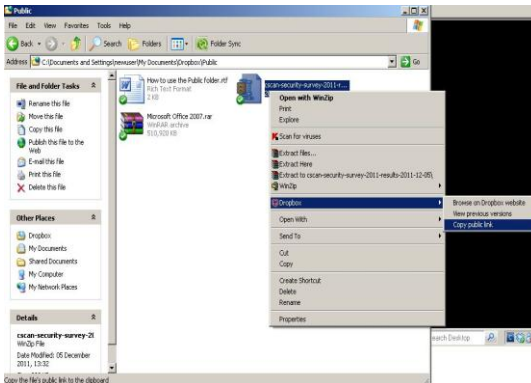
11. Click **Next**



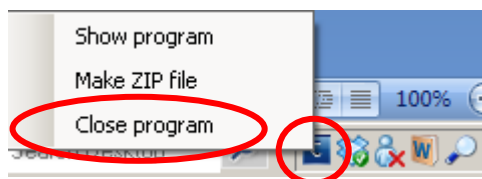
12. Click **Finish** (officially you have installed the Dropbox in your computer)



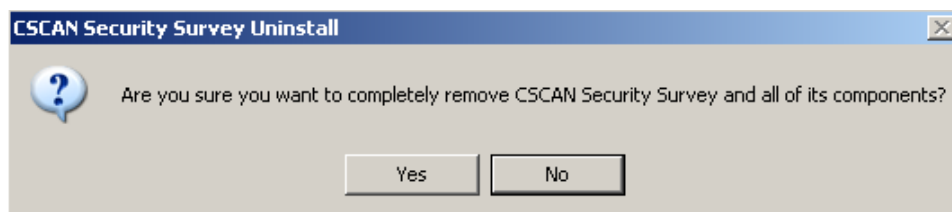
13. Double click Dropbox icon on your system tray

	 <p>14. The interface after clicking the dropbox icon is likely to be this.</p>
 <p>15. Click the public folder and copy the zip file (Figure 13) on your desktop and paste it in public folder. Wait until the Tick icon(green background) appears. It means that the file is fully loaded.</p>	 <p>16. Right click the file that has been pasted, choose DropBox, choose copy public link. (Here, it will automatically generate the link/URL)</p>
<p>17. Instantly, open your e-mail and paste the link (Right click and choose paste). Send it to usurf2011@gmail.com</p>	

4. Uninstall Process



1. Right click C icon on your system tray and choose **Close program**
2. On your computer, Click Start – Program - CSCAN
3. Choose Uninstall



4. You will receive CSCAN Security Survey Uninstall dialogue box and click **Yes**.
5. Uninstall process completed

5. Help

If you need further assistance please contact the principal investigator:

Zarul Fitri Zaaba

Centre for Security Communications and Network Research (CSCAN)
A304 Portland Square
University of Plymouth
Drake Circus
Plymouth
PL4 8AA
Telephone:01752586287
Email: zarul.zaaba@plymouth.ac.uk

Should you have any concerns about the way in which this study is being conducting please contact the secretary of the Faculty of Science and Technology Ethics Committee:-

Paula Simson

Faculty of Science and Technology
Dean's Office
Smeaton 009
University of Plymouth
Drake Circus
Plymouth
PL4 8AA
Telephone: 01752 584503
Email: paula.simson@plymouth.ac.uk

Appendix D

User Study 4 Documentation

Faculty of Science and Technology

Smeaton 009, Plymouth

To:	Zarul Zaaba	From:	Paula Simson
cc:			Secretary to Human Ethics Committee
Your Ref:		Our Ref:	scitech:\d:\human ethics:
Date:	6 November 2012	Phone Ext:	84503

Application for Ethical Approval

Thank you for submitting the ethical approval form and details concerning your project:

'Automated Security Interface Adaption (ASIA)'

I am pleased to inform you that this has been approved.

Kind regards



Paula Simson

UNIVERSITY OF PLYMOUTH
FACULTY OF SCIENCE AND TECHNOLOGY

Human Ethics Committee Consent Form

CONSENT TO PARTICIPATE IN RESEARCH PROJECT / PRACTICAL STUDY

Name of Principal Investigator

Zarul Fitri Zaaba

Title of Research

Automated Security Interface Adaptation (ASIA)

Brief statement of purpose of work

Automated Security Interface Adaptation (ASIA) is being used to conduct an experiment as part of a PhD project at Plymouth University. This research is about the adaptation of security warnings (i.e. messages, notifications, pop ups) that you may receive on PC systems. The Automated Security Interface Adaptation (ASIA) prototype presents you with a series of warnings and then attempts to adapt one of them into a new version based on your preferences. This study will help to provide evidence of how security warnings should be best presented to support and inform their users. This study is designed for adults **aged 18 years or older**. Please read the following sections before continuing to ensure that you understand your rights to withdraw, the procedures of the study and issues relating to confidentiality and data protection.

The objectives of this research have been explained to me.

I understand that I am free to withdraw from the research at any stage, and ask for my data to be destroyed if I wish.

I understand that my anonymity is guaranteed, unless I expressly state otherwise.

I understand that the Principal Investigator of this work will have attempted, as far as possible, to avoid any risks, and that safety and health risks will have been separately assessed by appropriate authorities (e.g. under COSHH regulations). Under these circumstances, I agree to participate in the research.

Name:

Signature:

Date:.....

**UNIVERSITY OF PLYMOUTH
FACULTY OF SCIENCE AND TECHNOLOGY**

Research Information Sheet

Principal Investigator : **Zarul Fitri Zaaba**

Title of Research (ASIA) : **Automated Security Interface Adaptation (ASIA)**

Introduction & Aim :

Automated Security Interface Adaptation (ASIA) is being used to conduct an experiment as part of a PhD project at Plymouth University. This research is about the adaptation of security warnings (i.e messages, notifications, pop ups) that you may receive on PC systems. The Automated Security Interface Adaptation (ASIA) prototype presents you with a series of warnings and then attempts to adapt one of them into a new version based on your preferences. This study will help to provide evidence of how security warnings should be best presented to support and inform their users. This study is designed for adults **aged 18 years or older**. Please read the following sections before continuing to ensure that you understand your rights to withdraw, the procedures of the study and issues relating to confidentiality and data protection.

Procedure: A step by step process

A step by step summary of the actions involved in the study is as follows:

1. Volunteers will be given the consent and research information forms. If they agree to participate, they will give their signature before proceeding with the study. The PI will also highlight that they has the right to withdraw at any stage of experiment.
2. The PI will give participants a guidance sheet to help them understand the flow of the experiment and they are allowed to ask questions to clarify anything related to the experiment.
3. Firstly, users will be told by the PI that this experiment is a role-based study where users will play a role as management trainee in the IT Company. The experiment will begin when users click the “Begin” button which takes them to a brief demographics questionnaire section. They must complete all questions before proceeding.
4. Then, users are presented with 7 tasks, which each involve presenting a security warning and asking the user their opinion about its clarity and any further information that may help them. They will indicate their preference(s) on every task they are dealing with. After the last task, participants will receive a dialogue box saying that one of the previous tasks will be repeated again. Then after clicking “Next” button, they will be presented with the first enhanced version of a security warning that has been created by the system. With this security warning, if user does not click “Help” button then the PI will intervene with some questions. Shortly after that, user will click help to proceed.

5. After that, the PI will take over the session (section 3) where the questionnaire and interview sessions will take place. A questionnaire paper will be completed by the participant, followed by interview discussion with the PI.

(Note: In this section, users will be presented with standard security warning, followed by the questionnaire and interview. In the next part, users will be presented with an enhanced security warning, followed by further questionnaire and interview activity. Finally, the last part will involve the user being shown the full version of security warning (i.e. if they click all options in the checkbox in task 7)).

6. Finally, the participant will be asked few questions related to usability of security warning and their preferences. All of the conversation bits will be voice recorded and manually written in a log book by the PI.

What happen to collected data:

All data from this study will be treated as confidential. Your responses can only be accessed by the principal investigator only for the purpose of this research project. Your responses will **not** contain any identifying information. Novel results may be published into one or more journal/conference articles. Data and references to any participants will be anonymised so that true identities are not revealed.

Description of Risk:

Please note that this study will involve you to make choice(s) on the given tasks. At the final sections of this experiment, you will have to answer questionnaire and having interview which will be recorded and noted by the principal investigator. There is no specific risk identified in this study as none of the results reported from the study will include information that allows identification of named individuals.

Benefits of study:

This study will help the researcher to understand the effectiveness of the experiment to proof that the framework to enhance security warnings can be implemented in the future. In addition, this study able to give end users' knowledge and experience with regards to various types of security warning that they encounter day to day basis especially via the interview session.

Right to Withdraw:

Respondent are able to quit or withdraw at any time as mentioned in Guidance sheet and Research Information sheet.

If you need further assistance please contact the principal investigator:-

Zarul Fitri Zaaba

Centre for Security, Communications and Network Research (CSCAN)
A304 Portland Square
University of Plymouth
Drake Circus
Plymouth
PL4 8AA

Telephone: 01752 586287

Email: zarul.zaaba@plymouth.ac.uk

Should you have any concerns about the way in which this study is being conducting please contact the secretary of the Faculty of Science and Technology Ethics Committee:

Paula Simson

Faculty of Science and Technology
Dean's Office
Smeaton 009
University of Plymouth
Drake Circus
Plymouth
PL4 8AA


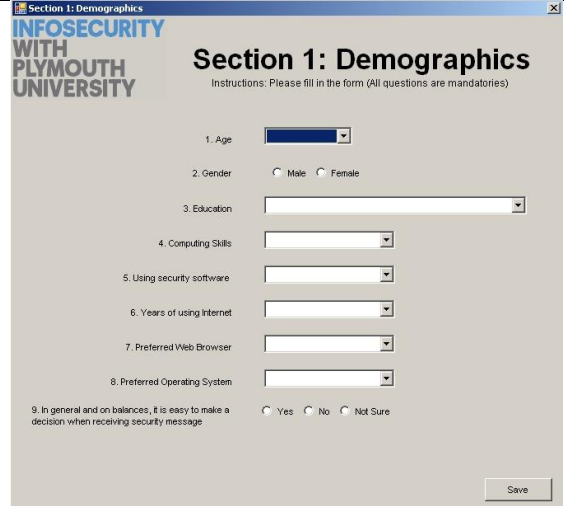
Telephone: 01752 584503

Email: paula.simson@plymouth.ac.uk

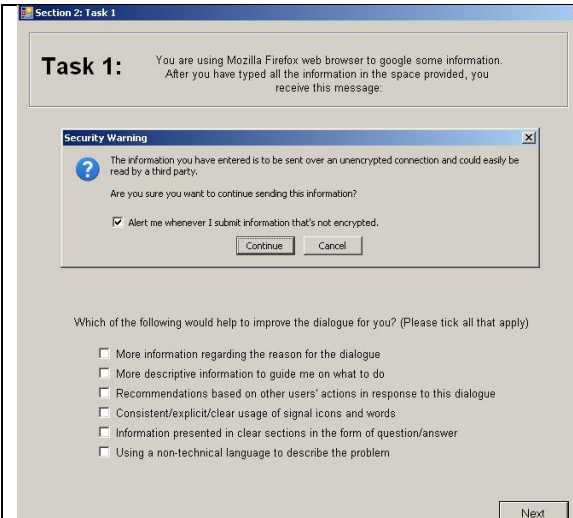
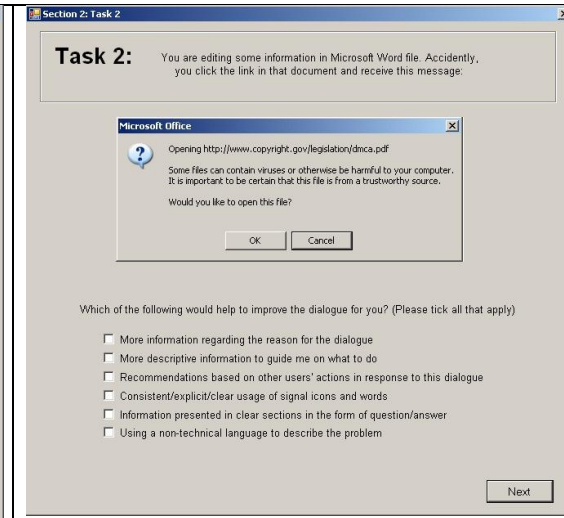
Guidance Sheet Automated Security Interface Adaptation

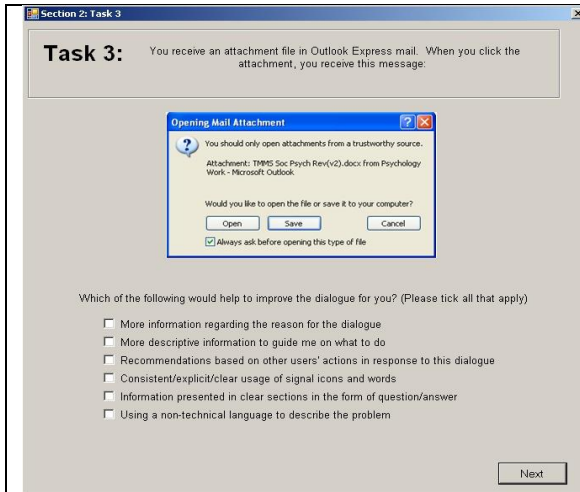
This guidance information will guide you to complete the experiment. There are 3 main sections that you will need to complete. All of this process will take approximately 40 minutes. You are allowed to ask any questions at any stage and you also have the **right to withdraw** at any time during this experiment. Please follow this guidance step by step. (**Note:** You are allowed to ask any questions if you facing any difficulties with this experiment).

Section 1: Demographics

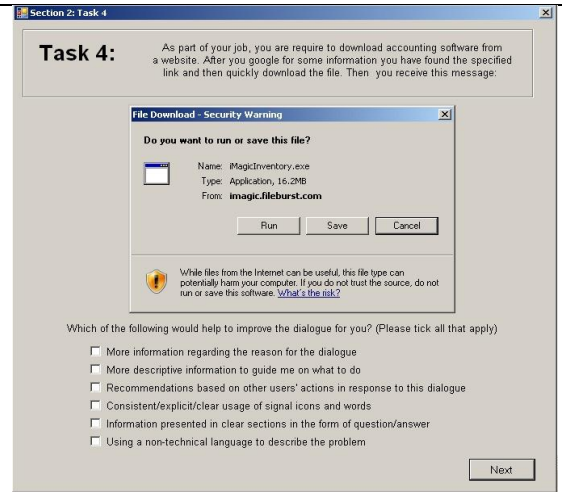
 <p style="text-align: center;">Read and understand the instructions and then click Begin.</p>	 <p style="text-align: center;">Fill in all required questions and click save.</p>
---	--

Section 2: 7 tasks and a repeated task

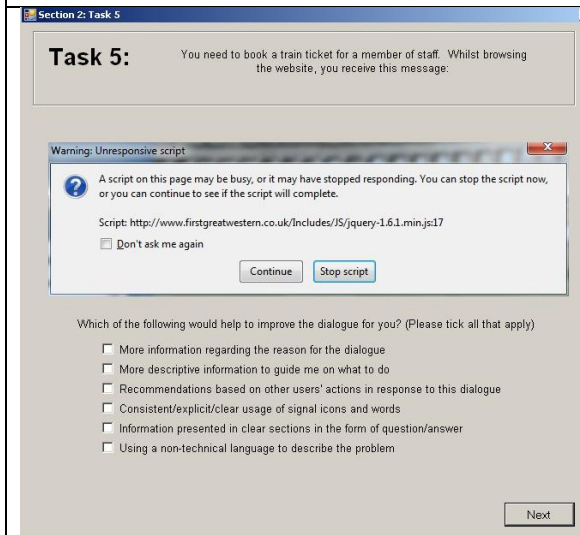
 <p style="text-align: center;">Please choose your preference(s) and click Next</p>	 <p style="text-align: center;">Please choose your preference(s) and click Next</p>
---	--



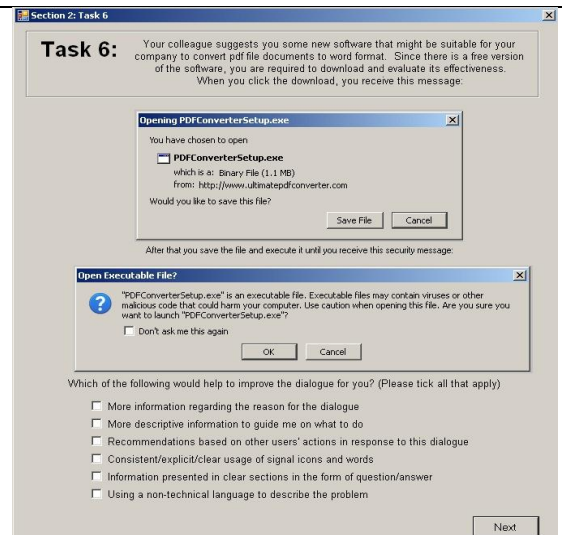
Please choose your preference(s) and click Next



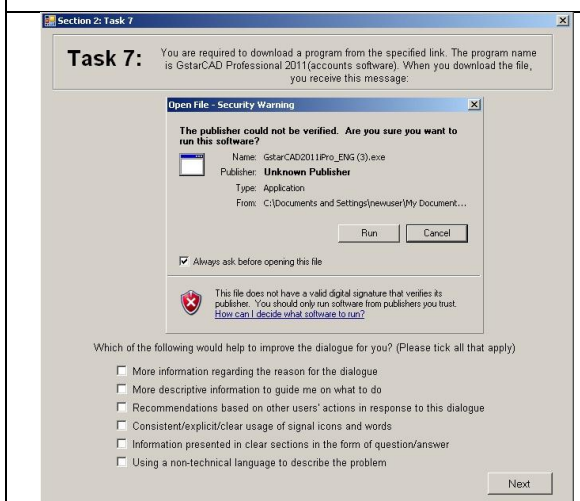
Please choose your preference(s) and click Next



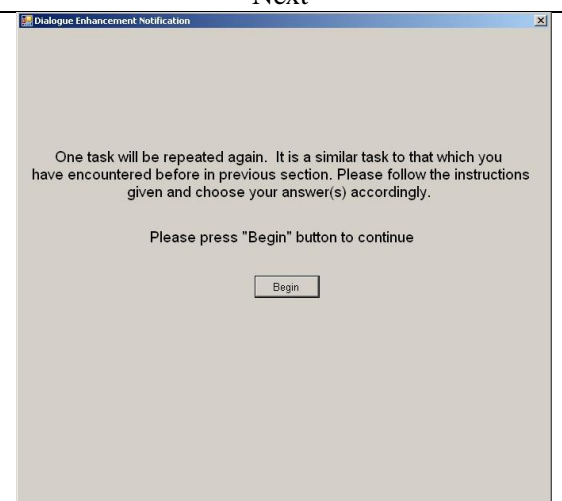
Please choose your preference(s) and click Next




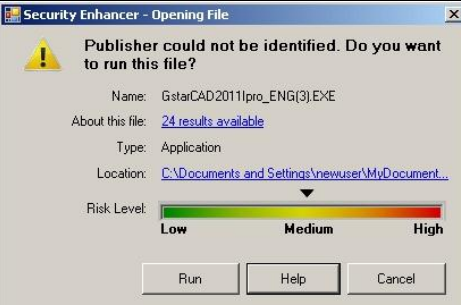
Please choose your preference(s) and click Next



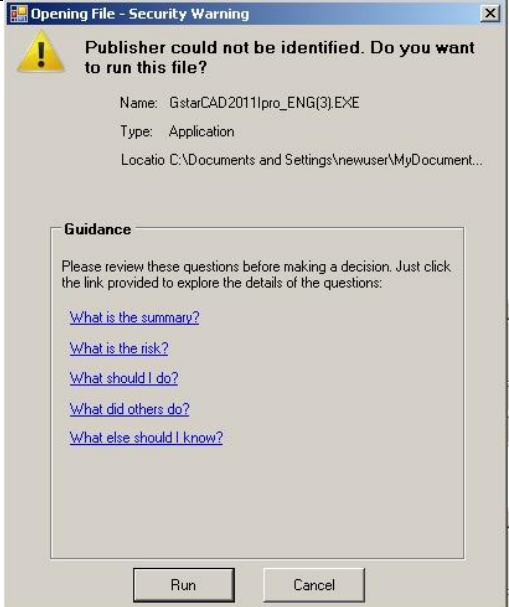
Please choose your preference(s) and click Next



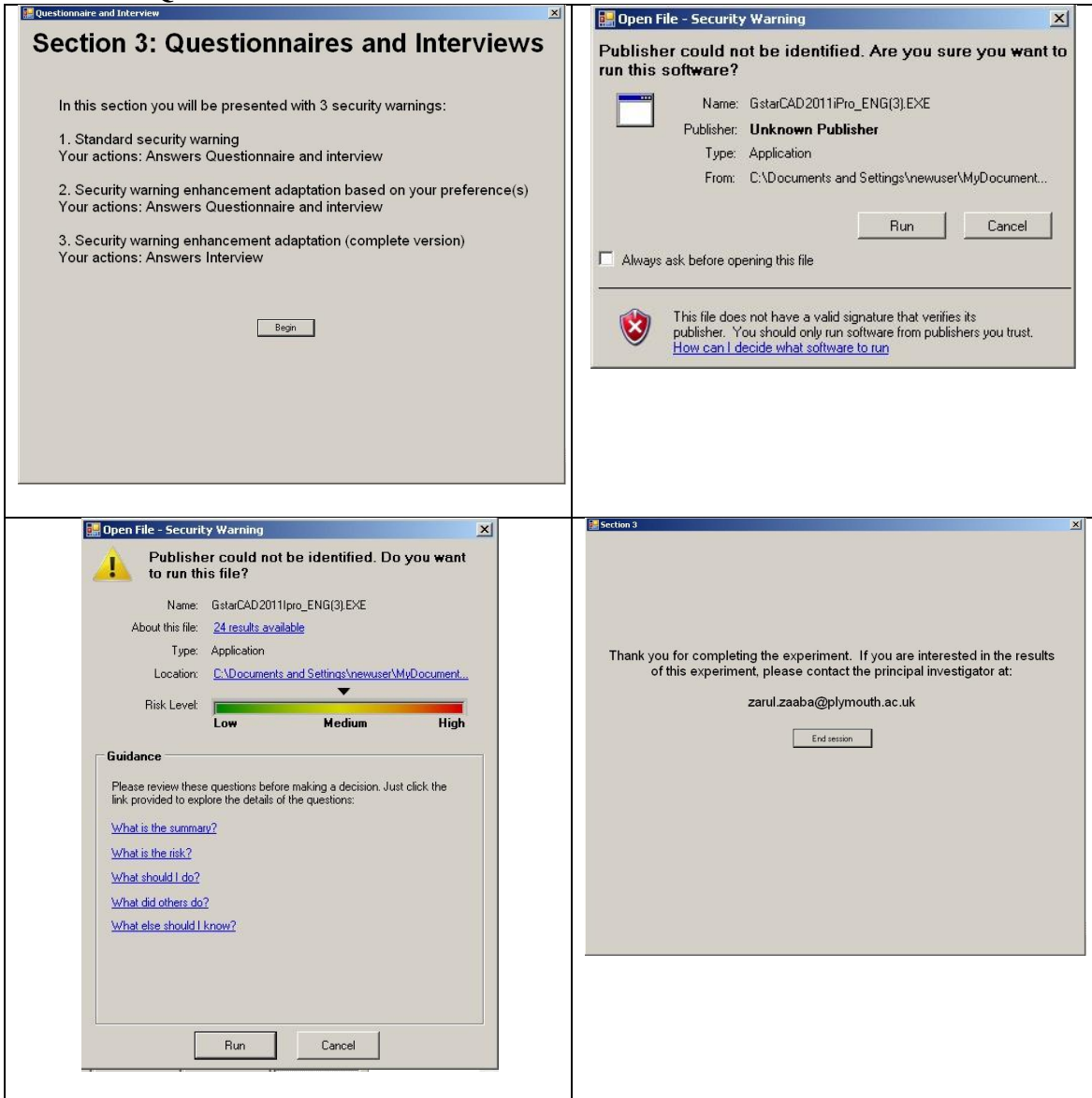
Click Begin for the next step

	 <p>You will receive this security warning. Then choose any of the actions.</p>
---	---

Read and understand the instructions then click **Next**

 <p>This is an example of an enhanced security warning based on the preferences chosen in previous sections. Shortly after this stage, the researcher will intervene and ask you to complete a questionnaire and interview</p>	
--	--

Section 3: Questionnaire and Interview



At this stage principal investigator will explain the process (i.e. questionnaire and interview questions). Questionnaire will be given as paper-based whilst interview will be recorded and the principal investigator also will write down the notes in log book. Principal investigator details:

Zarul Fitri Zaaba

Centre for Security Communications and Network Research (CSCAN)
 A304 Portland Square
 University of Plymouth
 Drake Circus
 Plymouth
 PL4 8AA
 Telephone:01752586287
 Email: zarul.zaaba@plymouth.ac.uk

Should you have any concerns about the way in which this study is being conducting please contact the secretary of the Faculty of Science and Technology Ethics Committee:-

Paula Simson

Faculty of Science and Technology

Dean's Office

Smeaton 009

University of Plymouth

Drake Circus

Plymouth

PL4 8AA

Telephone: 01752 584503

Email: paula.simson@plymouth.ac.uk

Note: Interview questions will not be revealed to participant involved.

Interview in section 2: Principal investigator will intervene when the user makes a decision with this security warning:



If the user clicks run/cancel, the principal investigator will ask these questions:

1. Why did you choose the run/cancel/help option?
2. What features helped you to understand the security warning?
3. Are you satisfied with the information provided? Why?

Then the principal investigator will explain that the user needs to click help to proceed to the next section in order for the user to view the enhanced security warning (adaptation version).

Questionnaire A – Standard security warning

1. What was the nature of the security dialogue? (Please choose only **ONE** answer)

- An error message
- Warning message
- Information message
- Questions message
- Others: Please specify

2. What type(s) of problem(s) did the security dialogue shows? (You may choose more than one answers)

- Unable to download the software due to an error
- Potentially became a victim of malware (e.g. virus, worms, Trojans etc)
- Trying to download.docx document
- Downloads from unauthorized publishers
- Does not facing any risk to proceed with the decision
- Unable to view what other people do with regards to security message
- Having difficulties to use guidance or help functions
- Facing potential problem with regards to his/her action o download software
- Others: Please specify

Instructions: Please choose only **(ONE)** answer per question.

1. The security dialogue was too complex for me to understand
2. I spent enough time to view the information provided
3. It was easy to understand the information provided
4. The way information was presented helped me to complete the tasks
5. I could effectively complete my task using the information presented
6. It was easy to find the information I needed
7. The interface of security dialogue was understandable
8. The security dialogue helped me to fix the problem in the way that I understood
9. The available help increased my knowledge and awareness about the contents and features of the dialogue.
10. This dialogue had all the functionality and capability I expected it to have

	Strongly Disagree						Strongly Agree
	1	2	3	4	5	6	7
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Questionnaire B – Enhancement security warning

1. What was the nature of the security dialogue? (Please choose only **ONE** answer)

- An error message
- Warning message
- Information message
- Questions message
- Others: Please specify

2. What type(s) of problem(s) did the security dialogue shows? (You may choose more than one answers)

- Unable to download the software due to an error
- Potentially became a victim of malware (e.g. virus, worms, Trojans etc)
- Trying to download.docx document
- Downloads from unauthorized publishers
- Does not facing any risk to proceed with the decision
- Unable to view what other people do with regards to security message
- Having difficulties to use guidance or help functions
- Facing potential problem with regards to his/her action o download software
- Others: Please specify

Instructions: Please choose only **(ONE)** answer per question.

1. The security dialogue was too complex for me to understand
2. I spent enough time to view the information provided
3. It was easy to understand the information provided
4. The way information was presented helped me to complete the tasks
5. I could effectively complete my task using the information presented
6. It was easy to find the information I needed
7. The interface of security dialogue was understandable
8. The security dialogue helped me to fix the problem in the way that I understood
9. The available help increased my knowledge and awareness about the contents and features of the dialogue.
10. This dialogue had all the functionality and capability I expected it to have

	Strongly Disagree						Strongly Agree
	1	2	3	4	5	6	7
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Interview on standard security warning

1. What do you think will happen if you click run?
2. What do you think of the feature(s) that are available to help you make a decision in this security warning?

We assess the details by asking them, please show me....

Anything else until they say no

3. Were there any aspects of the warning that you found hard to understand or interpret?

If user answers (Yes/No) investigator will probe users' understanding about signal icons, signal words, technical terminology, choices/options, help functions etc.

Do you understand the usage of signal icon/signal words in this security warning?

- Do you understand the way information was presented, especially any technical wording?
- Do you feel that that this security warning was presented with enough options to guide you?
- Do you feel satisfied with help available for this warning?

Interview on enhancement adaptation security warning

1. What do you think of the feature(s) that are available to help you make a decision in this security warning?

We assess the details by asking them, please show me....

Anything else until they say no

2. Were there any aspects of the warning that you found hard to understand or interpret?

If user answers (Yes/No) investigator will probe users' understanding about signal icons, signal words, technical terminology, choices/options, help functions etc.

- Do you understand the usage of signal icon/signal words in this security warning?
- Do you understand the way information was presented, especially any technical wording?
- Do you feel that that this security warning was presented with enough options to guide you?
- Do you feel satisfied with help available for this warning?

Interview on the last section (Comparison)

Start with Usability Question:

Effectiveness

- Which of security warnings able to provide effective solutions for you to make a decision?
- Why?

Efficiency

- Which of security warning able to guide me through to make a safe decision?
- Why?

User satisfaction

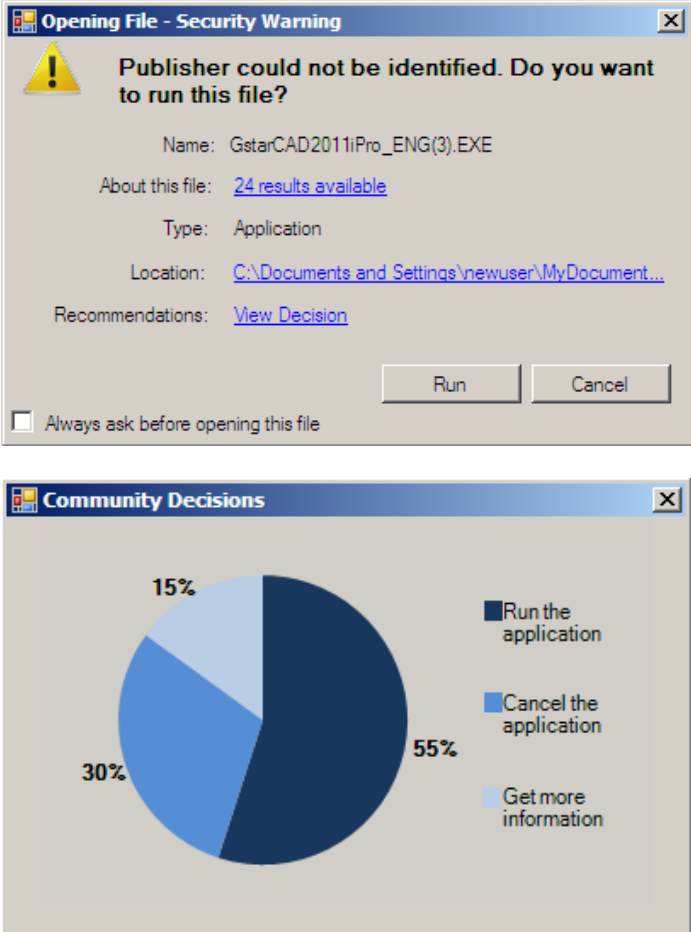
- Ease of use – Which of this would be easy for you to use? Why?
- Which of this would be your preferences? Why?

1. What other elements that you think would be needed to improve the standard security warning and enhancement security warning?
2. Comments/Suggestions

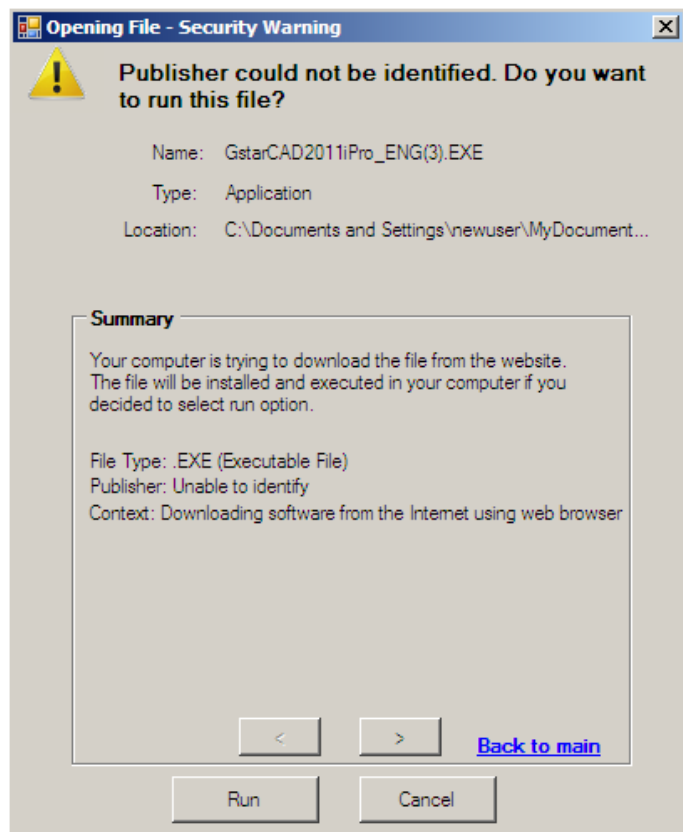
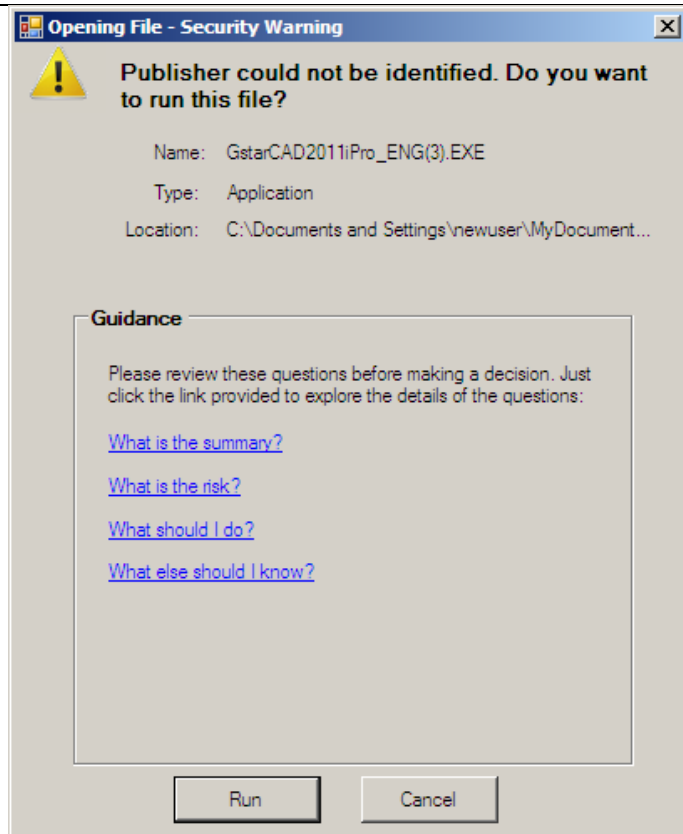
End of session

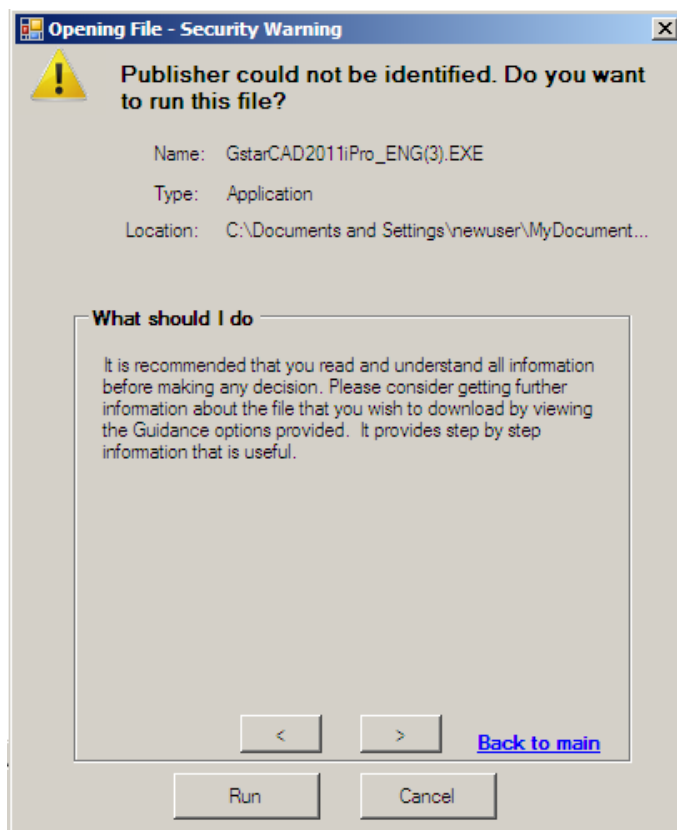
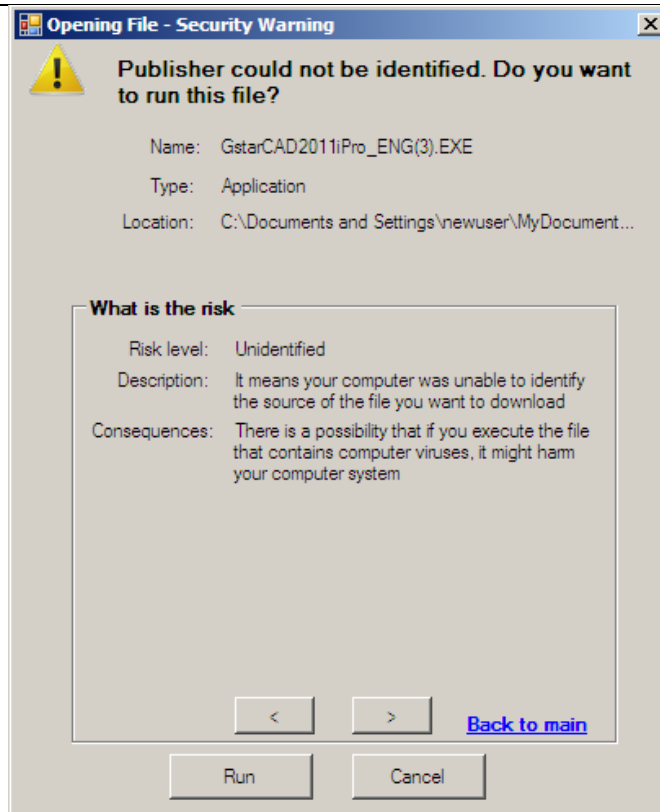
Some other examples security warnings preferences classification

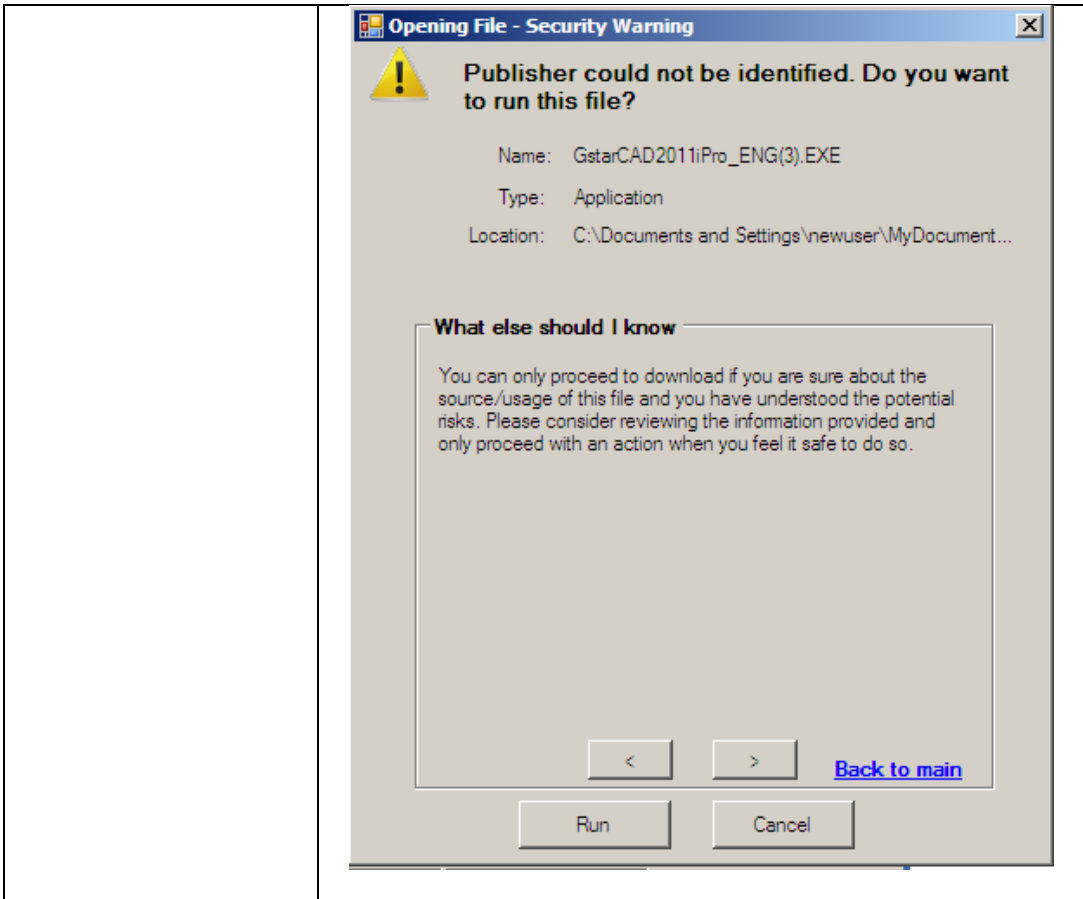
It can be noted that these were the security warning that had been generated by the ASIA mock-up software. Based on user's decision or preference in Task 7, this security warning is generated (i.e. by pressing help button in the simplified security warning) accordingly.

Combination	Security warning Image
Option 1 and 3	 <p>The image displays two screenshots of Windows security warnings. The top screenshot is a dialog box titled "Opening File - Security Warning" with a yellow warning icon. The text inside reads: "Publisher could not be identified. Do you want to run this file?". Below this, it lists file details: "Name: GstarCAD2011iPro_ENG(3).EXE", "About this file: 24 results available", "Type: Application", "Location: C:\Documents and Settings\newuser\MyDocument...", and "Recommendations: View Decision". At the bottom, there are "Run" and "Cancel" buttons, and a checkbox labeled "Always ask before opening this file".</p> <p>The bottom screenshot is a pie chart titled "Community Decisions". The chart shows three segments: a dark blue segment representing "Run the application" at 55%, a medium blue segment representing "Cancel the application" at 30%, and a light blue segment representing "Get more information" at 15%. A legend on the right side of the chart identifies these categories.</p>

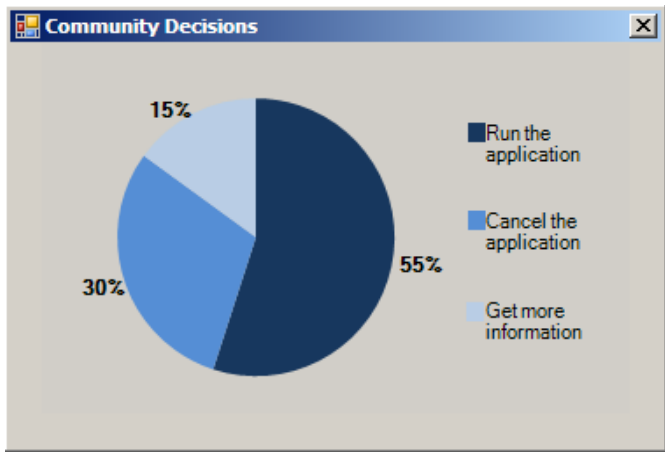
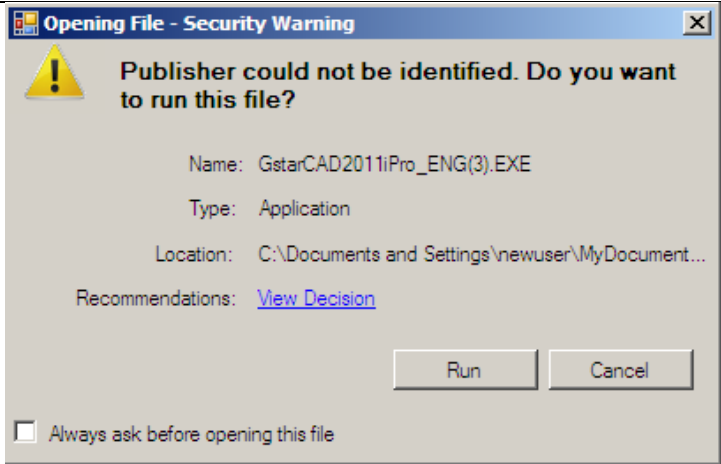
Option 5



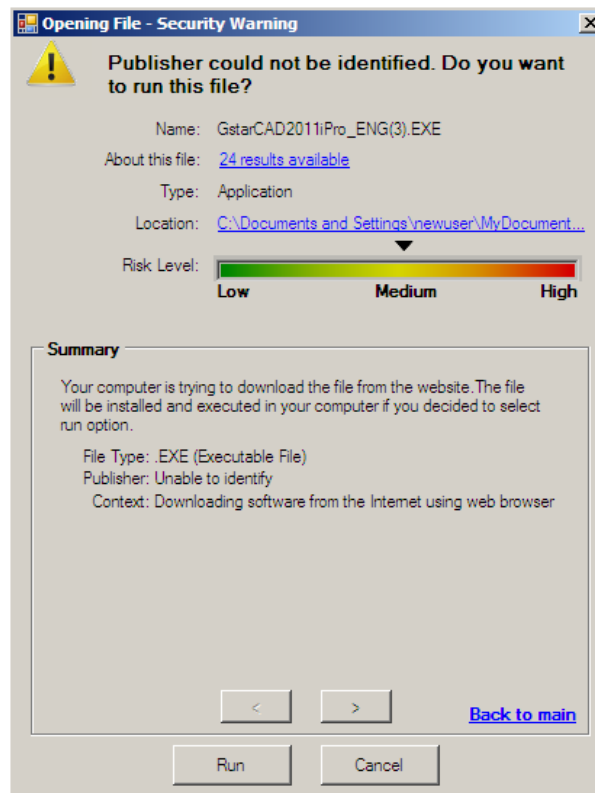
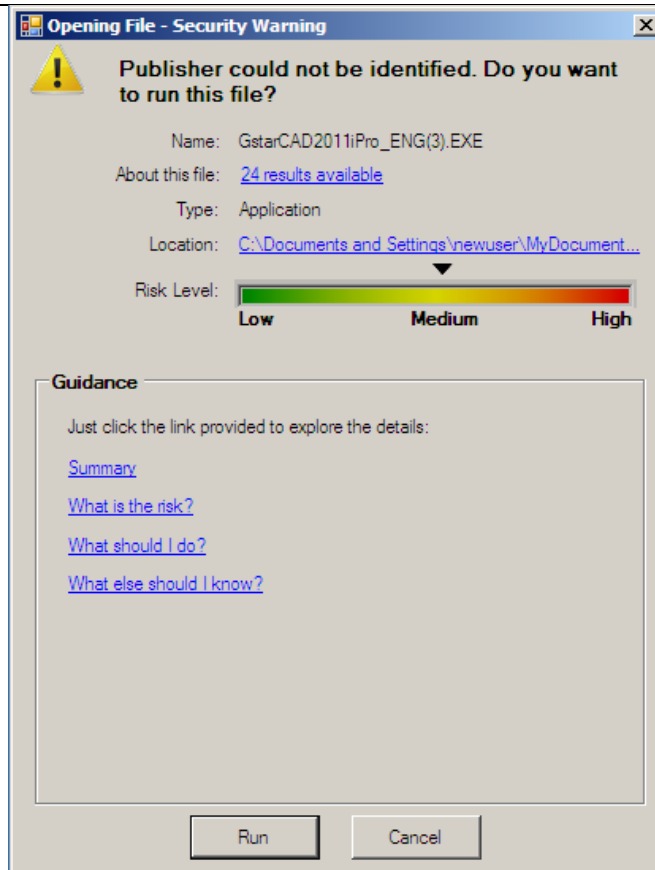


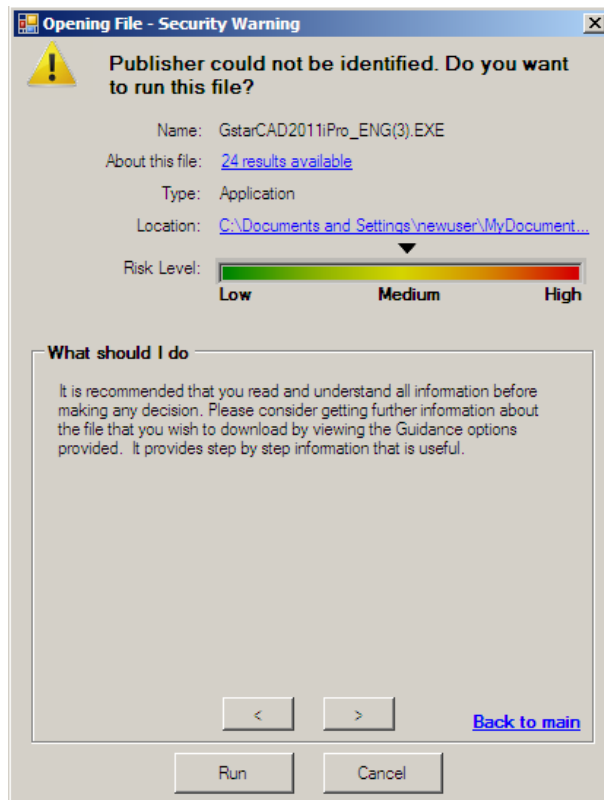
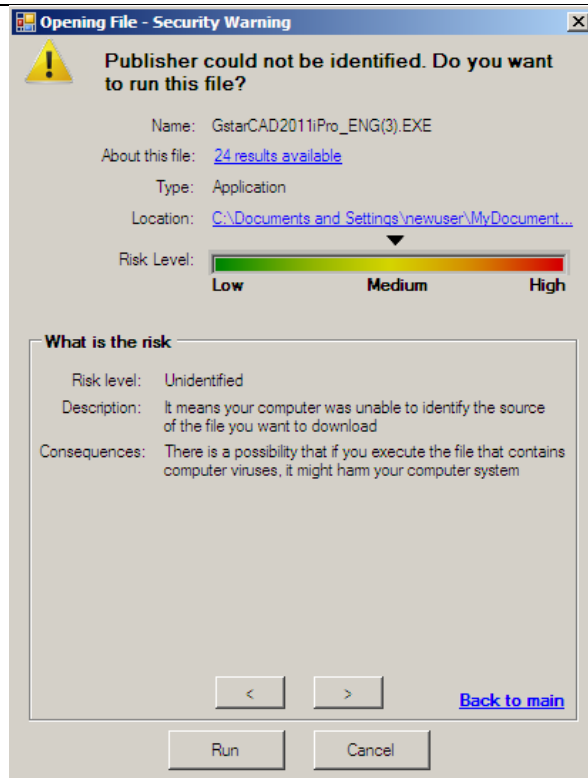


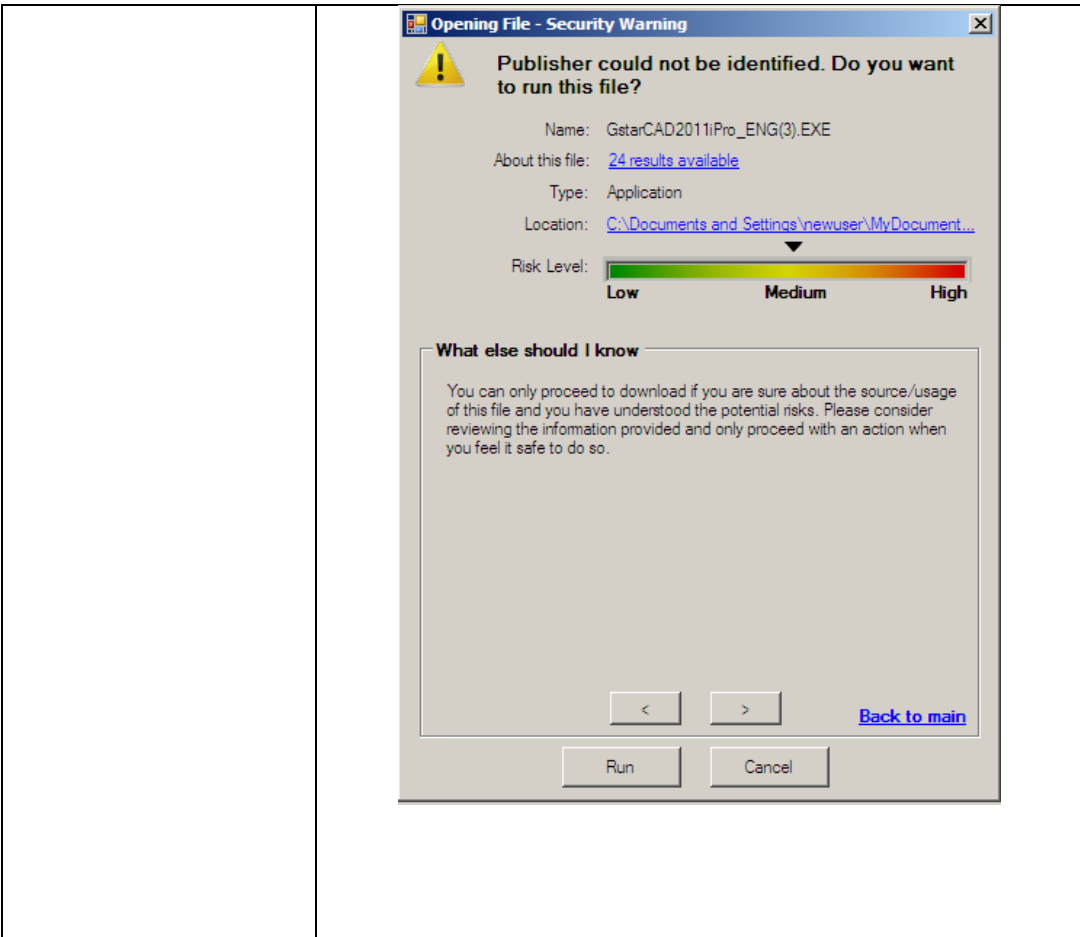
Option 3



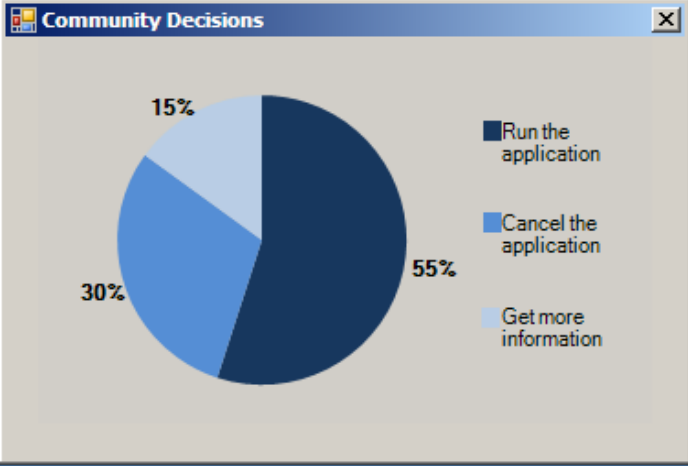
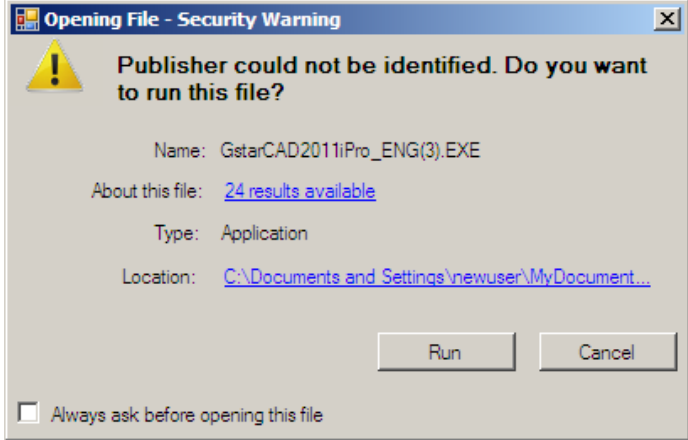
Option 1, 4 and 6







Option 1 and 6



Chi-Square Test results

Formula:

$$X^2 = \frac{(O - E)^2}{E}$$

Where **O** is the standard warning frequency (observed frequency)

E is the enhance warning frequency (expected frequency)

df is the degree of freedom (C-1)(R-1) C= total of column & R = total of row

X² is the Chi-Square

Therefore df (3-1)(2-1) = 2. Based on the df = 2 and $X^2_{.050}$ the critical value to be used is 5.991. If X^2 is equal to or greater than 5.991, \therefore null hypothesis is rejected.

The critical value is derived from **Chi-Square Distribution Table**.

Questionnaire 1	No	Yes	Neutral
Standard (O)	23	3	4
(E)	25	3	2
Enhanced (O)	27	3	0
(E)	25	3	2
Total	50	6	4
O - E (S)	-2	0	2
O - E (E)	2	0	-2
(O-E)² (S)	4	0	4
(O-E)² (E)	4	0	4
(O-E)²/E (S)	0.16	0.00	2.00
(O-E)²/E (E)	0.16	0.00	2.00
X²	4.32		

H₀ = There is no difference between standard and enhanced warnings in terms of “the security dialogue was too complex for me to understand”

$X^2 < 5.991 \therefore H_0$ is accepted

Descriptions: There is no significant difference between standard and enhanced warning that users’ encountered. This indicates that neither warnings were complicated, but the results revealed that users were pruned to the enhanced version of warning.

Questionnaire 2	No	Yes	Neutral
Standard (O)	5	23	2
(E)	5.5	21	3.5
Enhanced (O)	6	19	5
(E)	5.5	21	3.5
Total	11	42	7
O - E (S)	-0.5	2	-1.5
O - E (E)	0.5	-2	1.5
(O-E)² (S)	0.25	4	2.25
(O-E)² (E)	0.25	4	2.25
(O-E)²/E (S)	0.05	0.19	0.64
(O-E)²/E (E)	0.05	0.19	0.64
X²	1.76		

H_0 = There is no difference between standard and enhanced warning in terms of “I spent enough time to view the information provided”

$X^2 < 5.991 \therefore H_0$ is accepted

Descriptions: the enhanced version of warnings contained more information as compared to the standard warning. Surprisingly based on this result, there is no significant difference between standard and enhanced warning that users’ encountered. This indicated that users were using ample time to view warnings and the information provided.

Questionnaire 3	No	Yes	Neutral
Standard (O)	7	20	3
(E)	5	23.5	1.5
Enhanced (O)	3	27	0
(E)	5	23.5	1.5
Total	10	47	3
O - E (S)	2	-3.5	1.5
O - E (E)	-2	3.5	-1.5
(O-E)² (S)	4	12.25	2.25
(O-E)² (E)	4	12.25	2.25
(O-E)²/E (S)	0.80	0.52	1.50
(O-E)²/E (E)	0.80	0.52	1.50
X²	5.64		

H_0 = There is no difference between standard and enhanced warning in terms of “it was easy to understand the information provided”

$X^2 < 5.991 \therefore H_0$ is accepted

Descriptions: There is no significant difference between standard and enhanced warning in terms of the ease of understanding the information provided. However, the vast majority claimed that the enhanced warning is easier as compared to the standard version.

Questionnaire 4	No	Yes	Neutral
Standard (O)	11	11	8
(E)	6	19.5	4.5
Enhanced (O)	1	28	1
(E)	6	19.5	4.5
Total	12	39	9
O - E (S)	5	-8.5	3.5
O - E (E)	-5	8.5	-3.5
(O-E)² (S)	25	72.25	12.25
(O-E)² (E)	25	72.25	12.25
(O-E)²/E (S)	4.17	3.71	2.72
(O-E)²/E (E)	4.17	3.71	2.72
X²	21.19		

H_0 = There is no difference between standard and enhanced warning in terms of “the way information was presented help me to complete the tasks”

$X^2 > 5.991 \therefore H_0$ is rejected

Descriptions: There is a significant difference between standard and enhanced warning in terms of the way information was presented to complete the task. The vast majority of respondents agreed with the enhanced version, comparing it to the standard warning. It can be noted only 1 user specified that the enhanced warning was not helping the user to complete the task.

Questionnaire 5	No	Yes	Neutral
Standard (O)	9	12	9
(E)	5.5	20	4.5
Enhanced (O)	2	28	0
(E)	5.5	20	4.5
Total	11	40	9
O - E (S)	3.5	-8	4.5
O - E (E)	-3.5	8	-4.5
(O-E)² (S)	12.25	64	20.25
(O-E)² (E)	12.25	64	20.25
(O-E)²/E (S)	2.23	3.20	4.50
(O-E)²/E (E)	2.23	3.20	4.50
X²	19.85		

H_0 = There is no difference between standard and enhanced warning in terms of “I could effectively complete my task using the information provided”

$X^2 > 5.991 \therefore H_0$ is rejected

Descriptions: There is significant difference between standard and enhanced warning in terms of effectively able to complete the task using the information provided. the vast

majority of respondents claimed the effectiveness with the enhanced warning rather than the standard version.

Questionnaire 6	No	Yes	Neutral
Standard (O)	17	8	5
(E)	9.5	17.5	3
Enhanced (O)	2	27	1
(E)	9.5	17.5	3
Total	19	35	6
O - E (S)	7.5	-9.5	2
O - E (E)	-7.5	9.5	-2
(O-E)² (S)	56.25	90.25	4
(O-E)² (E)	56.25	90.25	4
(O-E)²/E (S)	5.92	5.16	1.33
(O-E)²/E (E)	5.92	5.16	1.33
X²	24.82		

H₀ = There is no difference between standard and enhanced warning in terms of “it was easy to find information I needed”

$X^2 > 5.991 \therefore H_0$ is rejected

Descriptions: There is a highly significant difference between standard and enhanced warning in terms of it was easy to find information that users needed. As the vast majority claimed the easiness in enhanced warning, it is likely 57% of respondents mentioned the difficulties with the standard warning.

Questionnaire 7	No	Yes	Neutral
Standard (O)	10	16	4
(E)	6.5	20.5	3
Enhanced (O)	3	25	2
(E)	6.5	20.5	3
Total	13	41	6
O - E (S)	3.5	-4.5	1
O - E (E)	-3.5	4.5	-1
(O-E)² (S)	12.25	20.25	1
(O-E)² (E)	12.25	20.25	1
(O-E)²/E (S)	1.88	0.99	0.33
(O-E)²/E (E)	1.88	0.99	0.33
X²	6.41		

H₀ = There is no difference between standard and enhanced warning in terms of “the interface of security dialogue was understandable”

$X^2 > 5.991 \therefore H_0$ is rejected

Descriptions: There is a significant difference between standard and enhanced warning in terms of the interface of security dialogue being understandable. (25/30) claimed this was the case with the enhanced warning, whilst only 16 with the standard warning.

Questionnaire 8	No	Yes	Neutral
Standard (O)	14	11	5
(E)	8	17.5	4.5
Enhanced (O)	2	24	4
(E)	8	17.5	4.5
Total	16	35	9
O - E (S)	6	-6.5	0.5
O - E (E)	-6	6.5	-0.5
(O-E) ² (S)	36	42.25	0.25
(O-E) ² (E)	36	42.25	0.25
(O-E) ² /E (S)	4.50	2.41	0.06
(O-E) ² /E (E)	4.50	2.41	0.06
X ²	13.94		

H₀ = There is no difference between standard and enhanced warning in terms of “the security dialogue helped me to fix the problem in the way that I understood”

X² > 5.991 ∴ H₀ is rejected

Descriptions: There is a highly significant difference between standard and enhanced warning in terms of the security dialogue helped users to fix the problem in which users can understand as the majority claimed it with enhanced warning. On the other hand 14/30 claimed difficulties with standard warning, and only 2/30 with enhanced warning.

Questionnaire 9	No	Yes	Neutral
Standard (O)	15	11	4
(E)	8.5	19	2.5
Enhanced (O)	2	27	1
(E)	8.5	19	2.5
Total	17	38	5
O - E (S)	6.5	-8	1.5
O - E (E)	-6.5	8	-1.5
(O-E) ² (S)	42.25	64	2.25
(O-E) ² (E)	42.25	64	2.25
(O-E) ² /E (S)	4.97	3.37	0.90
(O-E) ² /E (E)	4.97	3.37	0.90
X ²	18.48		

H₀ = There is no difference between standard and enhanced warnings in terms of “the available help increased my knowledge and awareness about the contents and features of the dialogues”

X² > 5.991 ∴ H₀ is rejected

Descriptions: There is a highly significant difference between standard and enhanced warning in terms of the available help increased users' knowledge and awareness about the contents and features of the dialogues. Therefore it can be suggested that security warning enhancement provided better contents and features as compared to the standard warning.

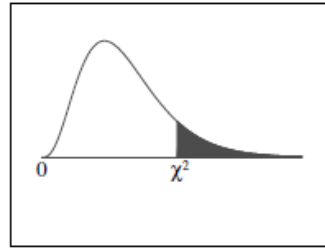
Questionnaire 10	No	Yes	Neutral
Standard (O)	12	10	8
(E)	7.5	16	6.5
Enhanced (O)	3	22	5
(E)	7.5	16	6.5
Total	15	32	13
O - E (S)	4.5	-6	1.5
O - E (E)	-4.5	6	-1.5
(O-E)² (S)	20.25	36	2.25
(O-E)² (E)	20.25	36	2.25
(O-E)²/E (S)	2.70	2.25	0.35
(O-E)²/E (E)	2.70	2.25	0.35
X²	10.59		

H_0 = There is no difference between standard and enhanced warning in terms of “this dialogue had all the functionality and capability I expected it to have”

$X^2 > 5.991 \therefore H_0$ is rejected

Description: There is a significant difference between both warning in terms of the dialogue had all functionality and capability that users expected to have. This suggested that security warning enhancement were better in the sense of the overall functionality and features to help users, as compared to standard version.

Chi-Square Distribution Table



The shaded area is equal to α for $\chi^2 = \chi_{\alpha}^2$.

<i>df</i>	$\chi_{.995}^2$	$\chi_{.990}^2$	$\chi_{.975}^2$	$\chi_{.950}^2$	$\chi_{.900}^2$	$\chi_{.100}^2$	$\chi_{.050}^2$	$\chi_{.025}^2$	$\chi_{.010}^2$	$\chi_{.005}^2$
1	0.000	0.000	0.001	0.004	0.016	2.706	3.841	5.024	6.635	7.879
2	0.010	0.020	0.051	0.103	0.211	4.605	5.991	7.378	9.210	10.597
3	0.072	0.115	0.216	0.352	0.584	6.251	7.815	9.348	11.345	12.838
4	0.207	0.297	0.484	0.711	1.064	7.779	9.488	11.143	13.277	14.860
5	0.412	0.554	0.831	1.145	1.610	9.236	11.070	12.833	15.086	16.750
6	0.676	0.872	1.237	1.635	2.204	10.645	12.592	14.449	16.812	18.548
7	0.989	1.239	1.690	2.167	2.833	12.017	14.067	16.013	18.475	20.278
8	1.344	1.646	2.180	2.733	3.490	13.362	15.507	17.535	20.090	21.955
9	1.735	2.088	2.700	3.325	4.168	14.684	16.919	19.023	21.666	23.589
10	2.156	2.558	3.247	3.940	4.865	15.987	18.307	20.483	23.209	25.188
11	2.603	3.053	3.816	4.575	5.578	17.275	19.675	21.920	24.725	26.757
12	3.074	3.571	4.404	5.226	6.304	18.549	21.026	23.337	26.217	28.300
13	3.565	4.107	5.009	5.892	7.042	19.812	22.362	24.736	27.688	29.819
14	4.075	4.660	5.629	6.571	7.790	21.064	23.685	26.119	29.141	31.319
15	4.601	5.229	6.262	7.261	8.547	22.307	24.996	27.488	30.578	32.801
16	5.142	5.812	6.908	7.962	9.312	23.542	26.296	28.845	32.000	34.267
17	5.697	6.408	7.564	8.672	10.085	24.769	27.587	30.191	33.409	35.718
18	6.265	7.015	8.231	9.390	10.865	25.989	28.869	31.526	34.805	37.156
19	6.844	7.633	8.907	10.117	11.651	27.204	30.144	32.852	36.191	38.582
20	7.434	8.260	9.591	10.851	12.443	28.412	31.410	34.170	37.566	39.997
21	8.034	8.897	10.283	11.591	13.240	29.615	32.671	35.479	38.932	41.401
22	8.643	9.542	10.982	12.338	14.041	30.813	33.924	36.781	40.289	42.796
23	9.260	10.196	11.689	13.091	14.848	32.007	35.172	38.076	41.638	44.181
24	9.886	10.856	12.401	13.848	15.659	33.196	36.415	39.364	42.980	45.559
25	10.520	11.524	13.120	14.611	16.473	34.382	37.652	40.646	44.314	46.928
26	11.160	12.198	13.844	15.379	17.292	35.563	38.885	41.923	45.642	48.290
27	11.808	12.879	14.573	16.151	18.114	36.741	40.113	43.195	46.963	49.645
28	12.461	13.565	15.308	16.928	18.939	37.916	41.337	44.461	48.278	50.993
29	13.121	14.256	16.047	17.708	19.768	39.087	42.557	45.722	49.588	52.336
30	13.787	14.953	16.791	18.493	20.599	40.256	43.773	46.979	50.892	53.672
40	20.707	22.164	24.433	26.509	29.051	51.805	55.758	59.342	63.691	66.766
50	27.991	29.707	32.357	34.764	37.689	63.167	67.505	71.420	76.154	79.490
60	35.534	37.485	40.482	43.188	46.459	74.397	79.082	83.298	88.379	91.952
70	43.275	45.442	48.758	51.739	55.329	85.527	90.531	95.023	100.425	104.215
80	51.172	53.540	57.153	60.391	64.278	96.578	101.879	106.629	112.329	116.321
90	59.196	61.754	65.647	69.126	73.291	107.565	113.145	118.136	124.116	128.299
100	67.328	70.065	74.222	77.929	82.358	118.498	124.342	129.561	135.807	140.169

	Adaptive Security Dialogues (ASD)	Automated Security Interface Adaptation (ASIA)
Goal	Introduced an architecture that matches the complexity and the intrusiveness of security dialogues to the associated risks with the decisions that end-users are made to improve security behaviour of computer users.	Introduced an architecture to improve security warning dialogues based on end-users preferences by utilising the information provided (interactively generate security warning enhancement) where it presented the information that end-users need on the first place. Then the user will receive their security warning with the information that they wish to have.
Means of data collection	Implementing role played web based e-mail client that simulates ASD based on five types of warning messages (i.e. text file, Ms Excel file, Ms Power Point file, PDF file and Ms Word file). Then participants are required to answer the questionnaire (i.e. usability, understanding and the interference with the tasks).	Implementing role played ASIA simulation software where it utilised users experienced dealing with various types of security warning dialogues. Then participants will be interviewed about their experience whilst using the software (recorded interviews) and finally they will be asked to complete a questionnaire in relation to the usability aspects and their preference on warning dialogue.
Participants involved	32 participants (i.e. 8 participants were excluded). Students in computer science and engineering were excluded as the focus was given to the general users.	50 participants (i.e. predominantly students and staff in the university) as long as they were eighteen years old or older. They received £5.50 token for the completion of the study.
How it works	Participants experienced five contexts the dialogue box (i.e. warn & continue (W & C), multiple choice, security training, blank filling and clarification) via three different versions of e-mail application (W & C dialogues, ASD and ASDF) where it matches the complexity of warnings with the risk based on the decision that users have to make. Then followed by the questionnaire session.	Participants experienced seven different tasks of warning dialogue where they are required to make a selection of the list of choices/information that should be provided in the warning dialogue. Then later, from the last task, the new security warning enhancement will be generated based on the selection that participant had chosen in the first place. The new security warning enhancement utilise the additional features and more useful functions (i.e. hover with the quick information, risk level bar, guidance information and matching the signal cues with the current context of warnings which has not been highlighted before). Then followed by interview and questionnaire session.
Limitations	<ol style="list-style-type: none"> 1. It was fixed into five types of warning messages rather than covers all types of warning dialogues. 2. The sample size was too small and not representative 3. It was difficult to conduct a long-term experiment that fully resembled the real scenarios pertaining to security warnings 4. The usability assessment was conducted in a simple manner where it only asked about the overall usability rather than specifically asked about three main elements of usability (effectiveness, efficiency and satisfaction) 	<ol style="list-style-type: none"> 1. The study had been conducted as a mock-up rather than real-time system 2. Sample size mostly was derived from the university's environment (i.e. students and staffs) 3. The usability assessment was more generic rather than a comprehensive assessment of each usability elements. 4. As the interview session was recorded by the principal investigator, element of bias would be existed as the majority of participants might tend to say only good things rather than providing an honest answer.

Appendix E

List of Publications

End-User Perception and Usability of Information Security

Z.F.Zaaba^{1,2}, S.M.Furnell^{1,3} and P.S.Dowland¹

¹Centre for Security, Communications and Network Research,
University of Plymouth, Plymouth, United Kingdom

²School of Computer Sciences, University Sains Malaysia, Penang, Malaysia

³School of Computer and Security Science, Edith Cowan University
Perth, Western Australia
e-mail: info@cscan.org

Abstract

This paper investigates users' understanding of security features and application and examines perceptions relating to usability. The study made use of an online survey consisting of five sections and recruited a total of 564 participants. Respondents were presented with a range of questions designed to measure their experience and knowledge of security. In addition, 2 scenarios were presented to respondents which examined their understanding of security warnings and potential threats, including email phishing and a potentially fraudulent attack through downloading an application. The survey results revealed that end-users are still experiencing significant difficulties with understanding and reacting to current state-of-the-art security applications, messages and potential threats. Furthermore, evidence suggests there is a corresponding need for a novel approach to improve perception and usability of information security.

Keywords

Usability, Security, Interface, Perceptions, Warning, Messages, Human Computer Interaction

1. Introduction

Security features enable users to mitigate security risks by providing protection from potential threats. However, the complex and sophisticated user interfaces hinder an end users' operation of such applications, which can potentially increase the likeliness of incorrect configuration and consequential exploitation. Whitten and Tygar's (1999) assessment of Pretty Good Privacy (PGP) 5.0 was one of the earliest studies on usability issues in the context of security. Proctor et al., (2000) found usability problems existed in third party authentication methods and Wool (2004), determined usability problems in configuring firewalls to selectively filter traffic. These usability problems indicated an essential link between usability and human factors. A lack of usability can cause users to inadvertently change a secure system into an insecure system. Users should be aware of the functionality and be provided with enough information to make informed decisions. In order to investigate the problem in practice, this paper presents findings from a survey assessing users' understanding of security dialogues within web browsers (i.e. a common end-user application in which security risks can often be found). The discussion begins with an overview of perception and usability issues, before proceeding to outline the research methodology and the associated findings. The study focused upon users' responses to two common security scenarios that can occur during web browsing (namely attempting to visit a potentially fraudulent website and an attempt to download a potentially harmful file). The discussion examines the extent to which the users were supported in understanding and responding to these warnings, and highlights some resulting recommendations for future systems.

2. Overview of perception and usability

According to Nielsen (2003), usability can be referred to as a quality attribute which evaluates how a user interface is being used. It was stated that usability needs to be defined by five quality components, namely: learnability, efficiency, memorability, errors and satisfaction. Usability was also defined by the ISO (1998):

“...the extent to which a product can be used by specified users to achieve specified goals with effectiveness, efficiency and satisfaction in a specified context of use”.

The interaction between usability and security is essential. The concept of using *design principles* was introduced to improve the security of computer system (Saltzer & Schroeder, 1975). This introduced eight examples of design principles that applied to protection mechanisms. One essential finding was the term *psychological acceptability* which stated that a human interface was designed for ease of use and users should be able to apply the protection mechanism correctly. Consideration of usability can help developers make better decisions and potentially help them to work more effectively (Radle & Young, 2001). Nielsen (2003) identified that usability became a requirement for websites, e-commerce transactions and even the Internet. Schultz (2007) demonstrated that there were significant problems in relation to usability in information security by examining research papers presenting results on the relationship between security and usability. He summarised that there were usability problems in security-related tasks with some rated “severe”. Mannan & Van Oorschot (2008) analyzed the gap between usability and security in online banking and found that many security requirements were too difficult for general users to follow and were often misled by the marketing related messages on safety and security. Venter et al., (2007) evaluated the usability and security of personal firewalls and concluded that current personal firewalls were generally weak at informing the users and creating security awareness. It was also suggested that the software obstructed the creation of fine-grained rules which is a notable obstacle to usability and security of personal firewalls. Furnell et al., (2007) assessed security perceptions of personal Internet users and found that users’ knowledge and understanding are still lacking. Although the problems mostly refer to novice users, they were also applicable to those considering themselves as advanced users. Albrechtsen (2007) conducted a qualitative study on users’ view on information security. His findings showed that there is a gap between users’ intention and the actual users’ behavior as users did not perform many individual security actions. Having said that, there is clearly a need to pay much more attention to human factors in information security tasks, this paper presents an initial study which was aimed to get a better understanding of user’s perception and usability of security features and applications. It is clearly futile to build an effective user interface if the user still ignores warnings or does not understand how to use the system correctly (in a secure manner). User feedback can help developers to create better, more understandable and more usable systems. However, according to Coffee (2006), many software developers lack the interest or technical skill to develop secure systems. They consider security as part of the non-functional requirements – i.e. security is not fully integrated into the development lifecycle process (Mouratidis et al., 2005). Security should be considered during the whole development process, if it is ignored or only emphasised after the implementation stage, conflicts will rise and it could lead to future problems. It is essential that developers are now slowly beginning to realise that information security is essential even if their primary function is not related to security (Tondel *et al.*, 2008).

3. Methodology

In order to determine users' perception and usability issues in information security, an online survey was conducted to investigate preliminary insights from users regarding their level of understanding of particular issues in relation to the security of their computer system. The survey was conducted online between February-March 2010, and promoted to the end user community via e-mail, snowball sampling and news entry information on the university's internal staff/student websites. This survey consisted of 41 questions offering both open and closed responses. Respondents were not obliged to answer all questions as some of the questions were conditional. Overall, 784 responses were submitted to the website however, only 564 responses were fully completed which represented a 72% completion rate. All of the figures and percentages reported were based upon the results of a simple statistical analysis on the proportions of completed responses in this study.

4. Results and discussion

From the 564 responses, there was an almost equal gender balance with 49% male responses and 51% female. Most of the respondents were aged between 18-30 years, with at least degree level education and been using computers for more than 5 years. This showed that the vast majority of respondents had considerable familiarity with computing technology. Respondents were primarily staff/students from the authors' university together with individuals from the public/private sector. Most respondents rated themselves as intermediate/advanced users and indicated that they were concerned with regards to issues relating to computer security. In terms of security software usage, 86% were using some form of protection at home or work leaving 14% who did not use it (or were unsure). Before proceeding with further investigation, the survey asked respondents to describe the types of problem that they regularly encounter whilst using their computer. Incidents of malware, problems with Internet connection, problems in understanding help functions, complex security features and user interface difficulties were the main concerns. 70% of respondents indicated that they were at concerned regarding issues of security in their computer with only 5% indicating they were not concerned at all. This finding provided an interesting baseline to assess the real situation of how end users' perceived the security features of information system. Indeed, the following responses from surveyed respondents highlight the issues:

"I do not have to use any security software because I am using Mac. I believe there is no virus at all so I don't have to use any of those"

"I am using Linux. It is free from any malware attack. I don't have to spend money to get antivirus software"

"I do not care whether I have the antivirus or not as I believe it's not my responsibility. It's my company's asset anyway"

End users' behaviour might lead them to a significant problem if they become a victim of a malware attack. In the next sub-sections two scenarios are presented considering how users understand the usability of security features and how this can lead them to make a security-relevant decision. Scenario 1 focuses on security warnings relating to possible phishing sites, while Scenario 2 looks at warnings that are issued when downloading executable files. These scenarios are used to assess a user's ability to

understand security features, usability and issues of security in their daily routine whilst using computer.

4.1 Scenario 1

In order to gauge the level of understanding of the usability of security features in a web browsing context, respondents were asked to indicate their preferred web browser. As each browser has different methods of presenting security warnings, respondents were then shown a screenshot based on their chosen browser. In this scenario, respondents were asked to imagine they had received an email from their bank and were asked to re-activate their online banking account by clicking the hyperlink within the email. Respondents were then asked what they would do next. The six images are depicted in Figure 1.

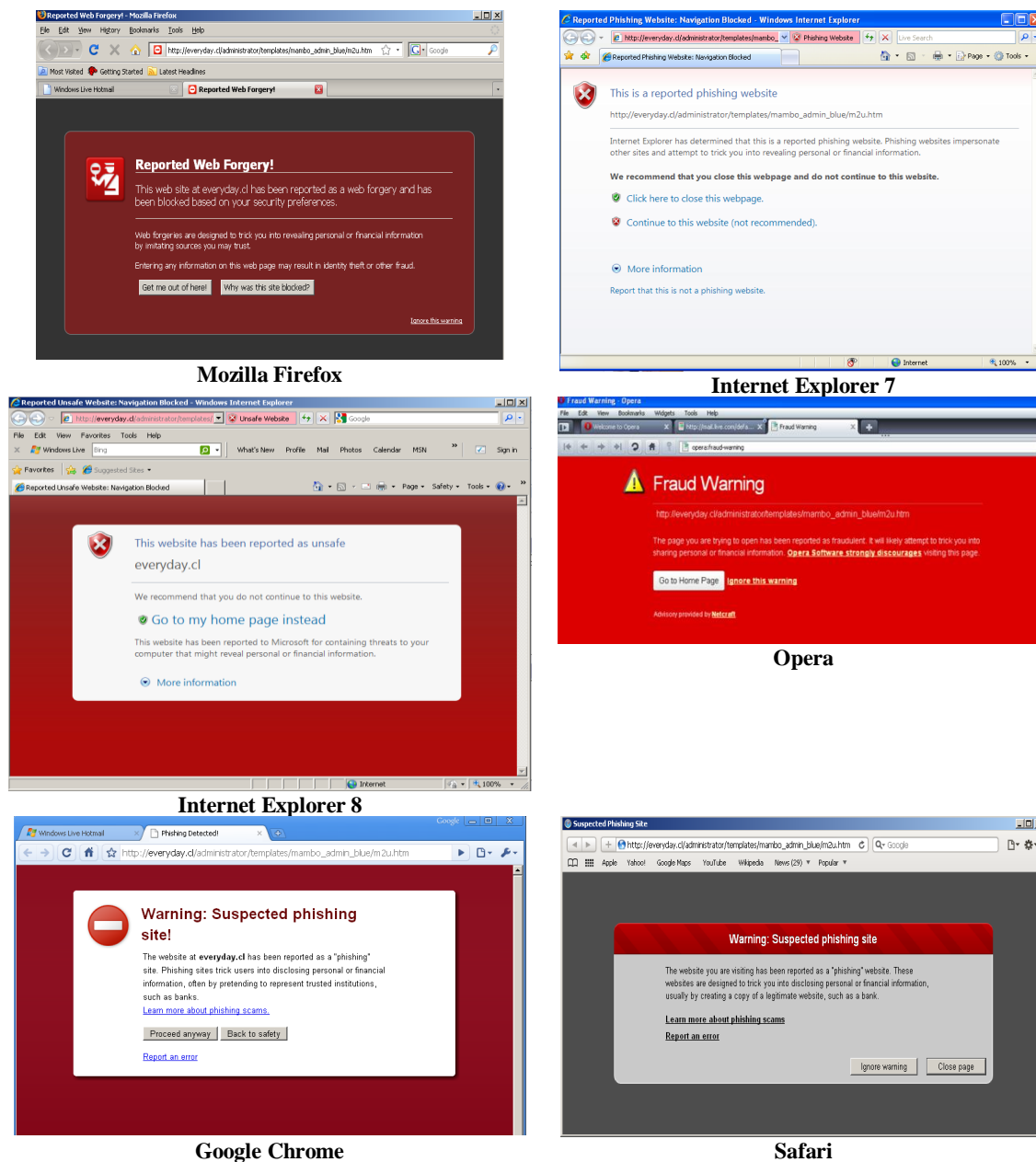


Figure 1: Screenshots from various web browsers showing a security warning having detected a possible phishing website

The *best practice* actions were chosen by the majority of users as depicted in Figure 2, although a small proportion of respondents indicated that they would have ignored the warning and proceeded with the transaction. Had this been a genuine email/website, it is likely that they would have become a victim of a phishing site that could result in their personal or financial information being passed to an unknown party. Although 13.3% indicated they would attempt to get more information about the meaning of the message, if they did not understand the information needed, it would also be possible for them to become victims. This survey revealed that there were clear distinctions in the way that security warnings were presented by each browser (see Table 1). This study focussed on 5 elements, namely: usage of help function, colours, icons, choices and terminology. Based on these features, this study revealed that there were no specific standards to present security warnings, messages or notifications. Each vendor had their own style or preference to present such warnings. Currently, Microsoft (2011), had more specific guidelines for users that covered issues on controls, command, text, messages, interaction, windows and visual. This documentation will guide them to create a standard and more meaningful outcome in relation of usability.

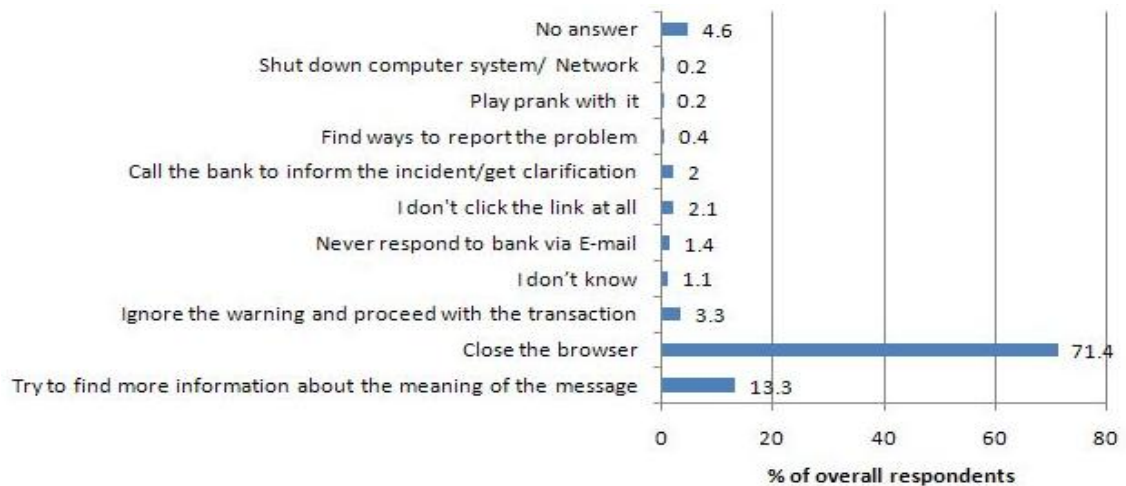


Figure 2: Users' preferred action when presented with the phishing security warning (Scenario 1)

After assessing the users' response towards the phishing warning, the next question attempted to assess users' general understanding of the security warning presented. 75% responses understood the warning with the remainder unsure how to interpret the information presented. From this group, 13% chose try to find more information about the meaning of the message. Of most concern were a small percentage of respondents with 1% claiming to understand the depicted screenshot but still ignored the warning and proceeded with the transaction. From the respondents who did not understand the phishing warnings, there were 3 main issues identified; technical terminology (62%), nature of the event being described (55%) and choices available (25%). No attempt was made to further question the elements that they did not understand as the question was only presented in a general context.

Browsers	Usage of Help Function	Usage of Colours	Usage of Icon	Available choices	Terminology used
Mozilla Firefox	<ul style="list-style-type: none"> • Providing information on why the website is blocked 	<ul style="list-style-type: none"> • Using a red background colour scheme to get attention 	<ul style="list-style-type: none"> • Using 2 types of warning icon 	<ul style="list-style-type: none"> • Ignore this warning • Get me out of here • Why was this site blocked 	<ul style="list-style-type: none"> • Reported as web forgery
Internet Explorer 7	<ul style="list-style-type: none"> • Providing more information about the incident 	<ul style="list-style-type: none"> • Address bar changing to red colour with Phishing website connotation 	<ul style="list-style-type: none"> • Error warning icon 	<ul style="list-style-type: none"> • Continue to website(not recommended) • Close the webpage • More information about phishing • Report that it is not phishing website 	<ul style="list-style-type: none"> • Reported as phishing website
Internet Explorer 8	<ul style="list-style-type: none"> • Providing more information about the incident 	<ul style="list-style-type: none"> • Address bar changing to red colour with Unsafe website connotation 	<ul style="list-style-type: none"> • Error warning icon 	<ul style="list-style-type: none"> • Go to my homepage instead • More information about phishing • Report this site does not contains threats • Disregard and continue (not recommended) 	<ul style="list-style-type: none"> • Reported as unsafe website
Google Chrome	<ul style="list-style-type: none"> • Providing more information about phishing scams 	<ul style="list-style-type: none"> • Using a red background colour scheme to get attention 	<ul style="list-style-type: none"> • No entry warning icon 	<ul style="list-style-type: none"> • Proceed anyway • Back to safety • Report an error • Learn more about phishing scams 	<ul style="list-style-type: none"> • Suspected as phishing site
Safari	<ul style="list-style-type: none"> • Providing more information about phishing scams 	<ul style="list-style-type: none"> • Using a red highlighted header colour 	<ul style="list-style-type: none"> • No icon 	<ul style="list-style-type: none"> • Learn more about phishing scams • Report an error • Ignore warning • Close page 	<ul style="list-style-type: none"> • Suspected as phishing site
Opera	<ul style="list-style-type: none"> • No details 	<ul style="list-style-type: none"> • Using a fully red background colour scheme 	<ul style="list-style-type: none"> • Warning icon 	<ul style="list-style-type: none"> • Go to homepage • Ignore this warning 	<ul style="list-style-type: none"> • Fraud warning

Table 1: Comparison of the security warnings from various web browsers

4.2 Scenario 2

Using the respondent's preferred browser, a second scenario was presented in which the user was presented with a security warning following a click on a link to install software (Figure 3). Most respondents indicated they would save the file and then scan for viruses (35%). Surprisingly, 29% of respondents who used Internet Explorer 7 decided to cancel or quit from the process. This could be caused by the rather specific warning within the dialogue (indicating that the files could possibly contain malware), although Internet Explorer 8 used an identical prompt. It is also notable that almost 10% of respondents would run the application straightaway without virus scanning it first (although it is possible that these users were under the impression that their anti-virus product would automatically scan the file before execution). It has to be remembered that this may not accurately represent users' real intentions as this scenario was effectively simulated. However, this demonstrated that users may be at risk by running applications directly from the source without scanning it. One interesting finding from this survey was that a small percentage of users would not download the software if they used their own laptop or computer.

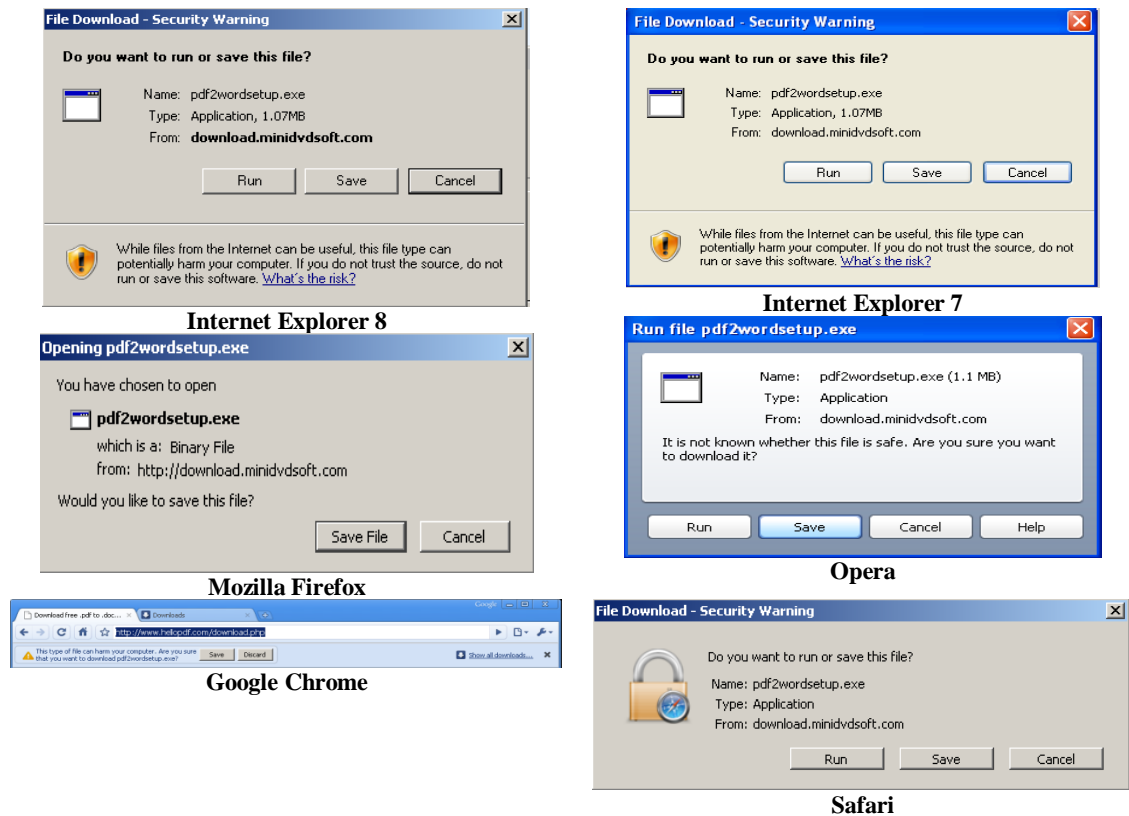


Figure 3: Security warning in various web browsers

By showing the six security warning messages in Figure 3, it can be noted that there was a clear method on how each security warning was presented except from the two versions of Internet Explorer. Internet Explorer used the footnote area to provide additional explanation and access to the help function whilst others did not use it at all. The usage of security icons was partially consistent except for Safari and Google Chrome. There were no warning icons used at all in Mozilla Firefox and Opera. When displaying the list of available choices (options) for users, each browser had a similar method. Opera represented the help function via a button whilst Internet Explorer 7 and 8 used a link to provide help. Surprisingly, Mozilla Firefox, Google Chrome and Safari did not provide a help function for the security warning. In terms of the title or header of the message, Internet Explorer and Safari used the same message, indicating “File Download-Security Warning” whilst the others presented the downloaded file name instead. When asked if they were satisfied with the level of information provided for the warning messages 43% were satisfied whilst 54% agreed that the information given was not enough. A somewhat interesting finding related to respondents who felt they had enough information based on the depicted warning, 17% decided to cancel or quit from the process whilst 9% decided to run the application straightaway. These users claimed that the information was enough for them to make a decision however they were still unable to demonstrate secure behaviour. When asked for additional content that would be useful when making such decisions, 38% would like to have details of the consequences if they were to proceed to run the application, 33% wanted to have confirmation of the legitimacy of the download, 27% wanted confirmation that their action was free from any kind of malware attack and 17% wanted to have provision of a proper help function. Some of the responses suggested that the computer should have a strict defence process, more understandable features and automatic virus scanning. Some of the respondents indicated they would like to see information of the provider of the application in order to gauge their trust level. They wanted to download only if it were from the provider that was well known and secured for them. A further option

considered by some users was to present historical information, indicating the choices made by previous visitors to the site (when presented with the same warning).

5. Conclusions and future work

Respondents were clearly concerned and aware of the security issues however, they were still unsure of the appropriate action to take when presented with certain security events. Respondents had demonstrated that they had used security technologies to help them to mitigate the risk of attacks (e.g. Antivirus, Internet Security etc). Usage of security technologies is fundamental but understanding how to use it and the risks or the threats they are facing is far more essential.

The results from the survey also revealed that users agreed that more appropriate information should be provided in security messages. Although such information will not directly solve the problem, it will give more meaningful support to help users' to make secure decisions and mitigate the risk of becoming a victim. Security features are expected to help users in making a decision but are still beyond the comprehension of users with a basic level of understanding. Users interact with computer with some purpose, when they have to cope with security features this can distract them from what they intend to do. The less security related activities interfere with their actions, the more likely they are to use the system. Yet, it is still not a guarantee for the users to use it correctly. Simply putting such functionality in software/systems without proper guidelines and user friendly features will lead to end user misunderstanding.

Current findings suggest that information provided in messages or warnings should use less technical terminology, offer sufficient provisional help to explain the circumstances and any further actions to be taken, and enough appropriate choices for the user. These results show the importance of usability as part of the design challenge. This study utilised scenarios to simulate computer security events, created based on the experience of dealing with computers as part of a daily routine and it was expected that most end-users dealt with similar issues. The current study was unable to determine the importance of the features as depicted in Table 1 (with the aim of developing a meaningful feature to help end-users). It is expected that practical experiment study will be conducted so that the end-user can face the real situation and be able to express what they really understand and need in relation to usability issues and their perception towards it. The results will be able to clarify the effectiveness of current security implementations and enhancement can be done to suit users' needs.

6. References

Albrechtsen, E. (2007), 'A qualitative study of users' view on information security', *Computers & Security*, vol.26, 4, pp.276-289.

Coffee, P. (2006) 'Security Onus Is on Developers'. [Online]. Available at: <http://www.eweek.com/c/a/Application-Development/Security-Onus-Is-on-Developers/> (Accessed: 03/03/11).

Furnell, S. M., Bryant, P. & Phippen, A. D. (2007), 'Assessing the security perceptions of personal Internet users', *Computers & Security*, vol.26, 5, pp.410-417.

ISO (1998) 'ISO 9241 Part 11: Guidance on usability'. [Online]. Available at: http://www.iso.org/iso/catalogue_detail.htm?csnumber=16883 (Accessed: 04/03/11).

Mannan, M. & Van Oorschot, P. C. (2008) 'Security and usability: the gap in real-world online banking', *Proceedings of the 2007 Workshop on New Security Paradigms*. New Hampshire ACM, pp. 1-14.

Microsoft (2011) 'Windows User Experience Interaction Guidelines'. [Online]. Available at: <http://msdn.microsoft.com/en-us/library/aa511440.aspx> (Accessed: 03/04/2011).

Mouratidis, H., Giorgini, P. & Manson, G. (2005), 'When security meets software engineering: a case of modelling secure information systems', *Information Systems*, vol.30, 8, pp.609-629.

Nielsen, J. (2003) 'Usability 101: Introduction to Usability'. [Online]. Available at: <http://www.useit.com/alertbox/20030825.html> (Accessed: 01/03/11).

Proctor, R. W., Lien, M.-C., Salvendy, G. & Schultz, E. E. (2000) A Task Analysis of Usability in Third-Party Authentication. *Information Security Bulletin*, 5, (W3schools), pp. 49-56.

Radle, K. & Young, S. (2001), 'Partnering usability with development: how three organizations succeeded', *Software, IEEE*, vol.18, 1, pp.38-45.

Saltzer, J. H. & Schroeder, M. D. (1975), 'The protection of information in computer systems', *Proceedings of the IEEE*, vol.63, 9, pp.1278-1308.

Schultz, E. E. (2007), 'Research on usability in information security', *Computer Fraud & Security*, vol.2007, 6, pp.8-10.

Tondel, I. A., Jaatun, M. G. & Meland, P. H. (2008), 'Security Requirements for the Rest of Us: A Survey', *Software, IEEE*, vol.25, 1, pp.20-27.

Venter, H., Eloff, M., Labuschagne, L., Eloff, J., von Solms, R., Herzog, A. & Shahmehri, N. (2007) 'Usability and Security of Personal Firewalls'. *New Approaches for Security, Privacy and Trust in Complex Environments*. Springer Boston, pp 37-48.

Whitten, A. & Tygar, J. D. (1999) 'Why Johnny can't encrypt: a usability evaluation of PGP 5.0', *Proceedings of the 8th USENIX Security Symposium*. Washington D.C, pp. 169-184.

Wool, A. (2004), 'The use and usability of direction-based filtering in firewalls', *Computers & Security*, vol.23, 6, pp. 459-468.

'Permission to reproduce this has been granted by Prof Steven M. Furnell Co-Chair of the Conference dated 25 March 2014'.

Assessing the usability of application-level security warnings

Zarul Fitri Zaaba^{1,2}, Steven M. Furnell^{1,3}, Paul S. Dowland¹ and Ingo Stengel¹

¹Centre for Security, Communications and Network Research
Plymouth University, United Kingdom

²School of Computer Sciences, University Sains Malaysia
Penang, Malaysia

³School of Computer and Security Sciences Edith Cowan University
Perth, Western Australia
info@cscan.org

Abstract

This paper investigates users' understanding of security messages that can be encountered on a daily basis whilst using their computer. An experimental study was conducted that made use of a custom-built program designed to capture security messages and examine users' views regarding whether enough information is provided by the application to enable them to understand the message and (where appropriate) make an informed decision. The study involved 36 participants with a range of education backgrounds and revealed that many participants still face difficulties in understanding the security warnings that they encountered on a daily basis. It is essential to use suitable and usable security features such as signal words, icons, help functions and accessible terminology in order to ensure that users fully understand security messages in the correct context. The results support the need for a better approach able to advance beyond current implementations of security warnings to improve end-users' chances of understanding and using security effectively.

Keywords: *Security warnings, Usability, Human Computer Interaction.*

Introduction

In the world of computing, interfaces become the medium of interaction to deliver the information to user. Most users' perceptions are based on what they feel and their experience with these interfaces. Computer security warnings are designated to protect users and their computers from any harm or potential threat. Wogalter (2006) puts forward the theory of hierarchy hazard control and states that warnings becomes the third line of defences after eliminating and guarding against hazards. Evidence suggests that some people do not read computer warnings (Egelman et al., 2008 and Sunshine et al., 2009), they quickly learn to visually and cognitively dismiss it (Bahr and Ford, 2010), they do not understand them correctly (Downs et al., 2006), they do not pay attention to it (Schechter et al., 2007) and consequently, this results in users frustration (West et al., 2008). For the end-user, usability becomes the main concern whilst security is a secondary matter (Besnard and Arief, 2004). Most of the aforementioned researchers assessed users' understanding of various security warnings and of various types of security warning interfaces. It can be suggested that warnings can be improved to provide more valuable information, hence able to reduce users' frustration. According to Bravo-Lillo et al., (2011), computer warnings not only protect users from harm but also are able to change influence their behaviour to comply with existing safety regulation. In contrast, in order to improve security warnings, it is essential to determine how users' understand the current security features by receiving various types of security warnings on a daily basis. This study makes use of Windows application security warnings using three web browsers (i.e. Internet Explorer, Google Chrome and Mozilla Firefox). These were the most popular browsers chosen by users (W3Schools, 1999 and W3Counter, 2004). This paper describes the results of the experimental study

that involves respondents from different backgrounds and may be relevant to the design of other configuration interfaces especially with regards to computer security warnings.

Background and Related Work

The interface of a particular system is important especially with regards to the security domain. Warnings should not be a replacement for good design and guarding but fundamentally it suffices as an add-on to good design (Lehto and Salvendy, 1995). A survey of 564 respondents conducted by Zaaba et al., (2011) revealed that end-users are still experiencing significant problems with understanding and responding to current state-of-the-art security applications, messages and potential menaces. Their results showed that problems in understanding help functions, complex security features, user interface difficulties and incidents of malware were the main concerns. Zurko et al., (2002) assessed the usability of Lotus Notes security warnings and found that the majority of its responses allowed unsigned content. Mandel et al., (2010) examined the effectiveness of improving warning efficiency. Based on the results, warning improvement was able to increase compliance albeit not at a statistically significant level. To this end, Downs et al., (2006) interviewed 20 non-expert participants to seek their level of understanding upon running into phishing sites. The results showed that, most of respondents were lacking awareness on phishing and security warnings, and thus failed to perform their duties. Hardee et al., (2006) performed a study with 56 students to assess their differences on how they perceived and made security decision with regards to computer and non-computer security domain based on security warnings scenarios. They revealed that the nature of gains across both domains were consistent in terms of protecting information, property and money. Furthermore, with regards to the loss of information it was varying within both decision domains. They proposed designers to make use of the attributes of security warnings based on the results of the study (i.e. explain the potential loss explicitly). Sunshine et al., (2009) conducted a survey with 400 users to examine their understanding and reactions on SSL warnings. Using two new design warnings on three web browsers, they suggested that using appropriate colours and text and reducing the warning frequency will improve the design of warnings. Raja et al., (2009) conducted a study with 60 participants to compare users' mental model on Vista Firewall (VF) using their prototype versus basic interface. They proved that their prototype improved users' mental model by revealing the hidden context. They suggested the designers should consider the impact of contextual factors before designing user interfaces of any security application. In summary, all of the aforementioned studies illustrated that computer security warnings still face a problem to convince users and to help prevent them from engaging in unsafe behaviours. It is essential to gather as much information as possible to determine whether users' are satisfied with every security warning that they encounter on daily basis. Then again, users' able to learn the importance of security warnings to convey security information in response to immediate problems. In order to improve users' understanding of security warnings, the authors developed a program to assess whether users' felt they were provided with enough information to answer various security warnings with confidence.

Methodology

In order to determine users' understanding whether enough information on the current features of security warning interfaces was available, a program has been created to capture users' daily security warnings from web browsers and other applications that they used. Then users made a decision whether enough information is provided to

enable them to understand the message and later able to make an informed decision. This has been implemented using the C# programming language. The subject group used this program for 5 days. For every security warning that users encountered, they received a custom dialogue (i.e. "Did you have enough information to understand the security dialogue that you just answered") with 3 options; Yes, No and Not sure. Following the ethical approval of the study, an invitation to participate was promoted to end-users via e-mail and via the University's Intranet portal.

After assessing the demographic information, for every security warning that users encountered, they received a custom dialogue box. The detection process was based on the class/application name of the three main web browsers used (Internet Explorer, Mozilla Firefox and Google Chrome) and from other applications (e.g. operating system, software etc). These three web browsers were chosen because previous research suggests that these are the most popular with end-users (W3Schools, 1999). According to Wogalter (2006) four main purposes of warnings are:

- i. To communicate an important safety information
- ii. To influence or to modify people's behaviour in a way that will improve safety
- iii. To decrease or to prevent health problem, workplace injuries and property damage
- iv. To act as a reminder to people that already knew this hazard

He claimed that using this guideline only, will not be adequate because every product and its design has its own characteristics and will involve people to use it. Based on these aforementioned principles, this study focused on various types of computer security warnings. The program captured these security warnings and stored them securely in a specific folder, while text data was stored in a database. This program also captured "receiving time" on every security warning that users received and "action time" with regards to the time when users took any action on the security message (i.e. clicking any buttons and clicking close).

Results and Discussion

Overall, 36 respondents participated in this study; 61% female and 39 % male. 69% of the total respondents were aged between 26-35 years with at least a degree level of education and have been using computer for more than six years. This indicated that the vast majority of these responses had evolved with Information technology during their early years. Respondents were primarily staff and students from Plymouth University and secondarily they were individuals from government and private sectors. They were allowed to use this program either at home or in the workplace as long as they consistently used it on the same computer. 53% of the respondents classified themselves as being intermediate computer skilled , 36% considered themselves as advanced users, 8% claimed to be experts and only 3% stated to be beginners. In terms of security software usage, a majority with 94% users claimed to use it, 6% did not used it (or were unsure). In the perspective of preferred web browsers, 47% had chosen Google Chrome, 33% used Mozilla Firefox, while only 20% used Internet Explorer. The last question regarding preferred operating system indicated that Windows 7 was the most popular chosen by 50% of the users, followed by Windows XP by 44%, Windows Vista and Mac OS X with 3% respectively. This paper addresses the clarity of messaging and conflicts with guidelines addressing the consistency of messages; and draws comparisons based on security warnings from three web browsers with regards to the consistency of experiences. The paper ends with conclusions and future works.

Clarity of messaging and conflicts with guidelines

Apparently, Microsoft (2011) was the only developer or provider that produced its own guidelines that covered the design principle, controls, commands, texts, windows, interactions, visuals, experiences and windows environments. Since Microsoft products are well-known and widely used by the majority of users, their guidelines had been used as a basis to compare the suitability with features on security warnings. Nodder (2005) conducted a Microsoft Case Study to discuss in further details on how users perceived implementation of security warnings and how trust can be developed with regards to the security warnings. This case study prompted four recommendations that should be applied to any trust interaction on computers; Let users make trust decision in context, make the most trusted option the default selection, present users with choices, not dilemmas and always respect the users' decision.

Below a set of images that have been captured are presented and analysed. The conflict began with the mismatch on the usage of signal icons in the context of security warnings. According to Microsoft (2011), the question mark icon should be used as a help entry whilst the information icon should be used to present only useful information in banners context. Nevertheless, in Figure 1, Figure 2 and Figure 3, the question mark icon and information icon had been used as a query sentence. This clearly conflicts with the guidelines.



Figure 1: Usage of question mark icon inappropriate context

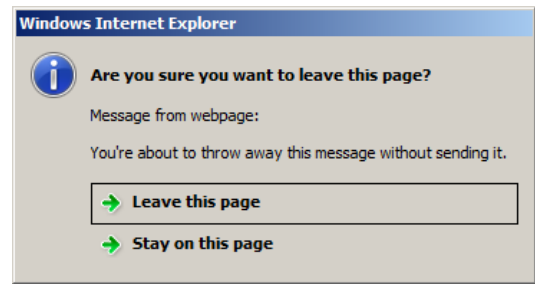


Figure 2: Usage of information icon inappropriate context

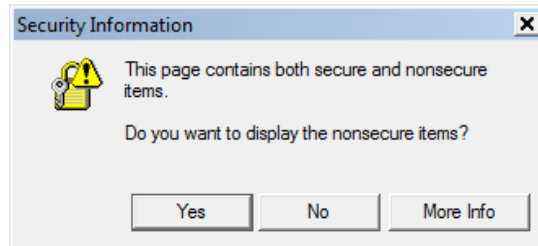


Figure 3: Technical terminology (i.e. secure & nonsecure items)

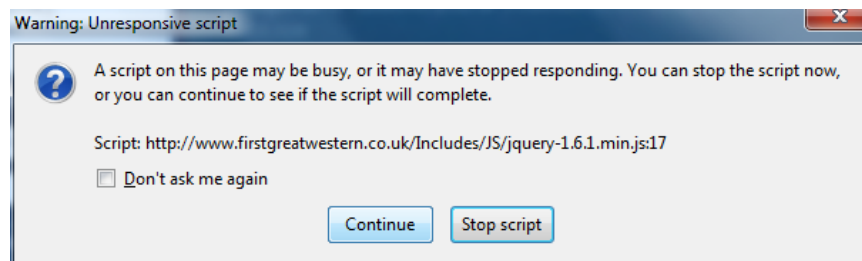


Figure 4: Usage of question mark icon in Mozilla Firefox in inappropriate context

Meanwhile, in Figure 3, the security warning used a technical approach to present the information to users (i.e. secure and non-secure item). In contrast, however, it can be argued if the non-secure items caused harm to the user, it must not be presented in the first place as a choice to end-users. A similar usage of technical jargon occurred in the security warning shown in Figure 4. The usage of question mark was inappropriate and the warning icon should be used instead, as the security warning presented a condition that might cause a problem for users in future as mentioned by (Microsoft 2011). Information is delivered using technical terminology that baffled end users (i.e. unresponsive script, stop script). It complicated the situation for end-users and made it hard to understand the security warnings. Furthermore, it was noted that 16 users who claimed “no” and “not sure” on custom dialogue box choices took an average of approximately 2 seconds to proceed with this security warning. It can be speculated that they took fast action to read or to get rid of this security warning based on the average time taken. It was not surprising, as the majority of this group claimed themselves as intermediate ability users.

In a different context, six users received a similar type of security warning as depicted in Figure 5 and all of them stated “no” and “not sure” when custom pop up appeared. They were among the users with higher and postgraduate background where four of them had intermediate computing skills, and two were beginners and advanced respectively. Users took 8 seconds on average with this type security warning. It can be speculated that they needed longer time as they did not know what to do with this

version of security warnings. With this version of warning, there was no help function available. This can be troublesome especially for non-technical savvy users. For the next example shown in Figure 6 were four users who agreed that not been enough information has been provided. The technical way in which information about the usage of “secure HTTPS connection” has been presented, contributed to the reasons users’ baffled with this security warning. Albeit users can use the “more info” button, in this context, they rarely decided to do that as already Bahr and Ford (2010) revealed. Users took only a quick glance of the pop up and considered it as highly annoying. More technical approaches to convince users were only suitable for those users that understood the meaning of terminology being used but not for laymen. As a result, 5 seconds average time was recorded on this scenario.



Figure 6: Technical terminology on security warning

Figure 5: Unknown icon been used in security warning before opening file

One of the most interesting findings of this study is linked to comparing the two signal icons shown in Figure 7. Obviously, the question mark icon should not be used in this context as it is intended only to be used as a help entry point as stated by Microsoft (2011). Another problem occurred with the usage of information icon in the footnote area. Two such icons should not be used concurrently in one security warning as it can confuse users. It is more useful if the security warnings are presented with a help function to help users to compare the basic and the complete set of options just before they press the options given. In another scenario, conflicts generated by signal words and signal icons have occurred as shown in Figure 8. The message stated that an error occurred with the connection. However, the warning icon has been used instead of an error icon. It has been shown that an error or a problem has occurred and clearly an error icon should be used instead. The wrong usage of signal icons and words contributed to users’ interpretation of every security warning that they received. It usually results in users’ dismissing the security warning even though an essential decision is needed.

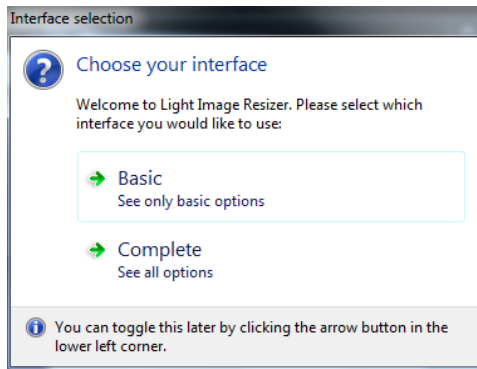


Figure 7: Scenario with two conflicting signal icons

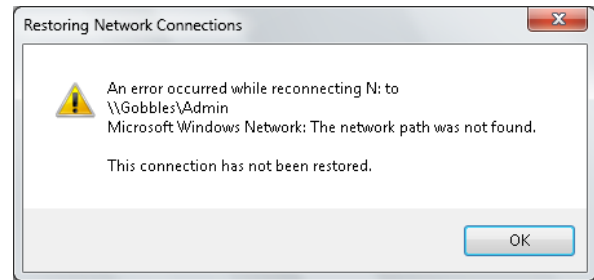
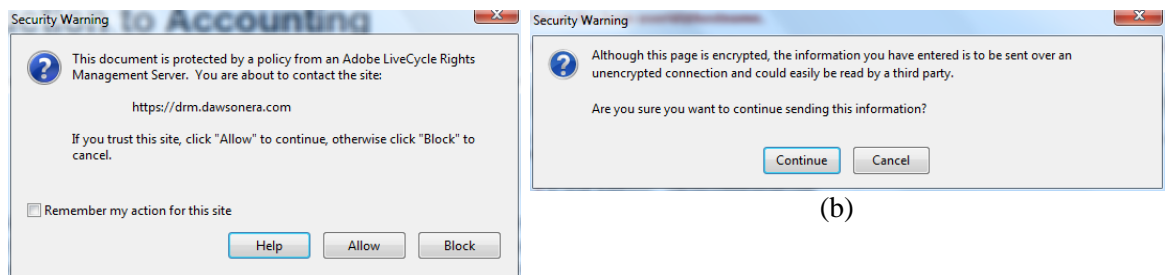


Figure 8: Mismatch of signal word and signal icon

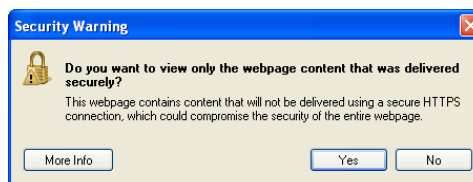
Consistency of messages

The authors showed a similarity with the header name of security warnings within two groups. These images used the same header name. However, it served for different purposes and contexts. Although these security warnings had a similar header name, the information is presented clearly differently, especially in terms of signal icons, technical terminology and help functions. Group A was presented with security warnings that had similar header “security warning” whilst Group B shared the same header of an “Open File – Security Warning”.



(a)

(b)

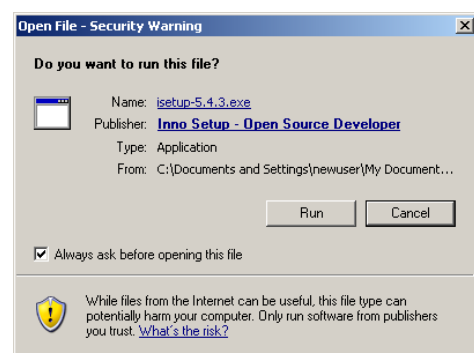


(c)

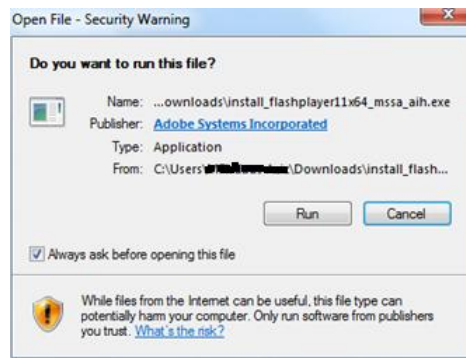
Figure 9: Security warnings from Group A



(a)



(b)



(c)

Figure 10: Security warnings from Group B

Referring to Group A, Figure 9a displays the security warning from an Adobe application. The security warning used the question mark icon and asked user whether to allow or block the website. In this context, the Warning icon should be used instead of question mark icon. Clearly the header was stated as a security warning and not as a help entry point (Microsoft, 2011). In Figure 9b the security warning from Mozilla Firefox is shown. It warned users that the connection was unencrypted and can cause a problem. Having said that, the terminology “encrypted” and “decrypted” was too technical for laymen. Furthermore, there was no appropriate help function for users supporting them in making the right choice. Clearly, it was meant to be a warning. Here, the signal icon warning should be used instead of the used question mark icon. On the other hand, a similar problem occurred in Figure 9c regarding a secure connection but apparently it used “HTTPS connection” terminology. In order to gain more information users need to press the help button. Users always neglect an unpleasant job and always get rid of any kind of pop up when it appears. Instead of using complex jargon, it is more useful to use understandable language for all users. In terms of signal icon usage, it was used correctly and is suitable to the context of warning.

In Group B scenarios security warnings addressing file opening within web browsers are presented. Here, the signal icon, information details and the help link have been used consistently on the footnote area based on Figure 10. However, the authors argued on the method of assistance on the footnote area as the information given suggested that users should run the software from the publishers that they trust. In reality, it was impossible for average users or laymen’s to know all the possible approaches/help options used by different publishers of the software that they wanted to download, especially if the software can be downloaded for free from website (i.e. it happen most of the time and preferred choice by end-users).

Consistency of experiences

The mini experimental study has been conducted to make a comparison based on features that have been presented in security warnings generated by a software download process from three web browsers. It compared the usage of signal icons, signal words, technical terminology and usage of help functions. This scenario has been chosen to reflect from one of the most popular security warnings prompted to users. Based on the current study results, user claimed that they were still in baffled with this type of security warning. In addition, these security warnings still have a high level of layout/presentation and content complexity. Hence, if users make a wrong decision, it could potentially harm and put them at risk. The study revealed that there were clear distinctions in the way security warnings were presented by selected web browsers (with default settings) as shown in Table 1. Using a similar approach to Zaaba et al.

(2011), this comparison showed that conflicts occurred on the usage of signal icons, signal words, inappropriate help functions and difficulties on technical terminology. As previously observed, this study focused on Windows based applications or program as majority of used preferred to use it. Microsoft (2011) provided specific guidelines on how these features can be used on security warnings and its application. By using this guideline as a basis of comparison, it will provide a more meaningful way for developers and end-users to understand on how it can be used in different contexts. This investigation provided a good platform to assess current and future security warning implementations based on the gathered information. Figures 11 to 13 present the security warnings encountered from three web browsers; Internet Explorer, Mozilla Firefox and Google Chrome respectively.

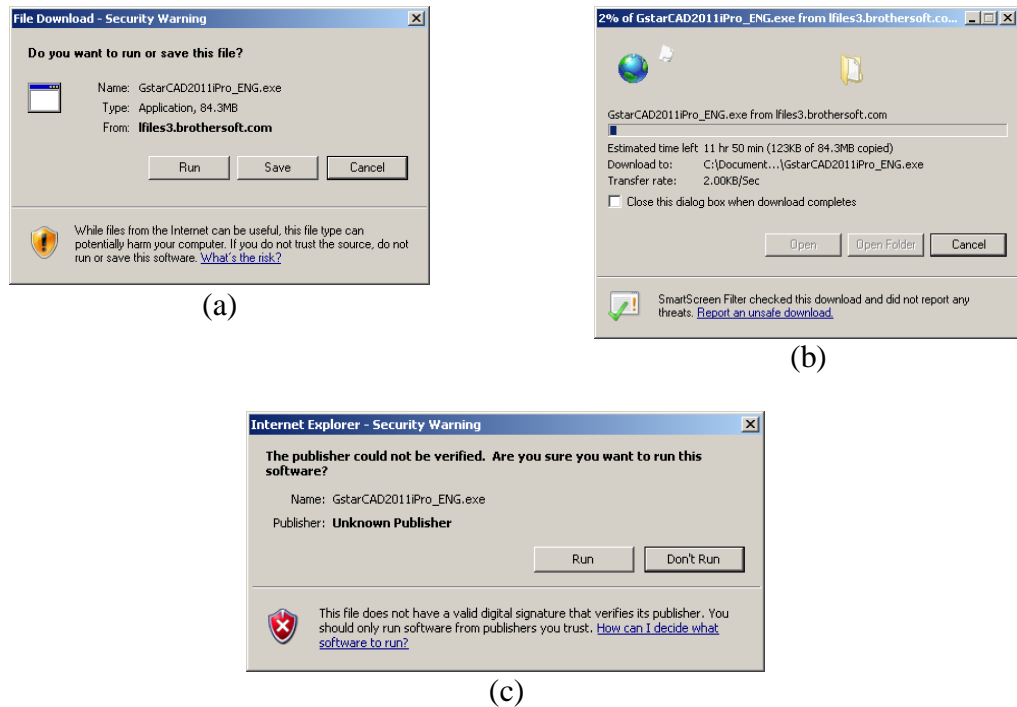


Figure 11: Security warning that users encountered from Internet Explorer

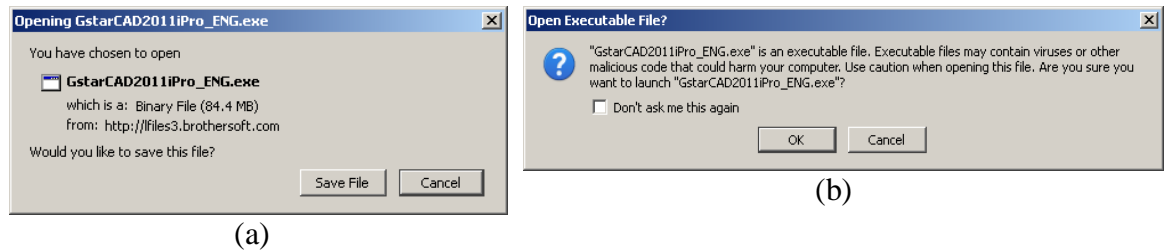


Figure 12: Security warning that users encountered from Mozilla Firefox



Figure 13: Security warning that users encountered from Google Chrome

After users executed the file, they received other versions of security warnings. In this scenario, only two browsers showed another security pop up; Figure 11b– Internet Explorer and Figure 12b– Mozilla Firefox. When users open the file based on the security warning they received, another security warning appeared as depicted on Figure 11c but only for Internet Explorer. A detailed of comparison of the various warnings is presented in Table 1.

	Internet Explorer	Mozilla Firefox	Google Chrome
Version	8.0.6001.18702	10.0.2	17.0.963.5
Usage of help function	<p>a: Provided a link for more information</p> <p>b: Details of information stated that no threats have been detected</p> <p>c: Provided a link for more information</p>	None provided	a: Provided a link for more information
Usage of signal words	<p>a: Depicted as security warnings</p> <p>b: None</p> <p>c: Depicted as security warnings</p>	None provided	a: Depicted as security warnings
Usage of signal icon	<p>a: Using warning icon to indicate a potential future problem. Using an unidentified program icon (white background)</p> <p>b: Using ticked icon with green colour Using the world icon and a folder</p> <p>c: Using an error icon</p>	<p>a: Using an unidentified program icon (white background)</p> <p>b: Question mark icon</p>	<p>a: Using warning icon to indicate a potential future problem. Using an unidentified program icon (white background)</p>
Execution process	Application will be saved in designated location by the user. Then, user will execute the file	Application will be saved in download dialogue box (pop up). Then, user will execute the file.	Application will be saved in the download folder (default). Then, user will execute the file.
Technical terminology	<p>a: The way data have been represented in a technical way with details of name, type and outlining the source.</p> <p>b: The way data have been represented in a technical way with details e.g. transfer rate, estimated time.</p>	<p>a: The way data have been represented using a technical expression. (i.e. binary file, file name etc)</p> <p>b: Usage of malicious codes Usage of executable files</p>	<p>a: The way data have been represented in a technical way with details of name, type and outlining the source. Publisher (digital signature) could not be verified</p>

	Internet Explorer	Mozilla Firefox	Google Chrome
	c : Publisher (digital signature) could not be verified		

Legend:

- a** = security warning that users encountered as first security warning prompt
- b** = security warning that users encountered as second security warning prompt
- c** = security warning that users encountered as third security warning prompt

Table 1: Comparison of the security warnings from three web browsers

Conclusions and future work

Overall 36 respondents had encountered several types of security warnings on a daily basis on their computers. The paper outlined a good approach on how information can be gathered from users' context (real situation) with the usage of capturing security message in various contexts and detection time (i.e. action time vs. receive time) on every security warnings. It can be noted that, users are still facing a dilemma with certain type of security warnings especially when it came across the complex terminology without a proper help functions and with too much information (i.e. security warnings layout) Users took more than 2 seconds in average to read the security warnings that they received. Some of the security warnings had more content or information than the other whilst it actually makes it worsen the situation. However, some of users took less than average time to read the warnings. Then again, it can be speculated that users only had a quick glance on certain security warnings and quickly got rid of it (i.e. possibly users did not understand it or habituation effects).

Current findings suggest that information and details on security warnings should use less technical terminology, offers appropriate and usable help functions (i.e. explain the circumstances in approachable way), and use appropriate signal icons and words in a correct context. It shows the importance of usability of security warnings even in general applications. End-users should be able to understand their current situation whilst using their computer. The current study was unable to ask many questions on the custom dialogue box (i.e. every detection of security warning will interrupt users' current task by displaying custom dialogue box). It is expected that enhancement can be done to current implementation of security warnings based on information that author's have gathered. Then it can be tested in a control group (e.g. expert, advanced, intermediate and beginner) so that a broad perspective from different users can be collected. Later, the results will be able to clarify whether the improvement and new enhancement meets users' satisfaction and needs. Microsoft (2011) provided a guideline on security warnings implementations in different contexts. It can be suggested to create a standard for the usage of signal words, icons, help functions and technical terminology so that users are able to learn and understand in a meaningful way the implementation of security warnings.

Acknowledgements

The authors would like to thank Kenan Kalajdzic for his assistance in the development of the software used to enable the data capture for the experimental study.

References

- Bahr, G.S. and Ford, R.A. (2010) How and Why Pop-Ups Don't Work: Pop-up Prompted Eye Movements, User Affect and Decision Making. *Computers in Human Behavior* 27(2), pp 776-783.
- Besnard, D and Arief, B. (2004) Computer Security Impaired by Legitimate Users. *Computers & Security* 23(3), pp 253-264.
- Bravo-Lillo, C., Cranor, L. F., Downs, J. S. and Komanduri, S. (2011) Bridging the Gap in Computer Security Warnings: A Mental Model Approach. *Security & Privacy, IEEE* 9(2), pp 18-26.
- Downs, J. S., Holbrook, M. B. and Cranor, L. F. (2006) Decision Strategies and Susceptibility to Phishing. In *Proceedings of the second symposium on Usable privacy and security*, ACM, Pittsburgh, Pennsylvania, pp 79-90.
- Egelman, S., Cranor, L. F. and Hong, J. (2008) You've Been Warned: An Empirical Study of the Effectiveness of Web Browser Phishing Warnings. In *Proceeding of the twenty-sixth annual SIGCHI conference on Human factors in computing systems*, ACM, Florence, Italy, pp 1065-1074.
- Hardee, J. B., West, R. & Mayhorn, C. B. (2006) To Download or Not to Download: An Examination of Computer Security Decision Making. *Interactions* 13(3), pp 32-37.
- Lehto, M.R. and Salvendy, G. (1995) Warnings: A Supplement Not a Substitute for Other Approaches to Safety. *Ergonomics*, 38(11), pp 2155-2163.
- Mendel, J., Mayhorn, C. B., Hardee, J. B., West, R. T. and Pak, R. (2010) The Effect of Warning Design and Personalization on User Compliance in Computer Security Dialogs. *Proceedings of the Human Factors and Ergonomics Society Annual Meeting*, 54(23), pp 1961-1965.
- Microsoft. (2011) *Window User Experience Interaction Guidelines*. [Online] Available at: <http://msdn.microsoft.com/en-us/library/windows/desktop/aa511258.aspx>, (Accessed: 13 February 2012).
- Nodder, C. (2005) Users and Trust: A Microsoft Case Study. In *Security and Usability. Designing Secure Systems That People Can Use* (Cranor LF and Garfinkel S, Eds), O'Reilly, pp 589-605.
- Raja, F., Hawkey, K. & Beznosov, K. (2009) Revealing Hidden Context: Improving Mental Models of Personal Firewall Users. In *Proceedings of the 5th Symposium on Usable Privacy and Security*, ACM, Mountain View, California, pp 1-12.
- Schechter, S. E., Dhamija, R., Ozment, A. and Fischer, I. (2007) The Emperor's New Security Indicators. In *IEEE Symposium on Security and Privacy, 2007*. pp 51-65.
- Sunshine, J., Egelman, S., Almuhimedi, H., Atri, N. and Cranor, L. F. (2009) Crying Wolf: An Empirical Study of Ssl Warning Effectiveness. In *Proceedings of the 18th conference on USENIX security symposium*, USENIX Association, Montreal, Canada, pp 399-416.
- W3Counter. (2004) *Global Web Stats: Web Browser Market Share*. [Online] Available at: <http://www.w3counter.com/globalstats.php>, (Accessed: 10 February 2012).

W3Schools. (1999) Browser Statistics: Web Statistics and Trend (Month by month). [Online] Available at: http://www.w3schools.com/browsers/browsers_stats.asp, (Accessed: 10 February 2012).

West, R., Mayhorn, C. B., Hardee, J. B. and Mendel, J. (2008) The Weakest Link: A Psychological Perspective on Why Users Make Poor Security Decisions. In *Social and Human Elements of Information Security: Emerging Trends and Countermeasures* (Gupta and S. Sharman, Eds), Hershey, PA: Idea Group Inc, pp 43-60.

Wogalter, M.S. (2006) Purposes and Scope of Warnings. In *Handbook of Warnings. (Human Factors /Ergonomics)* (Assoc LE, Ed), pp 3-9.

Zaaba, Z. F., Furnell, S. M. and Dowland, P. S. (2011) End-User Perception and Usability of Information Security. In *Proceedings of the Fifth International Symposium on Human Aspects of Information Security & Assurance (HAISA)*, London, pp 97-107.

Zurko, M. E., Kaufman, C., Spanbauer, K. & Bassett, C. (2002) Did You Ever Have to Make up Your Mind? What Notes Users Do When Faced with a Security Decision. In *Proceedings of the 18th Annual Computer Security Applications Conference*, pp 371-381.

'Permission to reproduce this has been granted by Prof Steven M. Furnell Co-Chair of the Conference dated 25 March 2014'.