2019

An Evaluation of Targeted Security Awareness for End Users

Mahmoud Ahmmed Ahmmed, Najem

UNIVERSITY OF
PLYMOUTH

AN EVALUATION OF TARGETED SECURITY AWARENESS FOR END USERS

by

NAJEM AHMMED AHMMED MAHMOUD

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

DOCTOR OF PHILOSOPHY

School of Computing, Electronics and Mathematics

May 2019

Acknowledgements

Firstly, I would like to give all praise and gratitude to Allah, the almighty, for everything he has given during my lifetime. Without him, none of this was possible. Thanks to him, I have had the health, perseverance, and potential to reach this stage of my PhD research.

I also would like to thank my beloved mother and father for their encouragement, support and prayers throughout this journey, without them, I would not have this stepping-stone into society, which defines the type of man that I became today. My hopes is that this research fulfils their hearts with pride and joy.

My wife and children, I send a great vote of thanks for their inspiration, dedication, and endurance throughout this journey. Their patient on all of those long days, nights, and holidays without me has resulted in this piece of work. May Allah bless them.

To my sisters and my brothers, I thank you for all of your prayers and motivation during this period of my life.

This thesis would not have been completed without the wisdom and guidance of Professor Steven Furnell and Dr.Paul Haskell-Dowland. Their enormous help, constant support, constructive feedback, and professionalism has aided me throughout the research and allowed me to nor only learn on the matter, but also grow. It has been a pleasure and rewarding experience working under your guidance and I wish you all the best.

Finally, I would like to thank all my friends and colleagues, by their positive contribution towards my progress. Many of them deserve mentioning, but mentioning all names would become too difficult. May Allah bless you all and I wish you all the best.

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 Doctoral College Quality Sub-Committee.

Work submitted for this research degree at the University of Plymouth has not formed part of any other degree either at the University of Plymouth or at another establishment.

This study was financed with the aid of a studentship from the Ministry of Higher Education and Scientific Research - Libya.

Publications:

1. Mahmoud, N., Furnell, SM., & Dowland, PS. (2017). Towards Targeted Security Awareness Raising. *In Proceedings of the Annual Information Institute Conference, 18-20 April, Las Vegas, NV. USA.* ISBN: 978-1-935160-18-2. URL: http://029e2c6.netsolhost.com/II-Proceedings/2017/IIVC2017_MAHMOUD_et_al.pdf

2. Mahmoud, N., Furnell, SM., & Dowland, PS. (2018). Design Principles and Guidelines for Targeted Security Awareness. *In Proceedings of the Annual Information Institute Conference, 26-28 March, Las Vegas, NV. USA*. ISBN: 978-1-935160-19-9. URL: http://029e2c6.netsolhost.com/infoinst15/annual-information-institute-conference-proceedings/

Word count of the main body of thesis: **56,851**

Signed.....

Date.....15-05-2019.....

Abstract

An Evaluation of Targeted Security Awareness for End Users

Najem Ahmmed Ahmmed Mahmoud

Users are frequently cited as being the weakest link in the information security chain. However, in many cases they are ill-positioned to follow good practice and make the necessary decisions. Part of the reason here is that even if security awareness, training and/or education have been provided, some of the key points may have been forgotten by the time that users find themselves facing security-related decisions.

There are several scenarios in which users find themselves facing security-related decisions. However, while in such situations, many do not have an adequate understanding of security and do not receive the appropriate advice to make the necessary decisions they are required to make. One possible solution to this situation is to ensure that security guidance and feedback are available when necessary, and to provide effective information that can help the user make informed decisions at the right time to avoid security risks. Such targeted security awareness-raising has the potential to provide support to users at the point of need, in order to take the necessary security precautions and make informed decisions.

To examine the approach of targeted security awareness-raising, an experimental study was conducted to test the effectiveness of this approach and presents the results of the study. This experiment was based around the scenario of connecting to Wi-Fi networks, and determining whether participants could make informed and correct decisions about which networks were safe to connect to. Four alternative interfaces were tested (ranging from a version that mimicked the standard Windows Wi-Fi network selection interface, through to versions with security ratings and additional guidance). The aim of the experiment was to determine the extent to which providing such information could affect user decisions when presented with a range of networks to connect to, and help to move them more effectively in the direction of security. The findings revealed that, users always tended to connect to the known names first in the absence of security information and very prone to connecting to names that look like a

known name. In addition, claimed signal strength is also found to be a persuading factor. Results have also revealed that users can be influenced positively, if suitably visible feedback and guidance is given at the task in hand.

While users did not exhibit perfect behaviour in terms of selecting more secure networks in preference to less protected ones, there was a tangible improvement amongst the users that had been exposed to the selection interfaces offering and promoting more security-related information. In common with findings from other security contexts, these results suggest that users' security behaviours can be positively influenced purely through the provision of additional information, enabling them to make better choices even if the system does not provide any further means of enforcement.

This research also has led to introduce a series of related design principles and guidelines that have been identified from the experimental study. To study the effectiveness of the proposed design principles and guidelines, existing applications have been examined in order to evaluate their consistency with these recommendations and have identified scope for improvement, which would in turn assist user awareness via a more targeted approach. This is illustrated through an example where the design principles and guidelines are applied to the appearance of email notifications that aim to assist users in spotting phishing threats.

In addition to the aforementioned results of the experimental work, the findings demonstrate that the abstraction of design principles and guidelines allows the lessons to be transferred to other contexts. Furthermore, following and applying the guidelines enables subtle but relevant refinements to the user interface. Considering the application of this security lesson more broadly, guidance and feedback/nudges should be provided by default in other security contexts.

Table of Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Introduction

Modern organisations are now characterized by their primary reliance on information systems. This makes it intuitive to rely on cybersecurity to ensure that related systems and data are available when needed, and protected from damage (Furnell et al., 2019). Over the past few years, the importance of information security has become clearer for individuals and organisations. Many of the witnessed security breaches indicate that protecting IT systems becomes a prominent concern and is no longer an optional duty (Crossler et al., 2013; Furnell et al., 2018). This is true, not only for companies offering their services through IT systems, but also for personal computer users (Korovessis et al., 2017). Unsurprisingly, the World Economic Forum (WEF, 2017) rated the large-scale breach of cybersecurity associated with data fraud or theft as one of the five most serious threats facing the world today.

According to the European Union Agency for Network and Information Security (ENISA, 2010), that analyses the state-of-the-art in cyber threats, the number of people and businesses most likely to suffer from security breaches is also increasing. Reasons depend on many factors, including vulnerabilities in the new and the existing technologies, along with device integration, the notable increase in the 'always on' connections and the continuous significant increase in the number of users within the European Union (EU). ENISA also stated that awareness of the risks along with the available safeguards is the first line of defence for security of information systems and networks.

The most serious security breaches are due to several failures from people, processes, and technology. However, the human factor is a fundamental issue. The report from PricewaterhouseCoopers (PwC, 2012) found that the main cause is often a lack of investment in staff security education. It is worrying that only 20% of surveyed employees had attended any form of cyber security training. This highlights the importance of staff awareness and vigilance, in addition to technical security solutions, that will effectively contribute to the protection of the organisation IT systems (DCMS, 2017).

In the information security chain, despite the advances in security technology, end-users are often perceived as the weakest link. In fact, even the strongest technical protection systems can be bypassed if an attacker successfully deceives the user to reveal a password, open a malicious email attachment, or visit a compromised Website (Heartfield and Loukas, 2018). There has been an increasing focus on the importance of information security awareness (Albrechtsen and Hovden, 2010; Banerjee and Pandey, 2010; Drevin et al., 2007; Hinson, 2014); with the aim of reducing human error, theft, fraud, and misuse of computer assets (Drevin et al., 2006).

One of the main challenges facing organisations is to ensure that their employees behave appropriately by increasing the awareness of IT security to avoid security breaches. Organisations have significantly improved information security awareness programmes to deal with the rapidly increasing threat. Furthermore, they have taken steps such as adding new features to their information security systems, setting new strategies, placing new information security task components and adding more people (Ernst and Young, 2016). In addition, the latest security solutions are implemented to ensure long-term asset protection and security. However, if the employees are unaware of the security threats and the importance of the organisation's IT assets, and

if they are prone to be manipulated, there will be no security tool or solution that would prevent such assets from being compromised (Švehla et al., 2016).

There is no doubt that the abovementioned steps and amendments would contribute to enhance information security capabilities. However, employees are continuing to be one of the most critical factors in terms of ensuring the security of IT systems and the information they deal with. In many cases, IT security incidents are the result of employees' activities made from distraction and lack of awareness of IT security policies and procedures. For example, according to Ernst and Young Global Information Security Survey (EY's GISS) (2017), careless or unaware employees continue to be perceived as an increasing risk. Participants in the same survey stated that careless employee behaviours represent a significant point of weakness for most organisations, as 77% of the respondents stated that they are worried about poor user awareness and behaviour and consider careless staff as the most potential source of attacks. Similarly, Ponemon Institute 2017 Cost of Data Breach Study revealed that 28% of organisations reported a human error or employee negligence as the primary root cause of data breaches (Ponemon Institute, 2017). Likewise, the DCMS Cyber security breaches survey 2017 indicated that 72% of reported security breaches occur after a staff member receives a fraudulent email (DCMS, 2017).

Recently, according to Ernst and Young report (2018), a significant number of organisations consider themselves to be more at risk compared to a year ago. For example, careless or unaware employees are seen by 34% of organisations as the vulnerability that has most increased their risk exposure over the past 12 months. Unsurprisingly, this is due to the fact that cyber attackers are becoming more sophisticated, while organisations are becoming increasingly connected and reliant more on the emergence of new technology that creates opportunities and risks. This

enormous development of connectivity driven by the growth of the Internet of Things (IoT) in many organisations has introduced new vulnerabilities that can be exploited by attackers (Ernst and Young, 2017).

There is growing recognition that all staff need some level of understanding of the part they can play in maintaining the security of organisation's data and systems. Many organisations offer security awareness training, yet there is real concern about their effectiveness. In fact, a recent study by Axelos (a joint venture of the UK Government and UK firm Capita) found that professionals responsible for security awareness training reported that the training was largely ineffective. All employees need some level of understanding on their role in preserving the security of the organisation's data and systems. However, a significant number of companies never provide training to help employees identify email-based cyberattacks, and many others do so only once, when the employee joins them (Caldwell, 2016).

One of the key reasons these systems are not always sufficiently secured resides in the users' issues related to understanding how to use technology security. Moreover, one of the long-term challenges associated with security technology is to ensure that it is available and consistent in a manner that can be used without causing confusion. Unfortunately, this theory has often failed to prove successful with how security is presented in practice, creating difficulties to the users when it comes to understanding security features. This often leads to mistakes and reluctances toward the use of security technology measures (Furnell, 2016).

Many issues still need to be solved, including finding a way to target the right users at the right time. Extensive training and security awareness programmes are designed to be delivered either as an introduction before the new staff start their job, after a breach

occurred or as a preventive line against a new threat. This can lead to users forgetting some key points when they face security-related decisions despite being exposed to security awareness, training, and/or education. In fact, some security issues need to be timely solved requiring users to be made aware and informed, in a timelier manner. In order to reinforce the human factor, it would also be desirable to deliver targeted security awareness to avoid the problem of overloading the end users with information about security issues, which may confuse or distract them.

Targeted security awareness raising is an emerging and promising approach that has the potential to be effective in raising the security awareness of the users by providing guidance and nudges during the task in hand. The use of the targeted security awareness raising approach has become more imperative than ever before. It is an emerging domain that has the potential to be considered as a valuable method for raising the security awareness of end-users by ensuring that security guidance and feedback is available at the point of need. This provides effective information to help the users to make the right timely decision to avoid security risks.

The information presented and the provided security guidance and feedback should serve, help, and be useful for skilled and non-skilled users. This includes staff, students, and personal users to understand the security issue. Targeted security awareness approach is intended to serve all categories of users who are using today's IT devices. It is imperative that the interface design and the provided information should assist non-skilled users to understand the security issue they are facing in order to help them to make informed decision, as such users have limited computer skills and are representing the largest population of computer users, while skilled users should have the additional supportive security features and information to access if they need further details to better understand the security issue.

It is worth noting that, the term 'end-user' referred to in this research comprises all user categories. This includes skilled and non-skilled IT users, and applies irrespective of whether they are employees, school or university students, or where they are using their technology (e.g. home, workplace, or public spaces).

1.2 Aims & Objectives

The main aim of this project is to study targeted security awareness raising approaches and investigate the possibility for new opportunities in which this approach could be useful and successful in terms of raising the security awareness for end users in timely manner. This aim is planned to be achieved through the following objectives:

- This project seeks to study potential opportunities where targeted security awareness raising approach can help end users in identifying potential threats inherent in IT systems before using them.
- Investigates opportunities where users can have support in real-time by providing adequate security information and appropriate recommendations to raise security awareness before they make their decisions, so that they will have a chance to understand the risk before they take an action that may endanger their system.
- Investigates the feasibility of the targeted security awareness by conducting experimental study to evaluate this approach.
- Develop mock-up interfaces for a security scenario that can offer best advice and recommendations to users by increasing their security awareness to avoid the potential security risks in the chosen scenarios.

1.3 Thesis Structure

The remainder of the thesis comprises the following chapters in order to addresses the aforementioned objectives.

Chapter 2 mainly presents a literature review of information security awareness. It also provides the evidence of problems due to lack of staff awareness and highlighted that a significant number of end-users are unaware of their exposure to security risks which leading to reduce the strength of the first line of defence. Moreover, it gives an overview to Information technology security learning continuum as well as presenting different definitions and perceptions of information security awareness in addition to present definitions and perceptions for neighbouring areas, which are security training and education. Furthermore, the chapter also discusses facts behind the increased need and importance of information security awareness through giving an overview of the increased need for security awareness, discussing the fast evolving threats, the key obstacles to information security effectiveness and ends with an extensive discussion about the current used methods to raise security awareness.

Chapter 3 discusses and reviews opportunities to increase awareness based on the principles of targeted security awareness. The chapter begins to discuss the shortcomings of the current security warnings and provides a conceptual background for a targeted security awareness-raising approach. Furthermore, it explores some examples of the targeted security awareness-raising approach. This chapter ends with a deep discussion of the opportunities to increase security awareness for end users by utilizing the targeted security awareness that can be used to conduct experiments for this project.

Chapter 4 examines the issue of targeted security awareness raising, and presents the results of an experimental study conducted to test the effectiveness of the approach. The aim of the experiment is to determine the extent to which providing security guidance and feedback could affect user decisions when presented with a range of networks to connect to, and help to move them more effectively in the direction of security.

Chapter 5 presents a series of related design principles and guidelines that have been identified from the experimental work. Seven valuable security design principles were identified that could be used by software developers as guidance to include improved security features in their software to help to make users fully aware of the security threats they may encounter.

Chapter 6 surveyed email applications in order to evaluate their consistency with the identified design principles and guidelines and has identified scope for improvement, which would in turn assist user awareness via a more targeted approach. This is illustrated through an example where the design principles and guidelines are applied to the appearance of email notifications that aim to assist users in spotting phishing threats.

Chapter 7 offers the conclusions arises as a result of this research. Moreover, this chapter highlights the key contributions and achievements, the limitations of the research, and the opportunities for future work that can be undertaken. It then ends with a summary of the future of cyber security awareness.

Chapter 2

Information Security Awareness

2.1 Introduction

In today's world, organisations have become digital by default. Although not every organisation offers its products and services through digital systems, they all run their business with the technology and processes of the Internet era. In addition, in the connected world brought by the Internet of Things (IoT), the digital landscape is growing rapidly, with each device owned or used by the organisation, representing another node in the network (Ernst and Young, 2017).

In regards to the online exposure, according to DCMS (2018), all the surveyed UK businesses stated that they rely on some form of digital communication or services. For example, 98% of UK businesses mentioned that they are dependent on online services, and similarly, 93% of charities stating the same. Furthermore, 52% of all UK businesses and 48% of charities consider online services as a core component of the goods and services they provide (DCMS, 2018).

Furthermore, the emergence of new technologies requiring Internet access led to a significant increase in the number of connected devices. According to Statista (2018), the number of connected devices (Internet of Things; IoT) worldwide is predicted to grow almost to 31B by 2020 (Statista, 2018).

In the meantime, executives worldwide recognise the increased high risks of cyber insecurity. For example, in the Global State of Information Security Survey (GSISS) 2018, leaders of organisations that use automation or robotics point out their

awareness of the potentially significant consequence of cyber-attacks. Yet, despite this awareness, many companies at risk of cyber-attacks remain unprepared to deal with them, with 48% of the surveyed companies stated they do not have an employee security awareness training programme in place (PwC, 2018).

As such, where the vast majority of operations are conducted and empowered through technology, information security has become a well-established component as business increasingly appreciate its value. It has been recognised that the human element plays an important role in information security. Therefore, any organisation that pursues to protect its IT systems and minimizes security risks should ensure that its employees have an adequate security awareness of the underlying security threats (Korovessis et al., 2017).

All of the aforementioned factors and figures have made the protection of the IT systems paramount to ensure business continuity and reliable connection. The IT security systems consist of hardware and software as well as users who operate and deal with these systems. Users are a key factor in ensuring the IT security, and they are perceived to be the first line of defence if they act appropriately. Thus, their security awareness regarding the emerging threats is vital to contribute protecting these systems.

This chapter discusses the trends and the current situation of the security awareness of end users, and highlights the problems related to lack of staff awareness. Moreover, it gives an overview of Information technology security learning continuum. It also presents definitions and perceptions for neighbouring areas including security training and education. Furthermore, the chapter discusses facts behind the increased need and importance of information security awareness, discussing the fast evolving threats,

the key obstacles to information security effectiveness as well as the currently used methods to raise security awareness.

2.2 Evidence of Problems Due to Lack of Awareness

While the technical faults are also a key element in the security accidents, deliberate or accidental human error is also considered as a key contributing factor in the occurrence of security breaches (PwC, 2015).

In terms of security breaches experienced in 2018, these results are similar to the number of security breaches witnessed in 2017, where 43% of businesses faced some kind of security breach over the Internet in the past 12 months (DCMS, 2018).

Over the last few years, staff often compromise the IT security of their organisations unintentionally. For example, as shown in Figure 1, the DCMS Cyber security breaches survey 2018 revealed that 75% of businesses reported cyber security breaches that take place after a staff member receives a fraudulent email (DCMS, 2018).

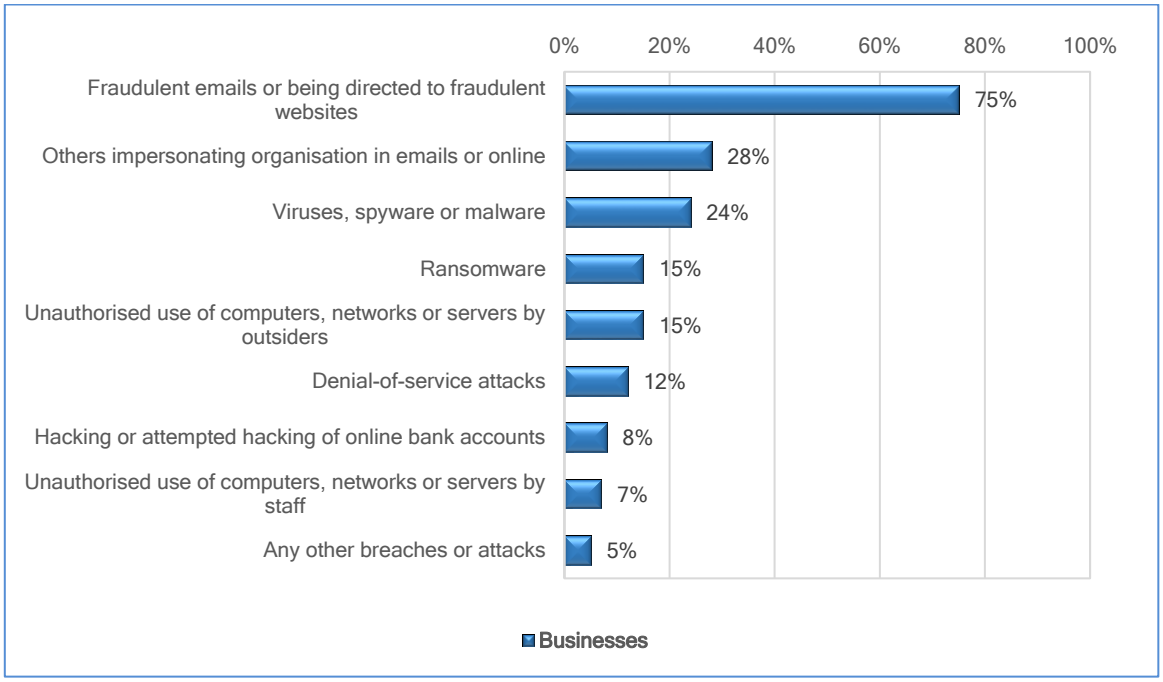

Figure 1: Attacks or breaches experienced in the last 12 months (DCMS, 2018)

Moreover, the results in Figure 2 indicate that the top four breaches that caused the most disruption to the businesses were related to exploiting staff unawareness. For instance 48% of the incidents were related to the staff being sent fraudulent emails or websites which were most commonly identified as the most single disruptive breach, 13% related to malware, 10% impersonating organisation in emails or online and 7% related to the ransomware. These results are similar to the findings of the 2017 survey (DCMS, 2018). This type of breaches or attacks is the most experienced by businesses compared to other types of attacks. As for technology related breaches, these were relatively minimal.

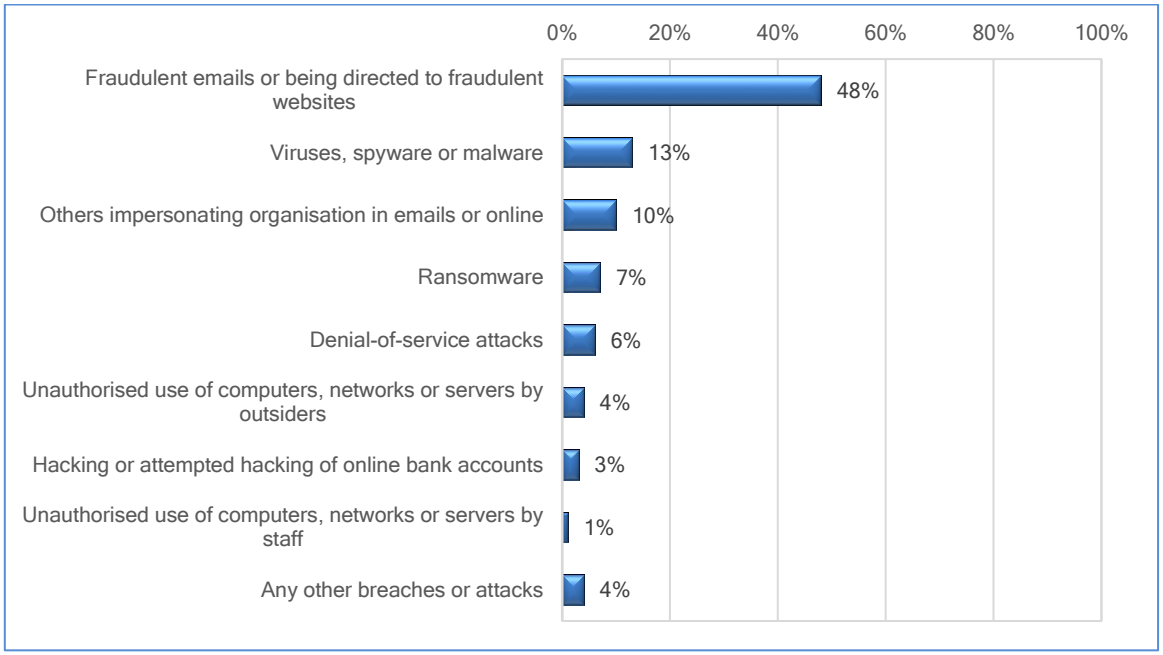

Figure 2: Attacks or breaches causing the most disruption (DCMS, 2018)

Although the vast majority of organisations still consider security as a high priority, as 74% of businesses considering cyber security a high priority for their senior managers, this is not in line with the other findings presented in this report. For example, with regard to adopting and providing security training, only 20% of businesses overall have had staff that attended any form of internal or external cyber security training in the past 12 months, which is similar to what is seen in the previous years. The overall figure consists of 12% of businesses providing internal training, 7% providing external training, and 10% of staff attending seminars or conferences. Large firms seem to have the greatest inclination to provide training for their staff by 65%, whereas only 26% of small firms are doing so.

Moreover, most businesses tend to provide training to directors or senior managers. For example the DCMS cyber security breaches survey (2018) showed that 76% of businesses provide it senior level staff, whereas only 30% provide it to IT staff, 26% provide it to staff members whose job role includes information security, and only 25% provide it for staff who are not security or IT related.

It is worth mentioning that businesses reporting cyber skills gaps are less likely to train their staff on cyber security. For example, 12% of businesses that reported a lack of skills had done so, compared to 20% overall. This suggests that organisations that have identified the problem of skills gaps have not necessarily taken the required steps to address this issue by providing staff training. The survey presented an explanation of this situation, where several barriers to training were raised in interviews.

Barriers to training

The survey raised many barriers to training, including cost, format, regularity, and lack of visibility of the need for training:

- It was perceived that induction training, irregular training, or non-mandatory training could easily be forgotten. There have been various examples of good practices to address this issue. For instance, one small organisation conducted individual sessions with each staff member, while another approached this by adopting a more targeted training, asking staff to do training sessions only after failing on an internal penetration test. Another organisation adopted another approach by asking all their staff to complete an annual online cyber security module, without which they will not be eligible for their annual bonus.
- The face-to-face training sessions were perceived to be difficult to accomplish due to the cost and logistics. Therefore, some organisations have already sought or adopted online video training courses or seminars.
- Those who took cyber security issue seriously sometimes have not realised the value that training will add to what they already felt they knew.

The report concluded that awareness raising and involvement among wider staff is vital. The most destructive breaches are most commonly spotted by individual staff rather

than automatically captured by anti-malware solutions, and this is similar to what has been reported in 2017. Organisations also realised the value and the good impact of regular and targeted training to all staff. However, in reality, staff training remains rare as mentioned earlier. Moreover, it is unlikely that businesses in the last survey have responded to breaches with additional staff training compared to 2017.

2.2.1 End-Users Still Unaware of Security Risks

Despite the availability of a wide range of security protection tools such as anti-virus scanners, firewalls and other security solutions, risky behaviour revealed by the end user has the potential to make devices vulnerable to compromise (Shepherd et al., 2013). Recent stories have highlighted that a significant number of end-users are unaware of their exposure to security risks. Due to the high level of breaches witnessed in recent times, it is more important than ever to raise the security awareness within organisations by making users the first line of defence. In this respect, all industry sectors have witnessed staff-related breaches, however, the technology companies in this regard has seen a better performance in comparison to other sectors (ENISA, 2010). Reasons behind the serious security breaches are associated with multiple failures in technology, processes, and people. It is not surprising that staff is one of the main underlying causes behind many of these breaches (PwC, 2013).

According to Crowd Research Partners 'Insider Threat" Report (2018), people often associate the term "Insider Threats" in cyber security with malicious staff who intend to deliberately damage the company either through theft or sabotage. In fact, negligent staff or contractors are equally causing a large number of security breaches and leaks unintentionally. The most damaging security threats today do not arise from malicious outsiders or malware but from trusted insiders, whether malicious or negligent insiders. For example, 90% of the surveyed organisations said they felt vulnerable to insider

attacks. Furthermore, 51% of the surveyed companies stated that they are worried about accidental/unintentional data breaches through user carelessness, negligence or compromised credentials and 47% stated that they are worried about the same breaches but from deliberate malicious insiders.

Practically, security professionals have a prominent responsibility in detecting, countering, and responding to cyber-attacks. However, this task becomes more difficult when threats come from inside the organisation from trusted and authorised users. It is often difficult to determine when users are simply doing their job or something illegal or unethical. The study conducted by the Crowd Research Partners (2018) indicated that 56% of regular staff and 55% of privileged or admin IT users pose the biggest insider security threat to organisations, followed by contractors with 42%.

In terms of the biggest enabler of accidental insider threats, the Crowd Research Partners (2018) revealed that incidental exposure by staff is perceived to be the most common enabler of accidental insider threat. For example, 67% of cyber security experts consider phishing attempts as the biggest vulnerability for accidental insider threats. Phishing attacks are used to deceive staff into sharing sensitive company information by providing phishing attempts as a legitimate business or a trusted contact, which often contain malicious attachments or hyperlinks to compromised websites. This is followed by 56% of the respondents who perceive weak or reused passwords as an enabler of accidental insider threat, 44% of the respondents referred to unlocked devices, the same percentage referred to bad password sharing practice, and 32% of the respondents mentioned unsecured Wi-Fi networks.

Moreover, regarding the enabling risk factors, 37% of the respondents in the same survey said that the key enabling risk factors were related to the very large number of

users with excessive access privileges, 36% said this was related to an increasing number of devices with access to sensitive data, and 35% said it was related to the increasing complexity of information technology. Noticeably, the human factor is also still playing a key role in this regard as 31% of the respondents considered the lack of staff training or awareness as an enabling risk factor. In addition, 53% of the surveyed organisations have reported insider attacks against their organisation in the last 12 months, 46% said insider attacks were the same as seen a year ago and 27% said the insider attacks are becoming more frequent. These results indicate that staff still play a key role in the security breaches.

The following are examples are also representing staff related breaches which have been reported in information security breaches survey conducted by PwC in 2013:

- Regarding the use of social networks, a Staff member at a large insurer in the South-West has misused Facebook as well as internal email systems. Fortunately, a routine security monitoring picked up this breach and it was quickly solved few days after it occurs.
- Regarding using email services, in a large government body there was an employee using their email service to send sensitive emails from his work email account to his personal email account. This breach was only discovered by accident. Because of the sensitive nature of the information used, it's was hard to put a value on the lost data. After this breach, the government body took legal action against the employee, and further, they improved processes and conduct additional staff training to avoid such breaches.
- With regards to the infection by viruses and malicious software, at a small Yorkshire charity there was a volunteer who received an email containing a link, the volunteer

clicked on the link inadvertently as result of this action the computer was infected with a blackmail virus. This virus was quickly removed using anti-virus software. Another story with regard to the infection of viruses and malicious software is seen in a large bank, where an employee has plugged an USB device which was not authorised into an unpatched computer inadvertently as a result this action introduced the Conficker worm into the network of the bank. This action caused for several days very serious business disruption. In terms of financial loss, this breach cost several hundred thousand pounds for cleaning up the infection and took many man-months of effort. After this breach, the employee was disciplined as a responsible by the bank. The bank took further action by conducting extra training for its staff on security risks. Moreover, the bank took further actions by enhancing the technical systems configuration, and introduced a real-time monitoring system to avoid such breaches in the future.

- In correlation to systems failure and data corruption, a combination of a lack of staff awareness, poorly designed configuration and process failures, allowed a staff member at medium sized technology company to delete sensitive data from a critical system. This mistake took about a month of work to restore the system and to solve the problem. After this problem, the company took action by changing its procedures, configuration of its systems and its backup in addition to its contingency plans.

- Another story involves outsiders in which these criminals targeted staff members working at a very large financial services provider. The criminals were sending emails to the staff members which appearing like from people they knew but containing links two malicious software. While this ‘spear phishing’ attack did not cause that much financial or reputational loss, it highlighted that staff members were

not aware of security risks. To avoid future similar incidents, staff received additional training.

Likewise, other examples of staff related breaches have also been reported in the information security breaches survey conducted by PwC in 2014 that include the following:

- A member of staff at an educational institution in London overlooked standard data handling procedure and this led to confidential information being leaked online. This incident was brought to light after a third party spotted the data and contacted the institute. The incident caused serious reputational damage and resulted in organisational restructuring, retraining and disciplinary action.
- An employee from a large UK consultancy firm accidentally sent an email containing sensitive personal information to the wrong client. They were only made aware of this error after the unintended recipient responded to the email by a formal complaint. This caused reputational embarrassment to the business and led to a full investigation.
- Similarly, an employee of a large services company in Wales caused unauthorised disclosure of information and breach of the Data Protection Act. This information breach resulted in a week of work and over £50,000 of recovery costs. Additional staff training was provided and amendments were made to security processes and procedures afterwards.

The aforementioned examples were mentioned in the 2013 and 2014 PwC information security breaches survey. Similarly, the next examples have also been reported in the PwC (2015) information security breaches survey:

- With regards to unauthorised access and use of data, a staff member in a large consultancy company obtained sensitive customer data and used it for business development purposes without obtaining the required permission. As a result of this breach, the company's reputation was damaged, resulting in the involvement of the legal adviser and a loss of more than £ 500,000. After the breach, the company provided targeted security training for its staff.
- Regarding the malware infection due to downloading files from untrusted sources, a staff member in a medium sized technology company caused a malware infection after downloading files from a peer-to-peer file-sharing website on a company laptop. This breach had a serious impact on business processes and took more than a week to recover. Moreover, it caused a loss of more than £100,000 as a result of this incident and more than £250,000 was also spent on addressing the breach.
- In connection with the theft of confidential information, a staff member of an IT from a large utilities company stole confidential information valued at more than £500,000. This breach has seriously affected business operations and has damaged the reputation of the company. The incident took between a week and a month to restore business operations, costing £100,000 to £24,999 to respond to the incident, and resulted in a loss of revenue between £100,000 and £249,999.
- With regards to the unauthorised disclosure of confidential information, improper staff behaviour at a large financial services company caused disclosure of confidential information without authorisation. This breach took more than 5 weeks to resolve the incident and return the operations to normal. After the breach, the company carried out additional staff training to address the security issues identified.

The aforementioned security breaches are among traditional issues that have long been known. However, with the development of technology and the changing nature of the threats such as Ransomware, new types of security breaches caused by staff are emerging. This is due to the lack of security awareness regarding evolving security threats.

An example of these security breaches is illustrated below which have been reported in the DCMS (2017) Cyber security breaches survey:

- In a large civil engineering company, the IT department issued advice to warn staff not to map network drives to their local laptops. One of the heads of departments and another senior manager ignored this advice and later unintentionally downloaded a ransomware virus to a local laptop with the mapped network drive. The attack was not aimed to obtain any specific data, but was just to extract money from the company. The mapping allowed the virus to spread across the entire server, rather than simply isolating it into a single device.

2.2.2 Humans Are the Weakest Link in Information Security Chain

While information systems are considered recently as a key to all organisations in order to survive, because these systems are mainly used to hold the value of organisational data resources (Ifinedo, 2009; Ifinedo, 2012). At the same time, the security landscape associated with the use of these systems is also changing continuously. With the movement and the increasing number of security threats, the information security solutions of today would be unable to solve the problems of tomorrow (ENISA, 2010). In order to safeguard these valuable assets, organisations employ a wide variety of tools and measures including anti-virus software, installing firewalls, using back-up systems, tightening control to access information using data encryption technologies,

and using monitoring systems (Ryan, 2004; Workman et al., 2008; Ifinedo, 2012). However, all these mentioned tools and measures are only covering the technical part of the problem and often not adequate in terms of providing a total protection to the information systems of the organisation (Sasse et al., 2001; Stanton et al., 2005; Herath and Rao, 2009; Ifinedo, 2012).

A number of researchers including (Vroom and Von Solms, 2004; Stanton et al., 2005); (Pahnila et al., 2007; Ifinedo, 2012), accentuated that organisations that take care of every aspect of technical and non-technical domains to protect its assets are more probably to be successful in terms of their efforts to protect their main assets. Thus, the onus is on organisations to take advantage of multi-perspective approach to safeguard their information systems assets and resources. In addition, a number of other researchers including (Vroom and Von Solms, 2004; Stanton et al., 2005; Pahnila et al., 2007; Ifinedo, 2012; Bulgurcu et al., 2010) have made clear that the social organisational imperatives are considered equally important for organisations with their needs to protect their assets and resources of information systems.

The human factor in any information security framework is the weakest link and the lack of awareness among staff reduces the strength of the first line of defence. Moreover, reducing the number of information security breaches effectively can be achieved by increasing the user awareness or organisational culture (ENISA, 2010). Therefore awareness and behaviour among all types of users are needful and important parts of information security performance of any organisation (Albrechtsen and Hovden, 2010).

It has been reported that one of the key elements that contribute to security incidents and breaches occurring continuously, is that the staff of the organisations are the

weakest link in ensuring security and also the root cause of problems in some of the most sophisticated technological implementations due to the lack of awareness and experience; they also pose a threat to their organisations from inside, and this is in addition to the vulnerabilities of people that can be exploited by the considerable outside threats (Vroom and Von Solms, 2004; Stanton et al., 2005; Wulgaert, 2005; Ifinedo, 2012; Voss, 2001; Bulgurcu et al., 2010; Shaw et al., 2009). For example, a study conducted to evaluate the trade-offs between computer security protection and accessibility concluded that employees are more likely to bypass security measures in order to complete a task (Ifinedo, 2012). Considering this conclusion, it would be very useful for organisations to focus on the intentions and behaviours of their employees.

Today, information security responsibility is an issue belonging to everyone and not only task management or information security department. Therefore, any information security framework needs to be a very important part of the business. All staff, functions and businesses projects, and relevant elements have a role to play (Ernst and Young, 2012).

2.3 Security Awareness, Training and Education

In order for an IT security program to be successful, it must contain the following elements:

- Development of information technology security policy based on business needs with an emphasis that this security policy can deal with known risks.
- Informing users of their security responsibilities in the use of IT systems as outlined in the agency security policy and procedures.
- Establishing a practice method to monitor and review the programme as a whole.

Security awareness and training should be focused on the user population of the entire organisation. Management should determine proper frameworks for the implementation of IT security within the organisation. An awareness programme should attempt from the start to raise staff awareness that can be deployed and implemented in wide range of ways and it should be targeted at all levels of the organisation and not exclude top management. The effectiveness of this effort will usually lead the way in making IT security and training programmes effective and is crucial to its long-term success.

An awareness and training programme is crucial, as it is the bridge to deliver information that is needed by both users and managers, in order to perform their jobs. In the case of an IT security programme, security awareness and training is the bridge used to communicate security requirements across the enterprise.

The key element to make IT security awareness and training programme effective is that it should clearly explain the proper rules of behaviour for the use of information and the IT systems of the agency. Moreover, the programme should communicate IT security policies and procedures that should be followed. This must be before placing any sanctions imposed as a result of non-compliance with security rules as users should be knowledgeable of the expectations. Accountability must be accounted based upon the fact that the workforce is fully informed, well-trained, and aware. The following part describes the relationship between awareness, training, and education – the awareness-training-education continuum (Wilson and Hash, 2003).

2.3.1 Information Technology Security Learning Continuum

It is well known that learning is a continuum, and therefore it begins with awareness, builds up to training, and develops to education. The continuum shown in Figure 3 is

clearly showing the conceptual relationship between awareness, training, and education as defined in NIST Special Publication 800-16 and the aim is to establish clear boundaries between the three approaches of learning.

There is no doubt that the main element that plays key role to make an effective IT security awareness and training program successful is to build it based on the agency IT security policy and IT issue-specific policies. When policies are written clearly and concisely, the awareness and training material will be built on a solid foundation.

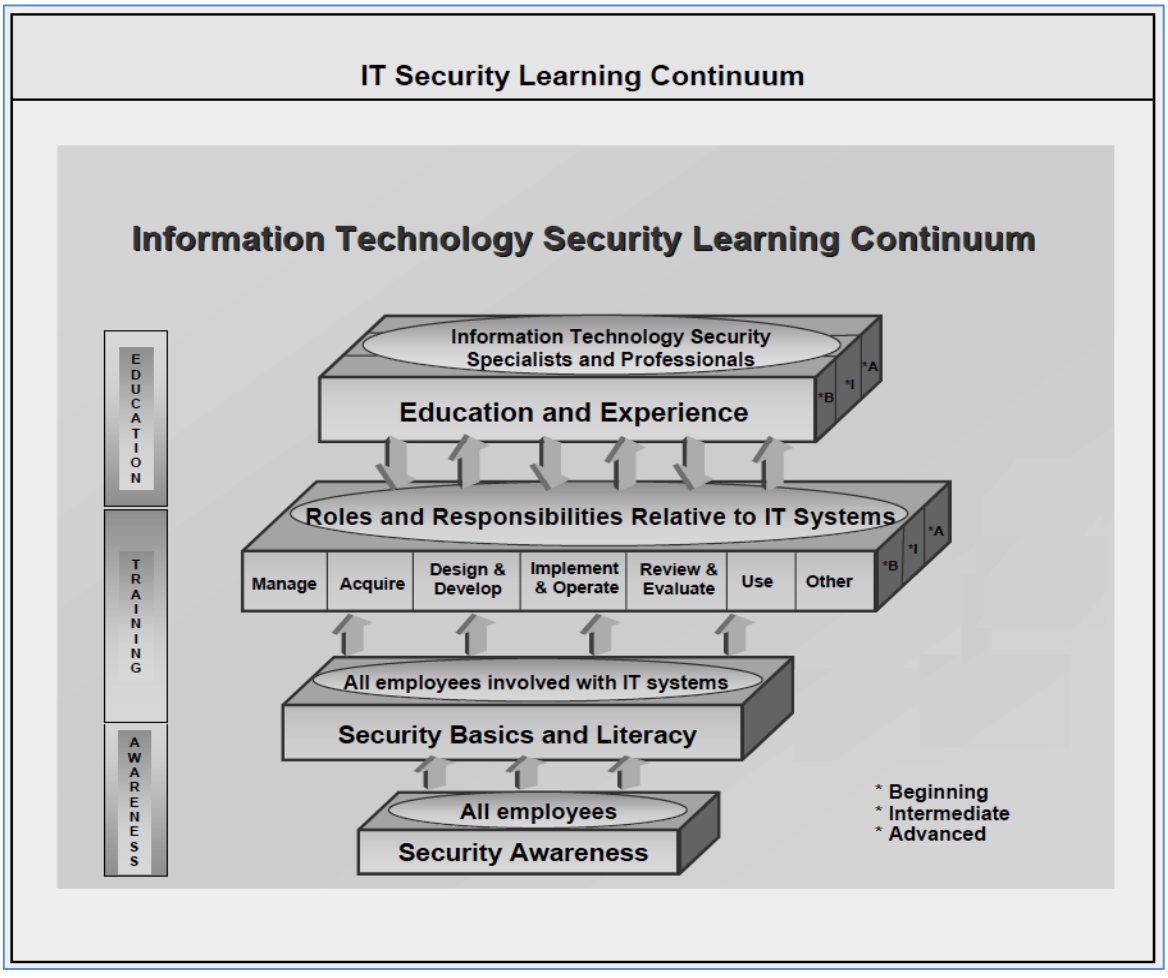

Figure 3: IT security learning continuum (Wilson and Hash, 2003)

The model illustrated in Figure 3 is based on the principle that learning is a continuum. Precisely, learning in this context starts with awareness, builds to training, and evolves into education.

This model is role-based and outlines the IT security learning required by a user within an organisation with different responsibilities with respect to IT systems. The model is also used to determine the knowledge, skills, and abilities required for a user in order to perform the responsibilities of IT security specified to the user roles in the organisation.

The type of learning that staff needs becomes more comprehensive and detailed in the upper part of the continuum. Accordingly, starting from the bottom, all staff need awareness. Whereas Training (represented by two layers namely "Security Basics and Literacy" and "Roles and responsibilities relative to IT systems") is necessary for staff that have a role in the organisation, it refers to the need for special knowledge of security threats, vulnerabilities, and safeguards. The "education and experience" layer relates mainly to staff that have made the IT security their line of work.

The model explains the following concepts:

- "Security awareness" is undoubtedly desired for all staff members, while the "security basics and literacy" is mandatory for all staff members, including contractor staff, who are involved in any way with IT systems. This typically means all staff within the organisation.
- The "Security Basics and Literacy" set is a transitional stage between the "awareness" and "training". This stage delivers the basis knowledge for the following training by providing a comprehensive base of the key terms and concepts of the security field.
- Focus on training comes after the previous stage, where the training stage is to deliver knowledge, skills, and abilities specific to a user's "Roles and Responsibilities Relative to IT Systems". Within the training stage, the levels of

beginner, intermediate and advanced skill requirements can be determined in addition to the differences between these levels.

- The top level is "Education and Experience" which is directed to develop the capability and the vision of the user to carry out complex multi-disciplinary and the skills required to promote the IT security profession and to keep up with threat and technology changes.

As explained previously, learning is a continuum in terms of the levels of knowledge, however gaining or delivering of needed knowledge is not necessary to be followed in sequence. Due to limited resources, organisations need to assess against the continuum of both the range of their IT security training needs and effectiveness of the delivered training. This will enable the organisations to allocate resources for future training to gain a greater value or return on investment (Wilson and Hash, 2003).

2.3.2 Distinction of Awareness, Education and Training

One of the key challenges of examining the information security awareness issue is the spread and the use of different definitions, and perceptions of information security awareness. In this respect, more attention should be paid on how information security awareness is perceived with relation to the neighbouring areas, which are, security training, and education. Despite the fact that a great number of researchers agree on distinguishing between information security awareness, training, and education, a mixture of the terms used still exists. Most of existing definitions conform that the information security awareness is the bottom base of a security-learning pyramid. The goal of information security awareness is to draw attention of all users of information systems to the security message, helping them to understand the importance of information security and the security obligations related to their work, whereas the goal

of training is to build desired knowledge and development required skills and competencies, while the goal of education is creating expertise (Wilson and Hash, 2003; Peltier, 2005; Katsikas, 2000; Tsohou et al., 2008).

2.3.2.1 Awareness

Awareness is the 'what' component of the education strategy of an organisation that is trying to change the behaviour and patterns in how to targeted users are using technology and the Internet and it is a distinct element from training. It consists of a variety of activities that make the users to be the first line of defence of an organisation. This is why awareness-raising activities occur on a continuous basis, using a variety of ways to increase awareness and less formal and shorter than training (ENISA, 2010). Awareness has been defined in many ways as presented in Table 1.

Table 1: Different Definitions for Security Awareness

Source	Definitions
(Wilson and Hash, 2003)	Awareness is not training. The purpose of awareness presentations is simply to focus attention on security. Awareness presentations are intended to allow individuals to recognize IT security concerns and respond accordingly. In awareness activities, the learner is the recipient of information, whereas the learner in a training environment has a more active role. Awareness relies on reaching broad audiences with attractive packaging techniques. Training is more formal, having a goal of building knowledge and skills to facilitate the job performance.
(ENISA, 2010)	Awareness is an on-going process of learning that is meaningful to recipients, and delivers measurable benefits to the organisation from lasting behavioural change.
(ISF, 2011)	Security awareness is the extent to which staff understands the importance of information security, the level of security required by the organisation and their individual security responsibilities.

(Siponen, 2000)	The term information security awareness is used to refer to a state where users in an organisation are aware of –ideally committed to - their security mission (often expressed in end-user security guidelines).
(Bulgurcu et al., 2010)	Information security awareness (ISA) is defined as an employee's general knowledge about information security and his cognizance of the ISP of his organisation.
(Peltier, 2005)	Awareness, which is used to stimulate, motivate, and remind the audience what is expected of them.

2.3.2.2 Training

Training is one of the 'how' components to implement security. A training program should be designed and developed based on the learning objectives set by the organisation. Therefore, the training aims to teach skills that allow a user to accomplish a specific task or function, whereas awareness aims to focus the attention of the individual on an issue or set of issues. The skills gained during training are built upon the awareness foundation, in particular upon the security basics (ENISA, 2010). Training has been defined in many ways as presented in Table 2.

Table 2: Different Definitions for Training

Source	Definitions
(Wilson and Hash, 2003)	The 'Training' level of the learning continuum strives to produce relevant and needed security skills and competencies by practitioners of functional specialties other than IT security (e.g., management, systems design and development, acquisition, auditing).
(ENISA, 2010)	Training is one of the 'how' components to implement security. A training program should be designed and developed based on the learning objectives set by the organisation. Therefore, the training aims to teach skills that allow a user to accomplish a specific task or function, whereas awareness aims to focus the attention of the individual on an issue or set of issues. The skills gained during training are built upon the awareness foundation, in particular upon the security basics.
(Peltier, 2005)	Training, the process that teaches a skill or the use of a required tool.

2.3.2.3 Education

Education is top level of knowledge and skills which is directed to develop the capability and the vision of users to carry out complex multi-disciplinary and the skills required to promote the IT security profession and to keep up with threat and technology changes (Wilson and Hash, 2003). Education has been defined in many ways as presented in Table 3.

Table 3: Different Definitions for Education

Source	Definitions
(Wilson and Hash, 2003)	The 'Education' level integrates all of the security skills and competencies of the various functional specialties into a common body of knowledge, adds a multidisciplinary study of concepts, issues, and principles (technological and social), and strives to produce IT security specialists and professionals capable of vision and pro-active response.
(Peltier, 2005)	Education is the specialized, in-depth schooling required to support the tools or as a career development process.

2.4 Importance of Information Security Awareness

Organisations, whether private or public store information and are making more information available electronically, the trend is on the rise. There is a large increase in terms of dependency on information technology systems. This is connected with a remarkable increase in the use of Internet services. This has become an increasingly important part of doing business all over the world. The absence of the internet can be detrimental to an organisation's business objectives.

The wide and increased use of information technology systems for storing, exchanging, and processing information has made the security and safety of these systems more important and more challenging than ever before. One of the key undertakings for any

organisation is to ensure that its staff acts in an appropriate manner by increasing their IT security awareness to avoid security breaches (Kessel, 2012).

The information security awareness is a key element within industry good practice for security. Some of the distinct international standards including BS ISO/IEC 27002:2013, BS ISO/IEC 27001:2013 refer to this as a key requirement.

The European Network and Information Security Agency (ENISA) has pointed out in its report 2007 some of key factors contribute to increased focus on information security awareness which including the following factors (ENISA, 2007):

- Business requirements are changing, as the use of technology is continuously evolving;
- For the regulatory aspect, there are foreign regulators such as the United States and Singapore which expecting staff to receive awareness training;
- Focus on the security from regulatory bodies within the Member States of the European Union is on the rise. For instance, the Information Commissioner's comments to UK Chief Executive Officers on “unacceptable privacy breaches”;
- The threats from organized crime are on the increase. A recently released report on Internet security pointed out those high levels of malicious activity online, with increases in phishing, spam, networks "bots", Trojans, and zero-day threats. In the past, these were usually well known threats and can be processed separately. Attackers are now using more sophisticated methods, so the attacks tend to involve several vectors. They are also promoting their assets to create global networks that support coordinated criminal activity;

- Customers are more sensitive to security issues than they were in the past. For instance, a reputation of an organisation can be significantly impacted by adverse press coverage;
- Identity theft is a security issue becoming more common. Organisations that deal with storing information and managing personal identity must take care to ensure the confidentiality and integrity of these data. Any compromise leads to personal identity data leakage can cause loss of public confidence, legal liability, and / or costly litigation.
- Given these motivations, it is not a surprise that four-fifths of respondents have rated information security as a high or very high priority for senior management. This is comparable to the rate observed in other security surveys recently.

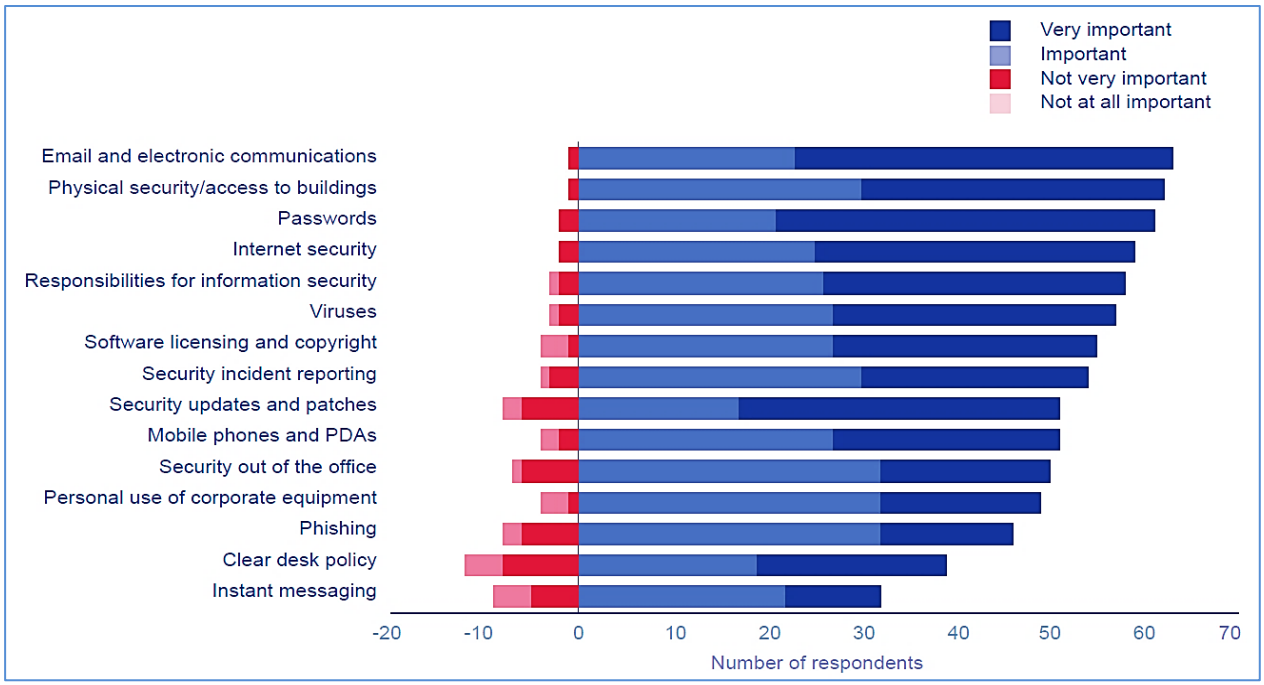

Figure 4: The importance of ensuring staff security awareness (ENISA, 2007)

From Figure 4, in overall, the majority of respondents agree that the four issues are very important for staff to understand:

- Email and electronic communications;
- Physical security/access to buildings;
- Passwords;
- Internet security.

For each of these issues, more than half of the respondents rated them as very important; almost nine-tenths rated them as very important or important.

2.4.1 The Increased Need for Security Awareness

Users must have some level of security awareness and ability to protect themselves, as there is a large number of threats which make it harder for technology to give a complete answer and threats exist are differ in many contexts to be able to rely upon a system administrator. However, recently, many users find themselves not quite well equipped to operate.

Moreover, as technology advances, there has been a significant and continuing shift in terms of responsibility and duty. This has made the need for acquiring security awareness an imperative matter in order to increase the security of the whole system. Unfortunately, more attention has been paid towards different types of security controls such as firewalls, IDS or other types of security controls that represent the technology-oriented safeguards comparing to awareness and training of users. It is not questionable that these investments are important, however, such investments are representing a part of the picture, but these investments are often easier to justify, based on targeting a defined threat whose impact can be measured easily. Users must have some level of security awareness and ability to protect themselves as there is a large number of threats making it harder for technology to give a complete answer.

There are still many users who have a lack of understanding about the technology and therefore find it harder to ascertain the associated threats (Furnell and Clarke, 2012).

Additionally, Ernst & Young's survey in 2012 indicated that there are some key trends in terms of speed and complexity of change that are occurring too quickly of which contribute to increase the need for security awareness because of the following reasons:

- Virtualization, cloud computing, social media, mobile, and other new and evolving technologies open the door to a wide number of internal and external threats.
- Emerging markets, the continued economic change and increasing regulatory requirements are all contribute to add more complexity to the information security environment that already is complicated.
- Organisations have made great strides in improving their information security capabilities. However, for as many steps as they have taken, they continue to fall behind, creating an information security gap that grows ever larger.

Despite the fact that there are many steps have been taken by organisations in terms of improving their information security capabilities, they continue to fall behind, which contributed to increase an information security gap, which grows larger than ever (Ernst and Young, 2012).

2.4.2 The Fast Evolving Threats

Although organisations are making improvements to foster their information security systems, however, the changing speed and the challenge in this field are also growing. In this regard, in 2009, 41% of respondents realised that the number of external attacks has increased. Within the year 2011, the number of respondents who realised the

occurrence of the external attacks jumped to 72%. In the year 2012, the number of respondents who indicated that these attacks will be increased has again risen to 77%. Examples of such external threats include hacking, state-sponsored espionage, organised crime, and terrorism.

In the same period of time, organisations have realised an increase in the number of internal vulnerabilities. In the Ernst and Young (2012), the Global Information Security Survey, 46% of respondents said that they have realised an increase. 37% of respondents ranked unaware or careless staff as the threat that has increased the most during the past 12 months. Interestingly, this number is not much less than that referred to in the year 2008, relatively, where 50% of respondents in 2008 cited that awareness within the organisation is the most challenging issue to deliver information security initiatives successfully.

2.4.3 Key Obstacles to Information Security Effectiveness

There is no single issue responsible for creating a gap between where information security currently is and where it needs to be. The gap exists because of a result of a wide range of issues related to people, process, and technology. Over the years, Ernst & Young's surveys GISS have consistently sought to recall key obstacles to information security effectiveness. The obstacles discussed below were cited in Ernst & Young's 2012 and 2017 surveys and are considered to be important up to the present time to explore as the following:

2.4.3.1 Lack of Resources and Skills

This could be understandable, especially in today's era of economic changes and spending controls. Where there is a lot of tasks required achievement and resources available are not sufficient. However, the lack of resources explains only part of the

picture. Information security needs many requirements that do not include only more resources, but indeed needs other requirements, including people with good skills and good training to meet the rapidly evolving changes in the information security landscape.

2.4.3.2 Resource Constraints

With regards to this issue, Ernst & Young's survey 2012 indicated that only 22% of respondents said that they are planning to increase spending in this area during the next 12 months. When organisations were asked about the main barriers and obstacles that challenge the ability and function to deliver information security, 43% of respondents claimed a lack of skilled resources. There is no doubt that this figure is linked to the only factor which relates to spending constraints.

According to Ernst and Young (2016), resource constraints are consistently perceived as one of the main obstacles or reasons that challenge the Information Security contribution to organisations. Although recent years, between 2013 and 2016, have witnessed an increase in the budget. For example, in 2016, 53% of respondents stated an increase in their budget over the last 12 months, compared with 43% in 2013. Likewise, 55% of respondents in 2016 expected an increase over the next 12 months, compared with 50% in 2013. However, organisations reported that more funding is needed, with 61% of respondents stating that the budget constraints is a challenge, while 69% of respondents stated they need an additional budget of up to 50%. While the additional budget may help to mitigate the effects of the skills shortage, it is not just an additional budget that is required, but also, more importantly, the executives support on this issue. According to the Ernst & Young Survey (2016), 32% of respondents believed that there is a lack of executive awareness and support challenging the effectiveness of cybersecurity. Figure 5 presents the main obstacles or reasons that

challenge the Information Security contribution and value to the organisations (Ernst and Young, 2016).

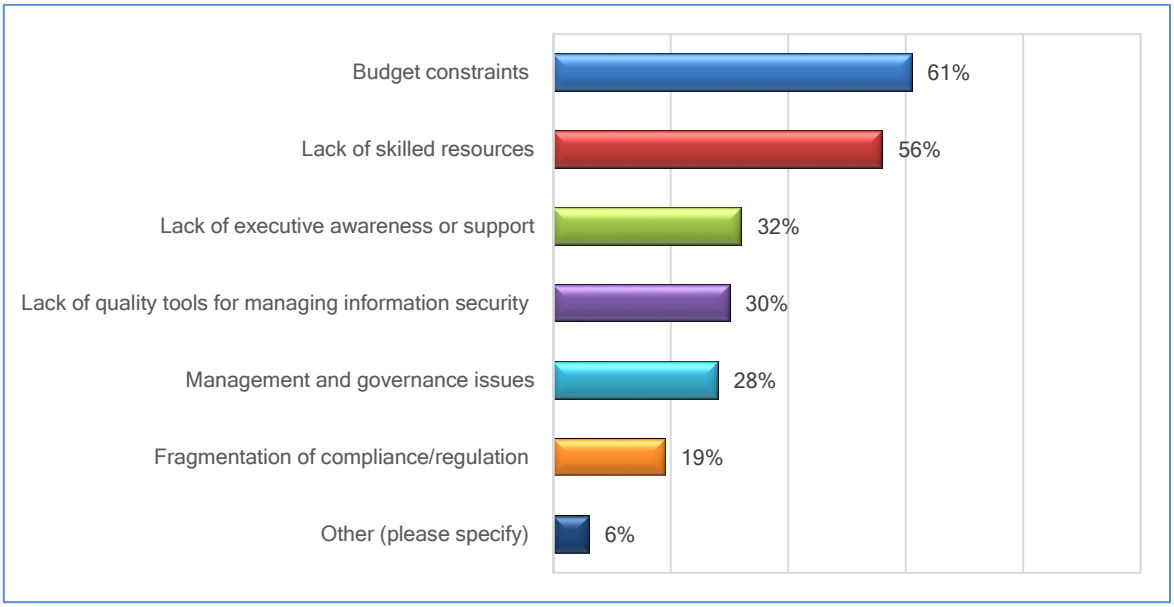

Figure 5: Main obstacles to Information Security (Ernst & Young, 2016)

2.4.3.3 Limited Security Awareness Training

Organisations need to train staff outside of the information security function on the role that staff must play in keeping the organisation's information safe. Finding the right skilled resources in information security is only one part of the picture. Due to the fast change of external threats, as well as the spread use of mobile devices and networks that are used for both work and play, organisations need also to allocate the resources and money to train staff from outside of the information security function on the role that they must play in keeping the information of their organisation safe (Ernst and Young, 2012).

With regards to the limited security awareness issue, the Ernst & Young (2016) survey reported that neglected or unaware employees are still posing increasing risks. For example, 73% of the respondents are concerned about the lack of user awareness and behaviour associated with the growing use of mobile devices. This exposes them to

risks associated with the loss of such device, the potential loss of information and the potential of identity breach. Figure 6 presents the main risks associated with the growing use of mobile devices for organisations (Ernst and Young, 2016).

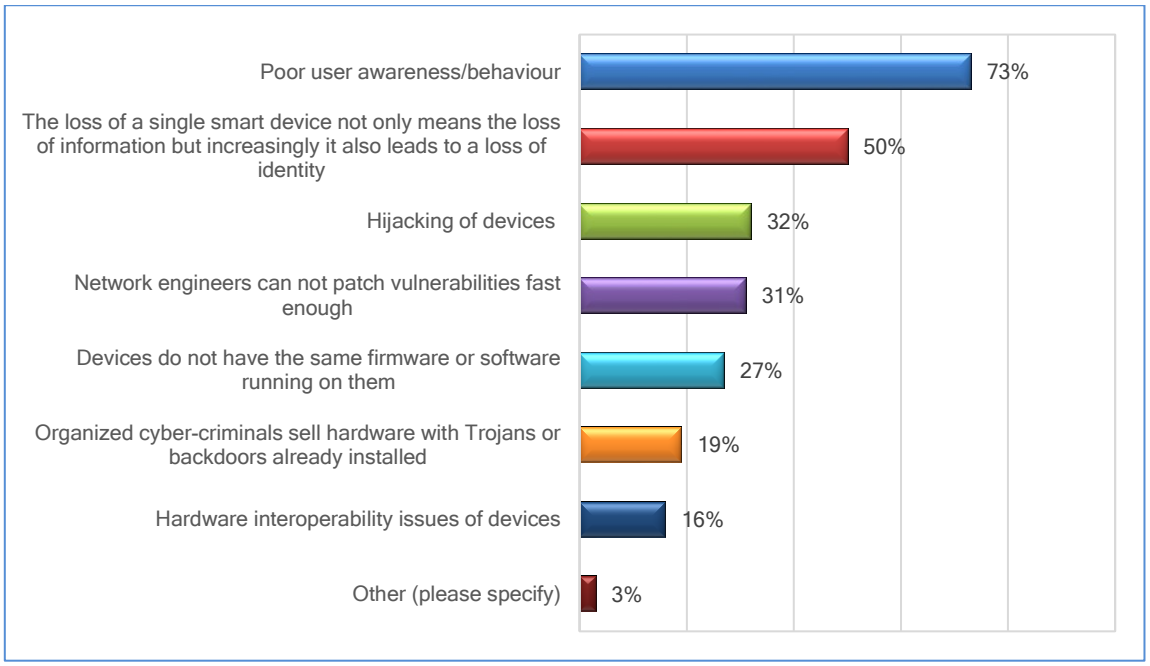

Figure 6: Main risks of growing use of mobile devices (Ernst & Young, 2016)

Based on the figures mentioned above, it is not surprising that the surveyed organisations are planning to spend more on security awareness and training. This is somewhat reflected in the spending budgetary priorities of the organisations. For example, with regards to the areas where organisations chose to put their budgets, according to the Ernst and Young (2016), 49% of these organisations stated that they were planning to spend more on security awareness and training, while 43% declared they would spend the same.

This is probably due to increased awareness among organisations regarding the importance of the security awareness and training which should be perceived as important as other security components of the IT system. This should contribute to address the continued issue of the lack of security awareness and training, reduce the

risks associated with the poor user awareness and behaviour and enhance the entire security of the IT system.

2.5 Current Methods of Security Awareness Raising

A formal security policy is the basis for any framework for information security awareness. Enforcing a good behaviour is very difficult without existence of a clear idea about the 'law' covering the use of information and systems.

The existence of good practice standards can position a strong emphasis on the existence of a security policy across an organisation. For instance, BS ISO/IEC 27002:2013 referrers to implementing training and awareness programmes within the organisations. There is a requirement of management to ensure that the people who are working for them are implementing and applying security with accordance to security policies. To accomplish this, they are required to provide training in proper awareness training and regular updates in organisational policies and procedures, related to the job function for all staff in the organisation and where appropriate contractors and third party users.

Additionally, BS ISO/IEC 27002:2013 standards refers and suggest that the company's security policy could be communicated to employees and relevant external parties in a form that is relevant, accessible and understandable to the intended reader, for instance in the context of an information security awareness, education and training programme (BSI, 2013).

A main element of any policy and information security awareness training is to look at the threats and risks facing the business. This analysis should be paid to areas that the policy and training need to cover.

Organisations are facing big challenges in terms of the changing environments, threats, and risks. In order to be effective, awareness-raising initiatives need to be supported by the senior management of the organisation. Ideally, this should be supported by the board or executive-level, in order to promote the importance of the issue with the staff. If senior management does not treat security awareness as an important and key issue in terms of protecting and safeguarding the organisations assets, it is unlikely that the training will be successful.

Most of the well-known standards including BS ISO/IEC 27002:2013, BS ISO/IEC 27001:2013, and the 2011 Standard of Good Practice for Information Security recommend that there is a need for a formal approach to information security awareness. This need to be achieved through three procedures including:

- **Requirements Analysis:** Management need to determine what topics staff needs to understand. Users should be aware of the parts of the security policy that is relevant to the nature of their work. Several standards including BS ISO/IEC 27001:2013, BS ISO/IEC 27002:2013 pointed out to look at issues such as spyware, virus, and choosing strong passwords.
- **Orienting Training Based on The Role:** Contractors and staff are both should to be trained, appropriately oriented towards the roles that they play in their working environment to help them achieve their work appropriately. Additionally, they should also be updated regularly with any relevant changes to security policies or procedures. Training needs to address how staff can implement security procedures in their day-to-day duties this has been referred by standards including BS ISO/IEC 27001:2013, BS ISO/IEC 27002:2013 and the 2011 Standard of Good Practice for Information Security.

- **On-Going Review:** The content of awareness programmes should be reconsidered and reviewed on periodic basis. The awareness programme on the intended participants should be reviewed regularly in terms of its effectiveness. And any suitable changes that take place in the original security policy should also be taking a place in corresponding information security awareness training programmes this has been referred by standards such as BS ISO/IEC 27002:2013 and the 2011 Standard of Good Practice for Information Security (ISF, 2011).

Based on the results obtained from information security breaches survey ENISA pointed out that:

- The vast majority of companies have taken some steps to make staff aware of their security responsibilities. Companies also make greater efforts to educate its staff than it was in the past. Most of the large companies included security responsibilities in their staff handbook and training new staff in the field of security;
- Almost every company that has a security policy has taken steps to educate staff about their security responsibilities;
- There is a strong correlation between the priority that given to information security by the senior management and the possibility that the staff will be trained, where the high priority is given to the importance of information security by senior management, the more likely is that the company to take steps to educate its staff. An example is that for those seen security as is not a priority at all, only half of them have taken steps to raise awareness.

The study conducted by PwC 2007 survey shows a steady trend. All the respondents use some techniques to make their staff aware of their security responsibilities.

As with much else in business, the presence of an approved budget is a main key to achieve effective awareness programme. It needed both time from staff and money to build appropriate materials. This is an investment in the future of business, and should be approved by senior management.

Although the security has been given a high priority, many respondents find it difficult to justify spending significantly on awareness programmes. There were only a third of respondents built a formal business case in order to justify this expenditure, and only half of these attempted to measure the benefits that their awareness programmes will achieve and there were very few of them assessed the return on investment. Only 15% of respondents have measured the benefits of their programme even though they do not prepare a formal business case.

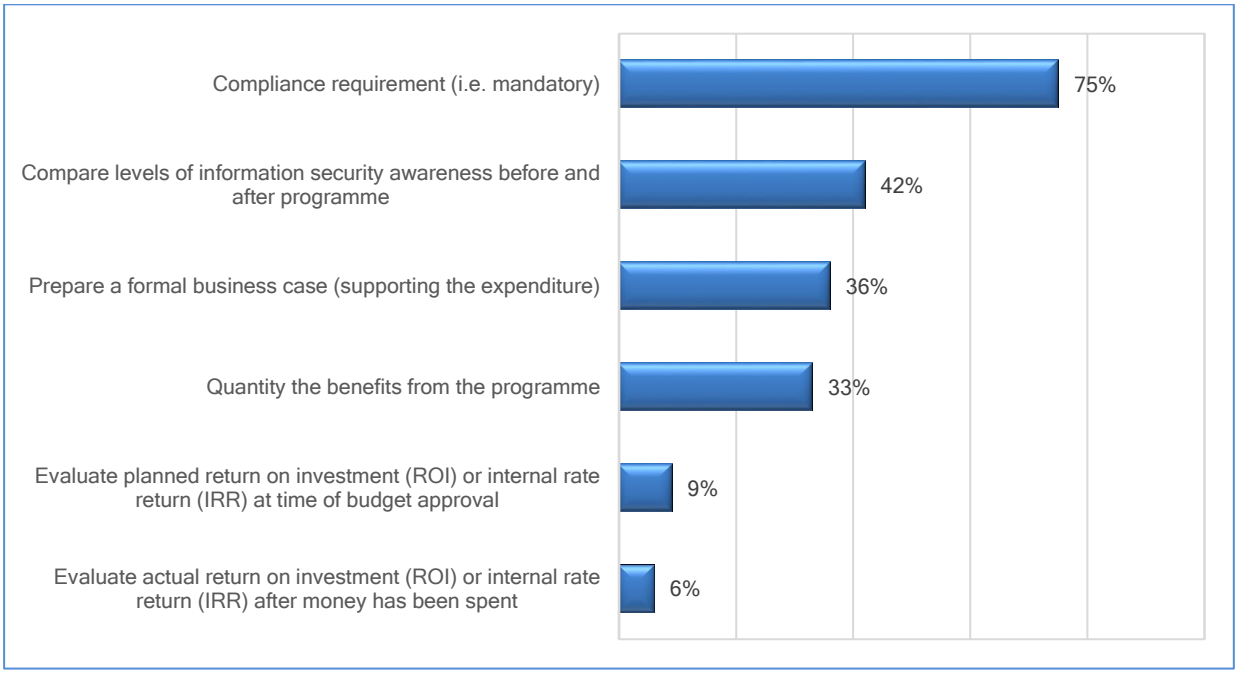

Figure 7: Justifications of the cost of awareness programmes (ENISA, 2007)

As presented in Figure 7, most respondents are seeing that the training in security awareness is something that they just have to do, i.e. it is only as a response to compliance. Based on that, it is dealing with security awareness in their budget as an

issue of overhead rather than as an investment. This is interesting, since the regulations in most of the Member States of the European Union do not require special training to information security. It appears that data protection laws in the European Union are driving the increase in awareness training.

About two-fifths of the respondents justify the programme by comparing the levels of awareness about information security before and after the program. The vast majority of respondents conclude that the benefits of improved security awareness are often not noticeable and measurable. People have difficulty in terms of defining good metrics for behaviours. Without reliable metrics to measure the change, the effort to work out the return on investment outweighs the benefits. On the other side, though, as metrics improve more organisations should take into account to prepare formal business cases.

Once the extent of information security awareness programme has been determined, the next step is to develop a communications plan. This requires analysis of the audience and determining which techniques are the most suitable to use. Slightly less than half of the respondents done this in a formal way and most just get on with the task at hand.

There are wide ranges available of awareness raising techniques. Most of the respondents use multiple techniques. Companies that give low priority to the security of information take the least number of steps to make staff aware of the security issues. Their desire is strong to reduce the costs to a minimum.

There seems to be some of the specific basic controls that should be existed in every organisation. The vast majority of respondent identified security policies as shown in Figure 8, both in staff handbook or a separate security policy. There were 85% of respondents have established an intranet site that provides guidance to staff on

information security issues. These techniques are low-cost, so this encourages organisations to use them.

However, many of the respondents believe that techniques, including policies, handbooks, and guidance alone are not an effective way to improve awareness as shown in Figure 9. It is simply unrealistic to expect most of the staff to read and understand all the information addressed to them with regard to information security. These techniques play a useful role in terms of supporting and promoting awareness activities. However, they are not alone the only effective way to change the behaviour of the staff.

Respondents found that the training in the classroom is the most effective technique with respect to changing the way how people behave. There was a number of 72% of those surveyed that have used security messages in induction training for new staff. This ensures delivery of the message to the highest risk people (staff newly joined the organisation) and relatively low cost, where security aspects can be combined in the existing events.

While classroom training is believed to be highly effective, relatively small number of respondents conducts continuous training for existing staff. This could be due to the associated cost to arrange and run these courses. Moreover, it appears that the time to cover training in a continuous manner is also another fact affecting the lack of conducting continuous training. It seems to be the most effective awareness programmes are those that fit the perceived budget for classroom training target those amongst the organisation staff who are having lack in terms of security awareness level and hence may jeopardize the organisation. It seems that the blanket classroom training is unlikely to be cost-effective.

Instead, half of respondents have used CBT (Computer Based Training), and two thirds of these have conducted CBT for all staff. It is agreed that the CBT is a cost effective in terms of investment, the reason beyond this is perhaps that the CBT when it started running the delivery costs are very low. Therefore, it assists well in terms of continuing training to a large number of existing users. In terms of consistency of delivery, the large classroom training programmes are usually better. The main benefit of using the CBT is that is also allow building tests into it in order to be used as a measure of how well recipients have understood and get benefits of the training process.

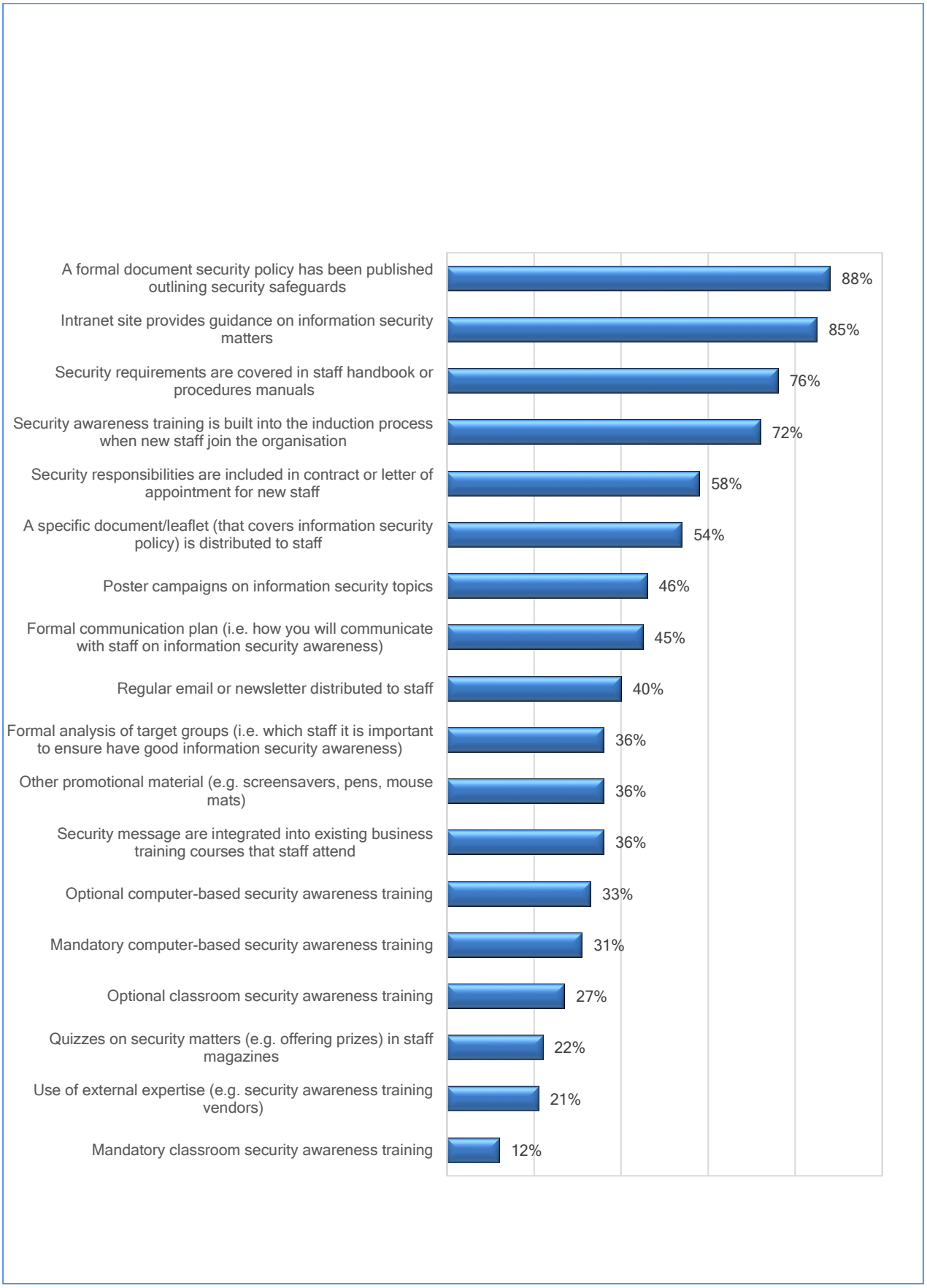

Figure 8: Techniques to raise staff security awareness (ENISA, 2007)

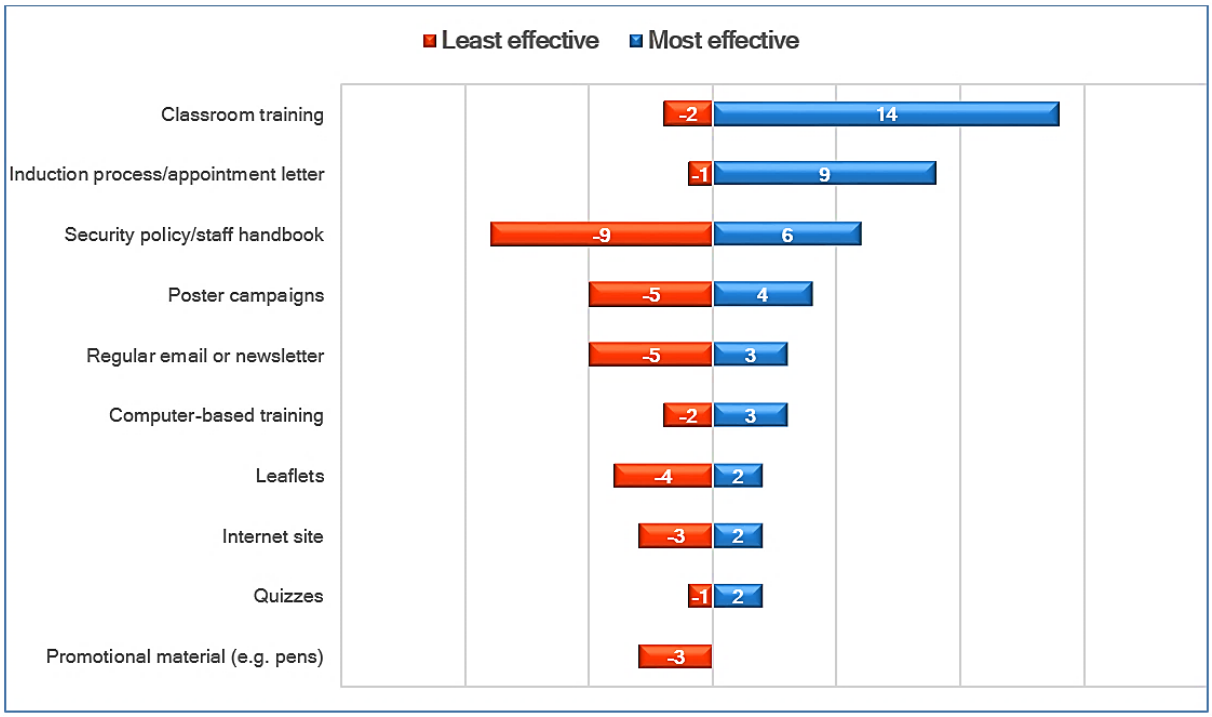

Figure 9: The effectiveness of techniques to raise security awareness (ENISA, 2007)

The main key to run an effective programme is to deliver the right messages to the right people. This includes understanding the current information security issues of each group and the degree to which they are aware. Unexpectedly, only 36% of respondents have a formal mechanism to do so. This happens more often in financial services than in other sectors. Many financial service providers learned that it is possible to spend large amounts of money on random awareness activities without having a significant impact on the overall risk. They now use a combination of blanket coverage of the basic disciplines and additional activity targeting areas of greatest risk that they may face.

Poster campaigns, promotional items (such as pens) and blanket e-mail messages are all used by a large number of participants. There were many respondents using these techniques in the past but now disused or reduced their use. They have a relatively short shelf life and can be expensive to distribute throughout the organisation. There are also limits to the amount of information that can be transmitted to the reader, and many people simply ignore them completely.

There is no doubt that there is a real need to increase the security awareness for the users; however, passive promotion, such as using posters up around the office or PowerPoint slides, do little to capture the interest of the users (Randell, 2013). The biggest threats to information security in any organisation is often not related to the presence of weakness in the technology control environment, and it is more related to the action or inaction by employees which can often lead to security incidents (PCI, 2014).

One out of every five respondents uses surveys and quizzes to foster interest and increase awareness. Of those that have tried them in the past, more respondents found that using these techniques is actually more effective than not using them at all. The appropriate use of these methods can increase the level of awareness and can actually get people to think about their actions and behaviours.

The implementation of the security awareness program successfully can be a hard task. It is likely that there will be some large difficult barriers to overcome along the way. What is most functional in the long term is to be able to recognize any restrictions hinder efforts, such as the lack of motivation of senior management with respect to the issue of information security interest or the existence of cultural resistance within the organisation. Identifying potential obstacles in advance is a key to the potential success of the plans that are developed to overcome these obstacles (ENISA, 2007).

2.6 Conclusions

While the security landscape is changing continuously, the complexity and the nature of the security threats are also changing. Although organisations employ a wide variety of technical tools and measures to safeguard their valuable IT assets, these solutions

are only covering the technical part of the problem and often cannot provide a complete protection, since IT assets are ultimately managed and operated by the human.

Due to the large number of recent security breaches experienced by organisations and caused by their staff either intentionally or unintentionally, it is paramount that users should have an appropriate level of security awareness and ability to protect themselves and their organisations' IT assets. Due to the large number and the changing nature of threats, it becomes difficult for technology solutions alone to provide a complete protection.

Although recent figures indicate that the vast majority of the senior managers recognise the increased high risks of cyber insecurity and consider security as a high priority, reflecting an increased need for security awareness, organisations are still not addressing the security threats appropriately. For instance, the root cause of the most disruptive security breaches were staff related incidents. However, organisations instead of addressing this problem by providing training to the widest category of the organisation workforce, i.e. staff who are not cyber security or IT specialists, they provide training to the smallest workforce category which are directors or senior management staff. The persistence of this approach will increase the complexity of combating threats in general and more specifically the insider threats posed by trusted insider users.

With the presence of obstacles to information security effectiveness and the use of current methods of security awareness raising, in addition to the barriers to training such as, irregular training or non-mandatory training which could easily be forgotten, costly and logistically complex face-to-face training sessions and the inability of some users to realise the value of training, the adoption of more targeted security awareness

approach to address these issues become imperative. Targeted security awareness raising is considered to be the most suitable candidate to address these concerns by providing guidance and nudges during the task in hand.

Chapter 3

Review of Targeted Security Awareness Opportunities

3.1 Introduction

As mentioned in the previous chapter, users are often referred to as the weakest link in the information security chain. This is mainly driven by the key factor that has significant influence, which is the lack of security awareness among users regarding emerging and evolving security threats. Recent stories and case studies as reported in the previous chapter and cited from the most well-known information security breaches surveys, have revealed that users are still unaware of the security threats. The aforementioned staff-related security breaches were among traditional security issues that have been known for a long time as mentioned in the previous chapter. For instance, related to the improper use of email services, visiting fraudulent websites, unauthorised access and disclosure of confidential information and breach of data, malware infection due to downloading files and attachments from untrusted sources, theft of confidential information, and mapping network drives to unprotected local laptops.

As an example, the most recent Ernst and Young security survey (2017) revealed that respondents acknowledged that careless employee behaviours pose a considerable point of weakness for most organisations. The report also underlined that addressing this weakness is indispensable for organisations to stay safe (Ernst and Young, 2017). As such, unaware users can pose additional and considerable risks to their organisations' IT security and can potentially cause security breaches. For example,

this can occur by staff responding to phishing emails, visiting malware infected websites, writing their passwords down or sharing them with others.

In the light of these facts, and in order to transform the weakest link into a crucial frontline defence against cybersecurity threats, and to reinforce them in an information security perspective, many organisations employ IT security awareness programmes. This in turn aims to raise the IT security awareness of their staff to reduce end-users' errors. However, providing awareness is one of the challenges facing many organisations, and one of the most important barriers is that users could easily forget what they have trained for.

Furthermore, there are further and diverse methods employed to support users during daily dealing with IT systems. These include the use of security warnings, passive interventions (such as the green URL bar in the case of active SSL certificates), and active warnings (such as those in the case of self-signed certificates). However, according to Zaaba et al. (2014) and Volkamer et al. (2013), these methods have drawbacks and are perceived to be ineffective in protecting end-users. This was due to many factors, including providing inadequate security guidance and information to users or providing information that is on a very technical level, which is not accessible to novice IT users. As a consequence, novice users may ignore these interventions and may act inappropriately, as well as not being able to recognise the consequences of ignoring these interventions. Furthermore, users learned through their dealings with many low-risk cases in their daily dealings with IT systems that nothing will harm their IT systems if they ignore these warnings (Volkamer et al., 2013). All of the aforementioned factors and figures have made introducing an innovative method to raise the security awareness for the end users an imperative issue.

This chapter primarily discusses and explores the opportunities and potential application of a targeted security awareness-raising approach. It begins with a detailed discussion on the shortcomings in existing security warnings and provides a conceptual background for the targeted security awareness-raising approach. Furthermore, it provides definitions to the neighbouring areas such as context-sensitive security awareness and security nudges to eliminate confusion and differentiate between these concepts. Moreover, this chapter explores various examples of the targeted security awareness approach that is currently being used in a number of well-known applications from prominent software developers. It then provides a broad discussion of the opportunities to increase the security awareness of end-users by taking advantage of targeted awareness-raising opportunities.

3.2 The Shortcomings of Present Security Warnings

One of the recognisable means to make the users aware of any security risks in their daily activities when interacting with IT systems is the use of security warnings. The security warning is used to warn the user about the potential security risks. However, the current security warnings do not seem to be effective and have flaws. Zaaba et al. (2014) identified six common problems related to security warnings including attention towards warnings, understanding of warnings, the use of technical wordings, and evaluation of risk from warnings, user's motivation towards heeding warnings, and user's assessment of implication of warnings. Moreover, regardless of the fact that there are wide varieties of technical countermeasures to mitigate security risks such as malware-related risks, users are in fact the last line of defence against security incidents and indeed users represent the last gate in the decision-making process (Silic and Back, 2017).

Moreover, many user studies and statistics on successful attacks against end-users present that neither passive interventions (such as green URL bar in the case of active SSL certificate) nor active warnings (such as those in the case of self-signed certificates) are effective in protecting end-users. There are several key elements identified by researchers behind this drawback. The key element is that existing interventions do not sufficiently take into account that security is their main objective and instead focus on the user task. The knowledge level of users about IT security is quite often incomplete. For example, many users believe that they are personally not being targeted by security attacks. Studies also show that people tend to make decisions about using a web page based on its design and not on the underlying reliability in terms of security. Broadly, it was observed that these passive security interventions currently used are not observable by most users. Active security interventions interrupt users to perform the task during their work, and therefore cannot be ignored. However, active warnings also may have not been successful for many reasons. One of the problems is that the information provided on the situation and the reason for this intervention is currently on a very technical level. Thus, users are not able to understand the risks and the consequences of ignoring this intervention based on the information provided. One of the most obvious examples that reflect this trend is that many currently used browsers provide the same security interventions in high and in low risk situations. Users learned through their dealings with many low risk cases in their daily lives that nothing "bad" happens if they ignore these interventions. Similarly, because of habitual effects, it would not be surprising that users will also ignore such interventions in high-risk situations (Volkamer et al., 2013).

3.3 Context Awareness and Information Security

Context is the circumstance within which something exists or happens that primarily helps explain and understand it. Context-based computing uses additional contextual information to improve the computing experience at the point of consumption. Applying this to information security frameworks, context-based security is the use of additional information to improve security decisions at the time such decisions are made.

Rapidly changing businesses and threat environments, as well as user demands are stressing static security policy enforcement models. Information security infrastructure must become adaptive by incorporating additional context at the point when a security decision is made. There are already some signs that highlight this transformation. Network security solutions are evolving to incorporate "application awareness" and "identity awareness" into their offerings. Information protection solutions are evolving to deliver "content awareness".

Application, identity, and content awareness are all part of the same underlying shift to incorporate more contextual information at the point when a security policy enforcement decision is made. To enable faster and more-accurate assessments of whether a given action should be allowed or denied, a solution where a real-time context based information at the point when a decision is made, needs to be incorporated (MacDonald, 2010).

3.4 Approaches for Raising Context-Sensitive Awareness

The future of information security is shifting towards being context aware. Today the greatest use of security infrastructure is built upon static-enforcing policies which are defined in advance in an environment where the infrastructures for both IT infrastructure and business relationships are relatively static. This is multi sourced and

virtualized, and where consumer-oriented IT is increasingly used instead of enterprise-owned and provisioned systems (MacDonald, 2010).

As per the findings of (MacDonald, 2010):

- Context aware security is the use of additional information to improve security decision at a time when security decision is made resulting in more accurate security decisions capable of supporting more dynamic business and IT environments.
- Context information that will be relevant to security decisions is not limited to environmental context and will include context information from multiple sources.
- Application awareness and awareness of identity and awareness of the content are all examples of a wider transition to context aware and adaptive security infrastructure.
- Context-aware security will be the only way to securely support the dynamic business and IT infrastructures emerging during the next 10 years.

3.5 Targeted Security Awareness, Context Sensitive Security Awareness and Security Nudges

One of the key challenges of information security is the various different definitions and perceptions of terms used to describe it. In this respect, more attention should be paid to how targeted security awareness is perceived in relation to related areas, namely, context-sensitive security awareness and security nudges. It is clear that the three concepts have similar interests. However, there is a lack of obvious definitions or comparisons of the three terms in the literature. The next section will present definitions of the three concepts.

3.5.1 Targeted Security Awareness

Targeted security awareness involves making people aware about something they need to know about rather than other superfluous information. It mainly focuses on making users aware of the security risk they are facing and before they take any action that could lead to compromising their IT systems. The targeted security awareness approach employs a wide variety of existing security tools and features to support users and help them understand the security risk and take proper actions to safeguard their IT systems when needed without overwhelming them.

3.5.2 Context Sensitive Security Awareness

Context sensitive security awareness, in simple terms, means that the user will get security advice at a time when it is relevant. In this approach, users get advice that is relevant to the task in hand. One of the most obvious examples of the context sensitive security awareness approach is the use of password meters in which users will be warned about the strength of their password whilst attempting to create one.

3.5.3 Security Nudges

It is mainly the impact that the security tools on the users to push them towards making better selection or action. For example, what the security meter does to nudge the user towards making a better password selection.

3.6 Examples for Targeted Security Awareness Raising Approaches

There are some good illustrative examples for targeted security awareness approaches such as the increasing popularity of password strength meters on websites and in operating systems, which provide guidance to users directly at the point when they need it.

Despite the fact that there are some existing examples of the use of targeted security awareness approaches like the use of password strength meters, file download security-warnings, and security warnings when inserting removable devices, the popularization and proliferation of these types of security interventions, which warn and alerts users before making their decisions about security risks are still limited. Some of the apparent and currently used examples of targeted security awareness approach are presented in Figures 10, 11 and 12.

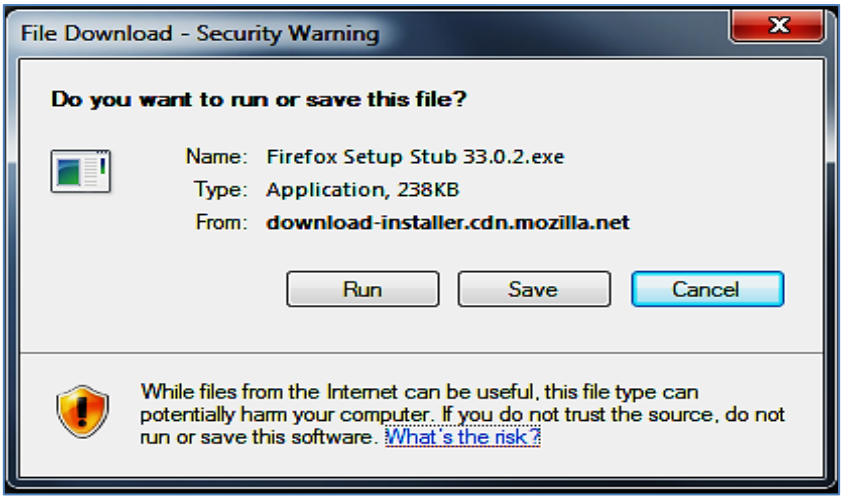

Figure 10: Example for targeted security awareness raising approach

Figure 11: Example for targeted security awareness raising approach

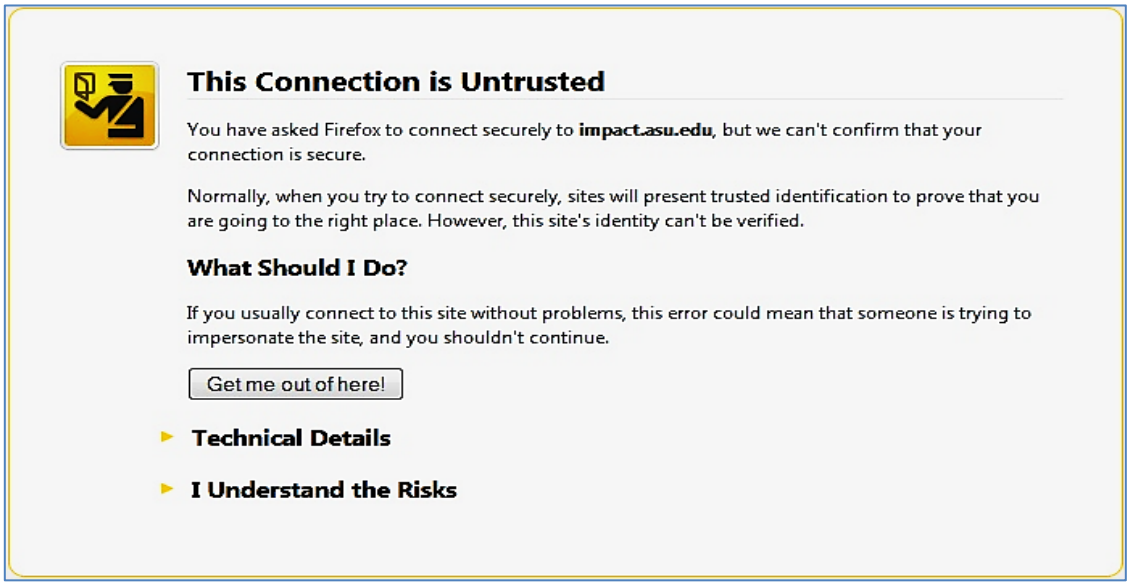

Figure 12: Example for targeted security awareness raising approach

One of the most apparent examples is the use of the security-warning message and trusting a PDF file in Adobe Acrobat and Reader. The screenshot shown in Figure 13 shows a warning message that pops up when a user tries to access a Web site via a link in a PDF file. This is a very apparent example of how to adopt a targeted security awareness-raising approach. In this example, the application warns the user before accessing the site by providing a simple warning message that can be easily understood and does not contain complex technological information that the utmost of non-technical users may not comprehend. The application also provides a Help function with this warning message to access additional information that provides interpretation and an additional explanation. The user will be directed to access a web page after clicking the Help button, the web page contains a full and detailed explanation of the potential threats of visiting sites via links found in PDF files. The link below leads to a page with additional information that a user can access when they click the HELP button:

https://helpx.adobe.com/acrobat/kb/security-warning-trusting-pdf-acrobat.html

This example demonstrates how effective it is to provide security information, recommendations, and explanation to the user about the potential security risk before the user takes any actions that may result in a security breach and consequently compromising the users' device, stolen or damage to their data. This provided feature will potentially be turning a possible victim into an educated user.

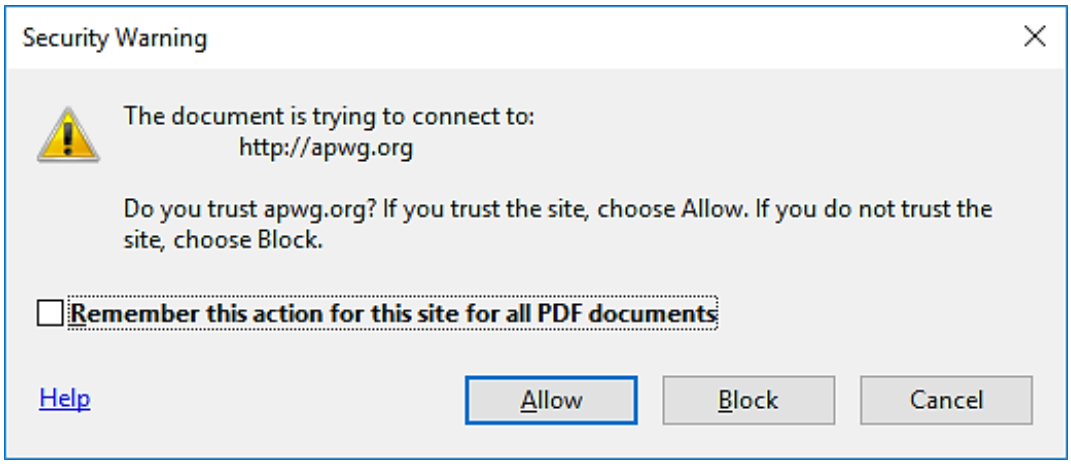

Figure 13: Security warning when the user clicks a link provided in a PDF file

While this example shows that some developers such as Adobe have taken encouraging and concrete steps towards making users aware of the potential security threats before taking any actions that could damage their IT systems, other leading software developers of well-known and widely used applications have not taken similar steps in this direction and failed to provide the same solutions for similar scenarios. For example, when using Microsoft Word (MS Word), users may experience the same scenario exactly when trying to access a website via a link provided in an MS Word file, it will show the user a warning message as shown per screenshot in Figure 14 similar to the warning message provided by the Adobe Acrobat and Reader. However, although the warning message provided by MS Word has provided security information stating that some files can contain viruses and may be harmful to the user's computer and that it is important to be certain that the intended file is from a trustworthy source, this information may confuse the user, because the user may be trying to access a

websites via links provided in MS Word and is not trying to open a file. Furthermore, it also does not provide the user with any possibility of obtaining additional security information or any recommendations or explanations regarding the potential threat. The warning message titled “Microsoft office” which is not reflecting the content of the message as it is a security alert or security message. The title of the pop-up windows in this situation should clearly indicate that this is a security-warning message. Perhaps this inconsistency would also cause confusion to the user. Moreover, this security message is not also using any security signs to attract the attention and make of the user aware of the security threat that the user may encounter because of this action.

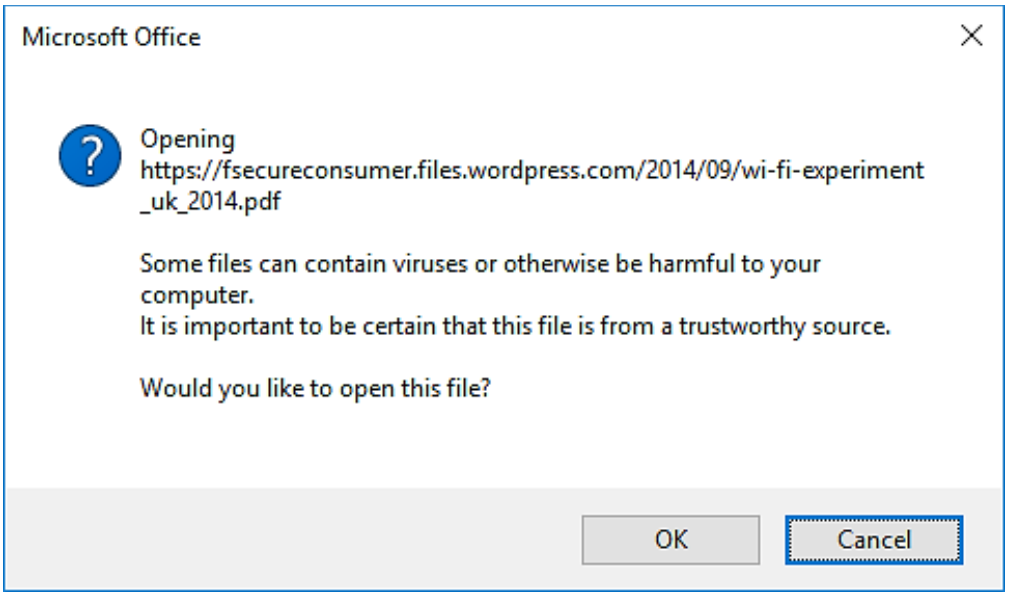

Figure 14: Security warning when the user clicks a link provided in a MS Word file

Also, this is a clear example that while some leading developers seek to adhere to known design principles to deliver applications that reduce security risks by providing security features that help users understand the potential threats before taking any actions that could damage their systems, other dealing developers who are developing well-known and widespread applications have failed to adhere to some basic design principles.

Another apparent example of adopting the targeted security awareness approach is illustrated in Figure 15.

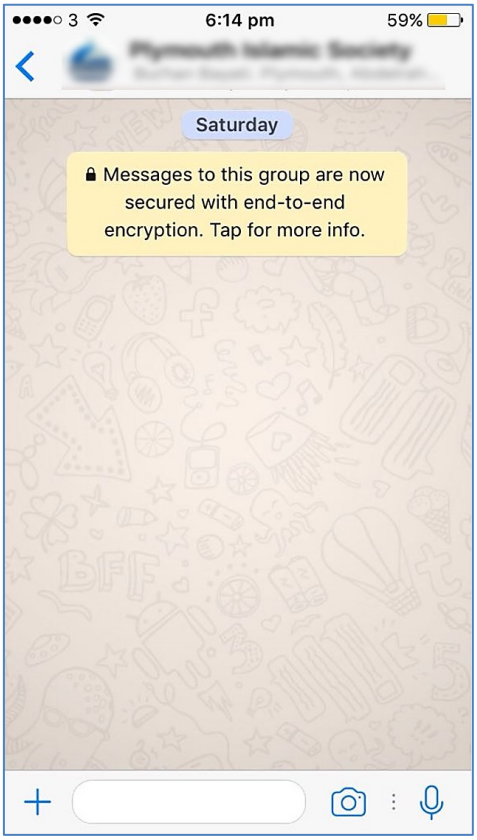

Figure 15: The message informing the user that data sent is encrypted

The screenshots shows the application of WhatsApp. The application provides a clear and simple initial message to inform the user that the data sent through this application /connection is secure and encrypted between the two ends of the connection and cannot be seen by any other parties. If the user does not understand the initial message, the user can then click on the initial message for more explanation as shown per screenshot in Figure 16.

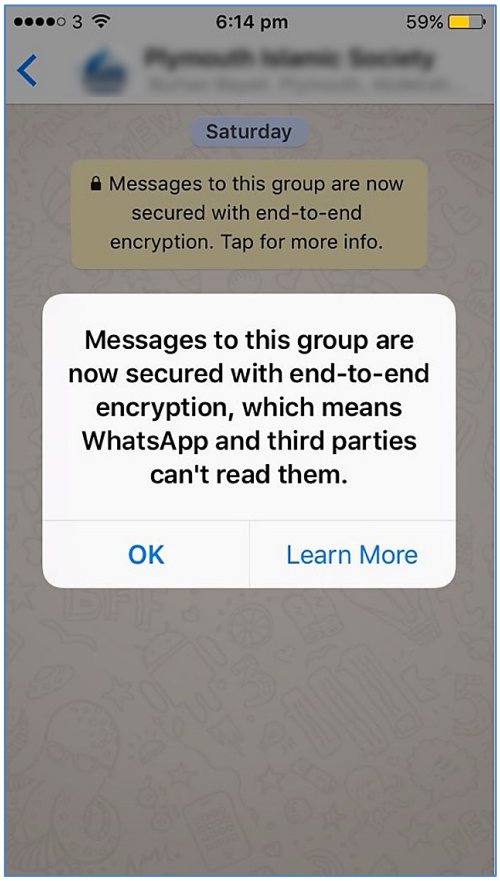

Figure 16: More information provided to the user by WhatsApp application

If the user is still in doubt and needs to acquire additional information, the user can then click the *Learn More* button and then access the page in the link below:

https://www.whatsapp.com/security/?lg=en&lc=GB

The page provides additional and clear information to clarify the security feature of the application where the application provides privacy and security and data protection when transferring data between the two ends of the connection through the provision of encryption between the two ends of the connection to ensure that no other parties can access to this data when transferring between the ends of the connection.

3.7 Opportunities for Targeted Security Awareness

There is a wide variety of scenarios and opportunities in which targeted security awareness raising could be an effective method in raising the security awareness of the users. This can be achieved by providing guidance and nudges during the time when dealing with the IT systems and supporting the users in making more informed security decisions when a potential risk arises. The following section will explore and discuss in more details these scenarios and opportunities.

3.7.1 Poor Password Selection

Despite countless efforts to displace passwords, passwords are more extensively used and rooted than ever (Herley and Van Oorschot, 2012). Password authentication continues to be the main method of user authentication for online systems. Unfortunately, users repeatedly still create passwords that are easy for them to remember but also easy to guess (Furnell, 2005), regardless of their deep-rooted and widespread use, the underlying password choices made by end-users continue to demonstrate a wide range of weaknesses. For example a survey conducted by Furnell and Bär in 2013, revealed that about one third of users chose weak passwords, including personal information or dictionary words (Furnell and Bär, 2013). Similarly, SplashData has published its annual list of the 25 most common passwords found on the Internet. The first communal used password was “123456” and the second was “password” (SplashData, 2014). Table 4 is presenting the annual list of the 25 worst passwords of 2013 and which found to be most common passwords on the Internet as SplashData has announced in 2014.

Table 4: The annual worst passwords list for 2013 announced by SplashData

Rank	Password	Change from 2012	Rank	Password	Change from 2012
1.	123456	Up 1	2.	password	Down 1
3.	12345678	Unchanged	4.	qwerty	Up 1
5.	abc123	Down 1	6.	123456789	New
7.	111111	Up 2	8.	1234567	Up 5
9.	iloveyou	Up 2	10.	adobe123	New
11.	123123	Up 5	12.	admin	New
13.	1234567890	New	14.	letmein	Down 7
15.	photoshop	New	16.	1234	New
17.	monkey	Down 11	18.	shadow	Unchanged
19.	sunshine	Down 5	20.	12345	New
21.	password1	Up 4	22.	princess	New
23.	azerty	New	24.	trustno1	Down 12
25.	000000	New			

In a similar study carried out by SplashData in 2014, the company released its annual list of the worst passwords of 2014, where the situation has not changed very much over the past year. The most common password is still the same as seen last year "123456", which has replaced the one in the head of the list for a long time "password". Other passwords that are selected based on the sequence of the keyboard are including "12345678", "QWERTY keys", "monkey", in addition to new passwords as shown Table 5. According to Burnett Forums security expert, the top 25 (below) represent 2.2 percent of all simple passwords vulnerable. Table 5 is presenting the annual list of the 25 worst passwords of 2014 and which found to be most common passwords on the Internet as SplashData has announced in 2015 (SplashData, 2015).

Table 5: The annual worst passwords list for 2014 announced by SplashData

Rank	Password	Change from 2012	Rank	Password	Change from 2012
1.	123456	Unchanged	2.	password	Unchanged
3.	12345	Up 17	4.	12345678	Down 1
5.	qwerty	Down 1	6.	123456789	Unchanged
7.	1234	Up 9	8.	baseball	New
9.	dragon	New	10.	football	New
11.	1234567	Down 4	12.	monkey	Up 5
13.	letmein	Up 1	14.	Abc123	Down 9
15.	111111	Down 8	16.	mustang	New
17.	access	New	18.	shadow	Unchanged
19.	master	New	20.	michael	New
21.	superman	New	22.	696969	New
23.	123123	Down 12	24.	batman	New
25.	trustno1	Down 1			

The situation has not shown any signs of improvement over the past few years, as in 2017 the problem persisted, as per results released by SplashData in its annual list of the worst 100 passwords of 2017. Table 6 presenting only the first 26 worst passwords in the list (SplashData, 2017).

Table 6: The annual worst passwords list for 2017 announced by Splashdata

Rank	Password	Rank	Password
1.	123456	2.	password
3.	12345678	4.	qwerty
5.	12345	6.	123456789
7.	letmein	8.	1234567
9.	football	10.	iloveyou
11.	admin	12.	welcome
13.	monkey	14.	login
15.	abc123	16.	starwars
17.	123123	18.	dragon
19.	passw0rd	20.	master
21.	hello	22.	freedom
23.	whatever	24.	qazwsx
25.	trustno1	26.	654321

In order to encourage and help users to choose an acceptable password in terms of its strength, numerous of websites have set up a password metre approach which gives the user visual feedback and indications to advise the user on the strength of the chosen password. Despite the widespread use of password meters, the effects of using these metres on security and their usability have not been well-investigated (Ur et al., 2012).

In order to change this behaviour, system administrators have introduced a number of methods, including the passwords that are created by the system with strict composition policies. The passwords set by system are difficult to guess, but users find often these passwords difficult for them to remember. Password composition policies, used to set requirements that each password on the system must meet and make them hard to guess. Furthermore, it also can lead to the user been frustrated and hence

users may make their effort only to meet the system requirements in simple ways that can be predictable.

Additional noticeable method used to encourage users to create strong passwords is to use password meters. A password meters is a visual illustration of the strength of the chosen password, which shown as colourful bar on-screen. Password meters employ suggestions to help users create strong passwords. Currently, many popular websites uses password meters to help users chose stronger passwords (Ur et al., 2012). Some of these websites offer a link of a list of tips and guidelines about password selection and why the user should do it in a certain way. Some examples are presented in Figures 17 and 18.

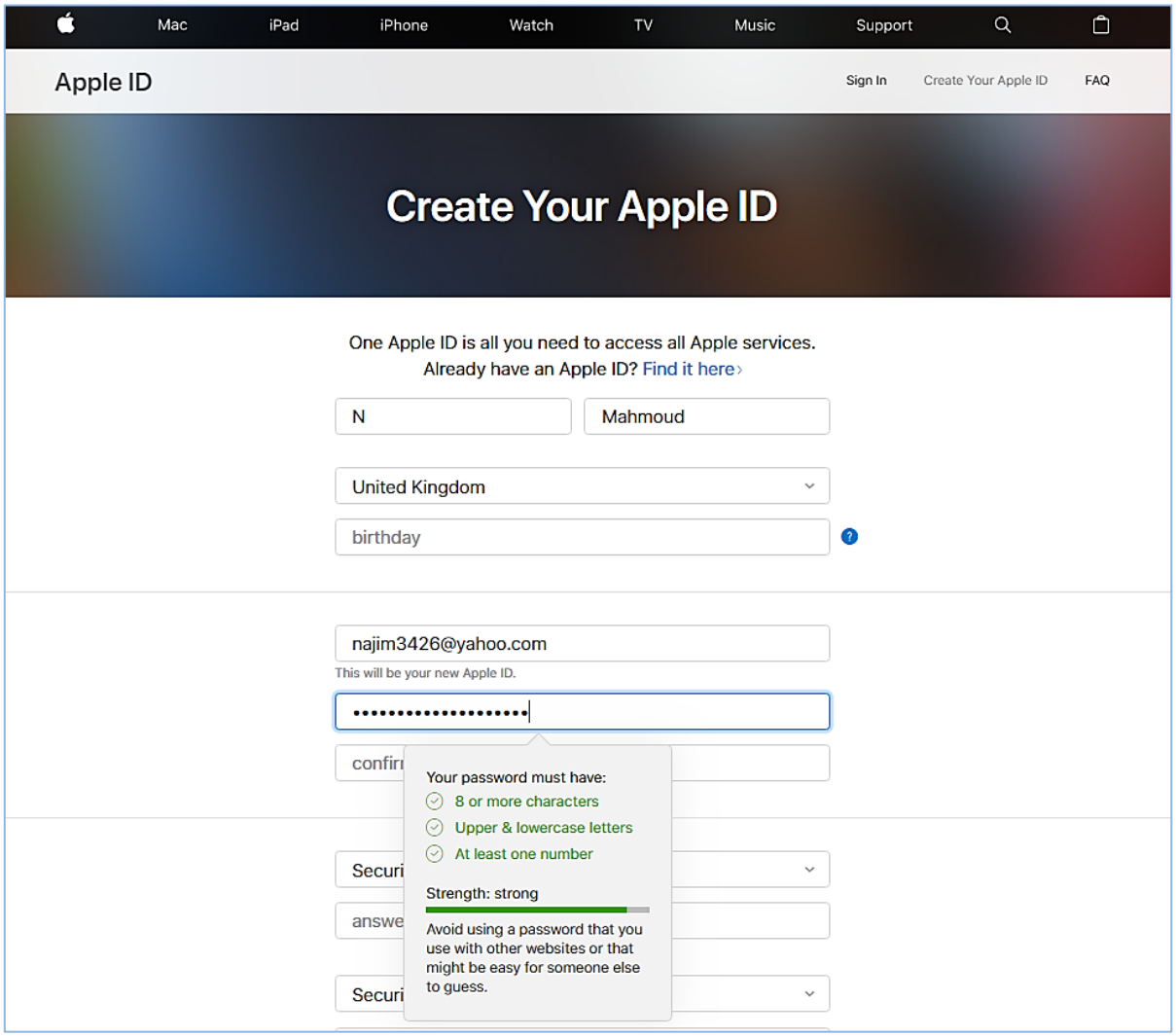

Figure 17: Example for the use of password meters (Apple ID)

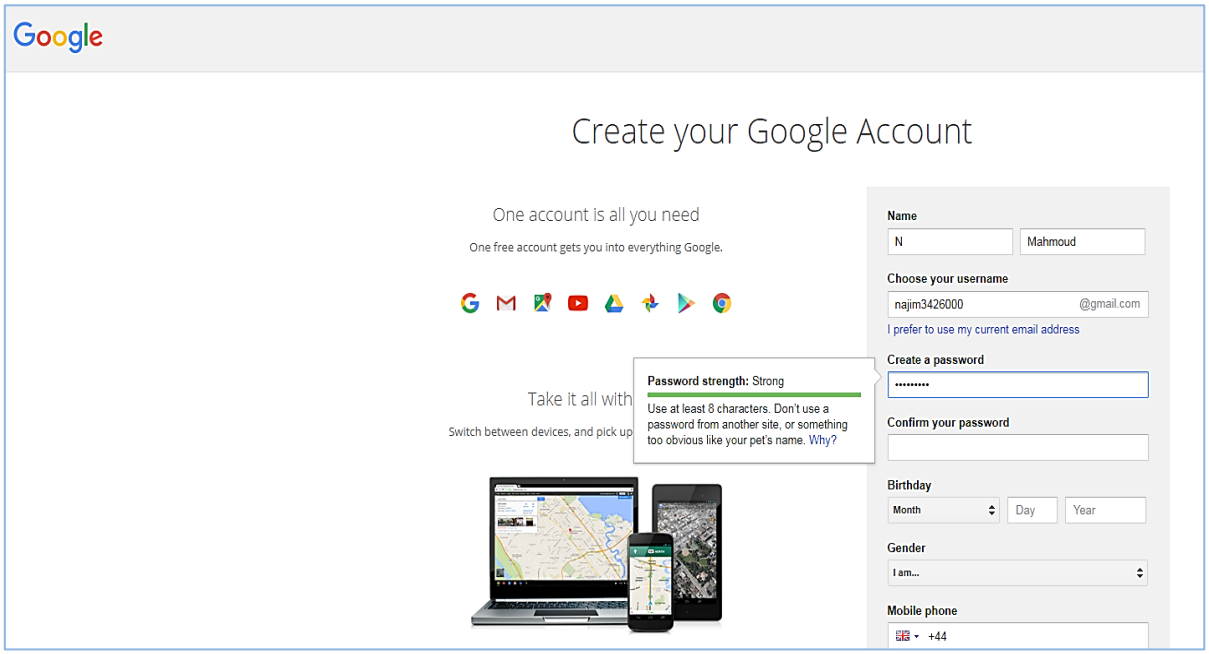

Figure 18: Example for the use of password meters (Google)

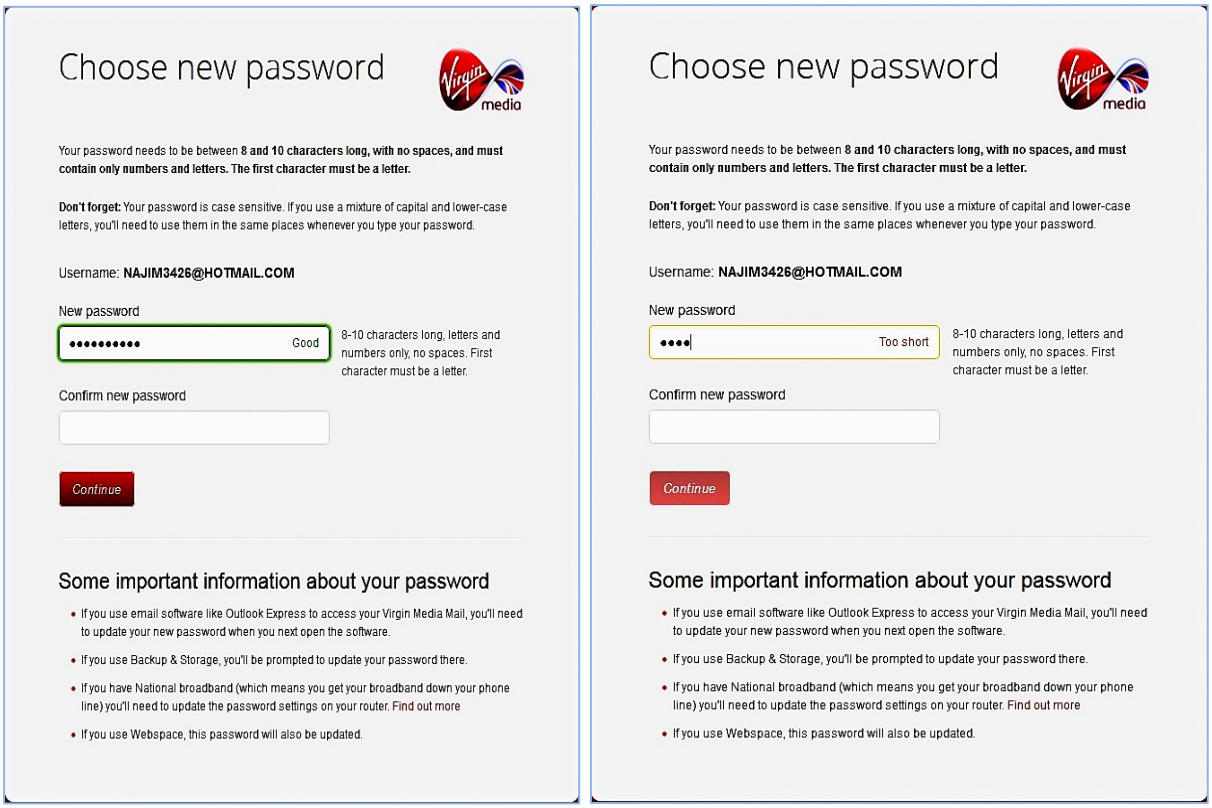

Figure 19: Example of password meters not requiring strong password choices

There are many password meters which guide the user to choose a password, but these password meters do not strictly require the user to choose a strong and complex password. An example of this type is shown in Figure 19. This approach reflects the concept of behavioural economics to gently prod or of soft control. This is done by stimulating and helping users through known behavioural patterns and biases, companies, governments and some of the other entities presented a variety of approaches for behaviour change.

Most users have a tendency to create simple passwords when there is no intervention (Florencio and Herley, 2007). Recently there are many organisations use password policies configured to force users to choose more complex passwords to increase the strength of users' passwords. However, users are expected to act in accordance with these policies in ways that can be predicted which potentially lead to reduce the strength of the password. Although previous work has shown that password-

composition policies require more characters or more character classes can improve resistance to automated guessing attacks, many of the passwords that meet the common policies are still weak. In addition, the stringent policies may cause to bother users, and which leads to prevent their productivity, and ultimately may lead them to write their passwords down or somewhere that anyone can access.

Figure 20 below illustrates the wide variety of types of password meters currently used by various companies. Some of these companies use the same type of password meters for the all sites that they owned such as Google and in other companies such as eBay use different types of password meters for their owned websites, for example ebay.de website uses a password meter that differs from that used by ebay.com (Ur et al., 2012).

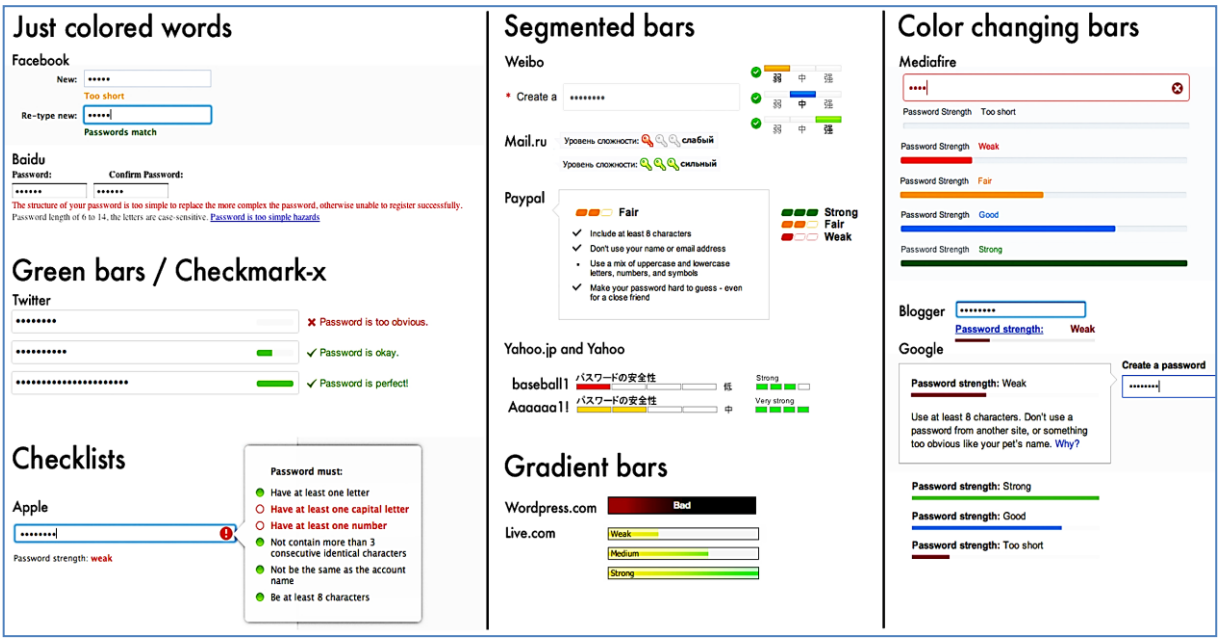

Figure 20: Examples of password indicators (Ur et al., 2012)

In the first and largest investigative study of its kind conducted by (Ur et al., 2012) on the use of passwords-strength meter found that the password-strength meter influence the user in terms of changing the behaviour and the security. Password-strength meters guide the user to make longer passwords. However, this study found that

unless the meters scored passwords stringently, the chosen passwords were only slightly more resistant to password cracking attacks.

Password meters that rated passwords stringently directed users to choose passwords significantly longer that contains a combination of more digits, symbols, and uppercase letters, and at the same time these passwords were not noticed to be hard to remember or unusable, yet these passwords cracked at lower rate by simulated adversaries. The most stringent meter that bothered users yet did not provide greater security benefits compared to those provided by slightly less stringent meters. A combination of visual and text indicators exceeded in excellence of performance. However, the appearance of visual indicators did not appear to have a significant impact.

Despite the fact that these more stringent meters contribute in adding more strength, it has been noticed the widespread use of more lenient meters. Similar research findings suggest that, as long as these metres are not perceived to be very difficult, the adoption of more stringent metres would increase security (Ur et al., 2012).

3.7.2 Connecting to Unknown Wi-Fi Networks

An alarming fact observed from research performed by Kaspersky Lab in partnership with Harris Interactive in 2012 is that 70% of tablet owners and 53% of smartphone/mobile phone users use free public Wi-Fi hotspots, meaning it is one of the most popular ways to go online. This means that mobile devices are become even more vulnerable, taking into account the well-known security problems associated with this type of unsecure connection, especially because most of these devices are not equipped with security software. Most users of mobile devices are exposed to data theft because there is considerable potential to intercept data transmitted over public Wi-Fi. Another surprising result of the survey is that although tablets are mobile devices,

they mostly connect at home. The survey found that Wi-Fi hotspots represent a real danger to the users of mobile devices as they are the most popular way used of the Internet connection for these devices although security almost non-existent. Figure 21 illustrating types of Internet connection used for mobile devices as found by Kaspersky Lab (2012).

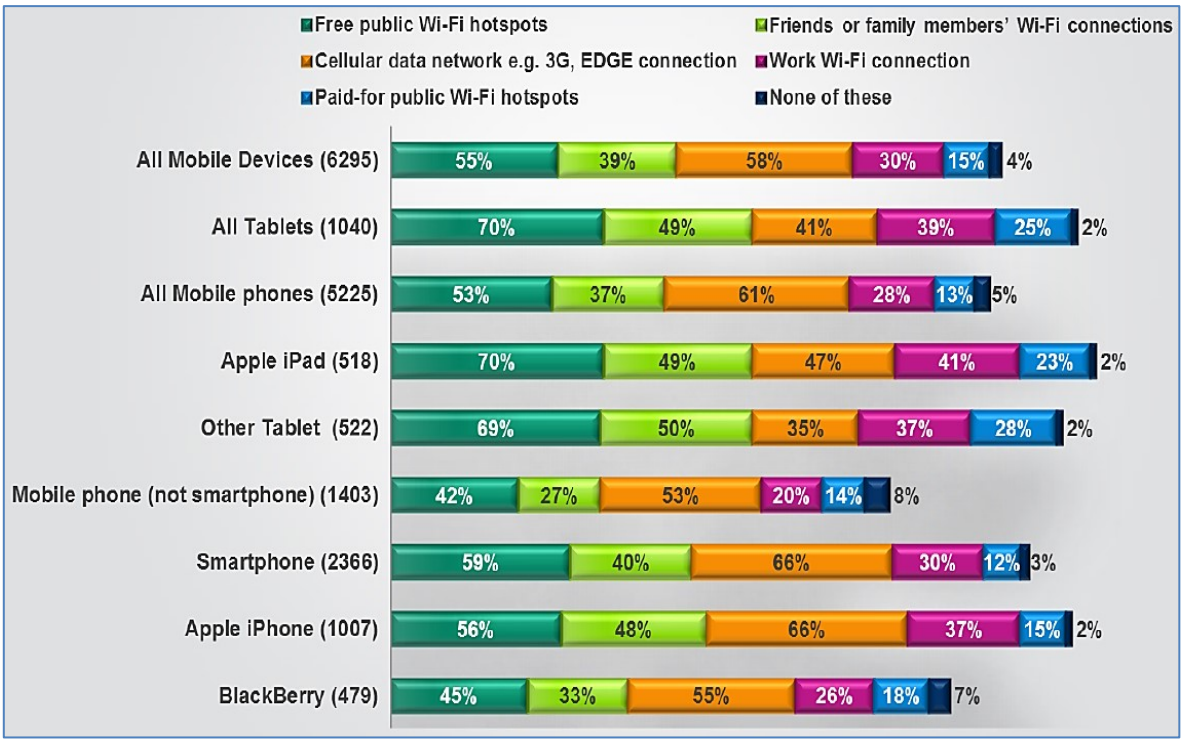

Figure 21: Types of internet connection for mobile devices (Kaspersky Lab, 2012)

The Europol has supported a comprehensive investigation of the Wi-Fi technology, the results of this investigations highlighted serious concern about the security of communications. An independent investigation was conducted by the Cyber Security Research Institute and the German penetration testing company SySS on behalf of ethical computer security company F-Secure. It found hundreds of people regularly logging onto "trojanized ' free Wi-Fi hotspot service that was created purposely to carry out their experiment (F-Secure, 2014).

The research into the Wi-Fi technology, which is used by more than 73% of households in the United Kingdom and 25% of households all over the world, found that users are impetuous about security risks related to the use of Wi-Fi, with more than 250 people having logged onto their Trojan hotspot in a period of 30 minutes.

The research also revealed the presence of significant weaknesses in the Wi-Fi system which allows the usernames and passwords for users who use email accounts on the POP3 protocol, which is widely used to be easily discovered when users send emails through Wi-Fi hotspots. This vulnerability can be exploited by any criminal who is offering and controlling a Wi-Fi hotspot to gather account information that would allow them to impersonate the user through their email account.

The experiment has confirmed and clearly highlighted that people pay no attention to computer security when they are on the move, a result confirmed by a recent survey from the broadcasting watchdog Ofcom, which found that more than 77% of the people were not concerned about the security risks linked with using public Wi-Fi.

This practically means that anyone can replace a current used hotspot by sending a stronger signal, catching the traffic, and then directing it to where it is desired. In addition, security experts have also raised other concerns by using the same Wi-Fi access point name, and blocking out the legitimate point by using a stronger signal and then allowing the computers using that access point to reconnect without having to sign in.

Other techniques currently being used by criminals include simply making available of access points that have a similar name to the organisation but disguised in the form of a guest or free account, all potential dangers that most people do not think of when looking for access to the Internet.

The investigation was carried out to test and examine the trust that misplaced by using a portable hotspot device built by experts from the German penetration testing company SySS at a cost of less than 160 pounds using a Raspberry Pi mini-computer system, an extended battery pack with a life of around two days and a Wi-Fi UTMS aerial, in addition to a USB port. The final product system is highly portable Wi-Fi hotspot that could easily be hiding in a small handbag as shown in Figure 22, and can be installed in seconds. It can be easily managed by an operator with a laptop to access the data captured.

Figure 22: The components of portable Wi-Fi access point (F-Secure, 2014)

The team made available of free Wi-Fi service in locations around London as part of an experiment to discover what type of actions that people are taken to protect themselves against possible danger when they are on the move.

Investigation of the F-Secure comes based on current conditions, which clearly shows the growing number people who reliance on the free Wi-Fi, which is also experiencing the mobile phone companies that offer a combination of cellular and Wi-Fi, which in many cases uses lists of open Wi-Fi hotspots.

This additional danger increases the risk to the public, since most consumers do not fully realize that the Internet service via mobile phone is being easily switched between different networks. The investigation of F-Secure also proved that offering free Wi-Fi hotspots, to maliciously to collect personal data from people when they are on the move is a very real and present danger.

Public Wi-Fi is not secure and security must be considered as a high priority, especially when moving in the fast growing area of hotspot 2.0. Now mobile phones connecting automatically to Wi-Fi hotspots, while there is not very much work done to verify the identity of the organisations that run and control the hotspots (F-Secure, 2014).

The researchers concluded that these experiments are evidence of the spread of ignorance among the population on a large scale on security issue of using unknown Wi-Fi. In spite of these experiences seem simple and easy to do, they should not be underestimated the seriousness of the results obtained.

The results show that the very real problem in the modern world is that while people heavily relying on the technology, the population is unaware of the capabilities that the technology has such as accessing their personal details and intrusion into their lives. The problem is that people implicitly trust their technology and are not aware of the negative impact of that trust.

There is a great request of bandwidth mainly driven by the desire of users to gain access to video, rich data applications and high-speed performance of the Internet during their movement. This desire for bandwidth is very similar to the desire of people to get things and free software on the Internet which in many cases has blinded sight of users to recognise the risks of the actions they are taking. With regard to the great

quest for a free bandwidth, the experiment carried out in spite of the strict conditions and circumstances clearly showed that users are willing to do anything.

Researchers have pointed out that there is a lack of collaboration between the different sectors of the industry. Telecommunications sector strives to provide increased user confidence and enhance the services it provides, but on the other hand, the sector has taken security shortcuts. The industry must be transparent by clearly illustrate what they are offering to their customers, and alert them when they are in contact with the Wi-Fi service that offers security risk. Moreover, telecommunications companies must explain clearly, what data is accessed on the customer's device in exchange for the service provided to the client over and above the terms and conditions. Finally, researchers pointed out that regulators, such as the Office of the Information Commissioner (ICO), should make an effort to alert customers of potential risks that could be faced (F-Secure, 2014).

Whilst using unknown Wi-Fi networks users should be made aware of the security risks that are associated with the use and security policies of such networks. Users' awareness should be raised before they get access to these networks. This could be done at the operating system level or the operator of the network should offer this opportunity before the users proceed to join the network. This perhaps will help users to know the security risks and hence have their chance to better decide whether to use or abstain from the offered Wi-Fi connection.

3.7.3 Using File Sharing Networks

One of the most appreciated features offered by the Internet is the ability to share and download files such as documents, programs, pictures, music, and movies. This is very common and practiced by users every day. Although there are a wide variety of large

retail sites that offer files for paid download. However, many users share files between one another. There is a wide range of ways that users can use to share files such as email and using peer-to-peer (P2P) sharing. However, the traditional sense of file sharing like using P2P sharing involves security risks which users should be aware of. The security risks are including copyright infringement, costly lawsuits, and potential criminal consequences (GetCyberSafe, 2014c).

File sharing networks which also called peer-to-peer networks (P2P), are widely used and very popular among users because are used to upload and download different types of files, such as music, pictures, movies, games, documents and in addition to the computer software across the internet. File sharing software products are available free on the global network. However, the use of file sharing network commonly involves significant security risks. The Canadian Bankers Association have tried to raise the security awareness of their customers by joining the campaign of the Cyber Security Awareness Month in October 2014 by strongly advising them not to install P2P file sharing software or use P2P websites. Customers also advised in the case that they decide to join or use these networks to exercise extreme caution (CBA, 2014). Precautions and tips offered by Canadian Bankers Association to users to keep in mind to protect themselves from the associate risk with the use of P2P including the following:

- In addition to issues related to breaking copyrights law, file sharing on peer-to-peer sites is widely used by criminals to distribute illegal or harmful files and viruses that are pretended to look like harmless downloads of popular songs, movies, or anything else popular that the user is looking for. The users also advised that relying on recent version of anti-virus software alone might not provide adequate protection.
- Users also advised not to accept the P2P software default settings, as doing so will make the user's system vulnerable by giving others the opportunity to gain access

to user's personal information, because almost default settings usually give other users access to personal folders, which could include full access to the My Documents folder on the user's home computer.

- Users advised at all times to manually determine which folders and subfolders they will share on the network.

For file sharing networks or P2P software, the operating system should warn the user about the security risks associated with the use of these networks. One of the big concerns of P2P networks is that it requires disabling firewall in order to work and hence leaving the user vulnerable to large scale of risks. In addition, users should also be made aware of opportunities of breaking copyrights law because of sharing some files like music, movies, as well as utilities software.

3.7.4 Posting Sensitive Information on Social Networking Sites

At present spread use of the Internet sites promote communication and encourage the dissemination and exchange of information between users such as the use of social networking sites like Facebook, Twitter and tumblr and use of the internet forums. While these sites are used for the purpose of communication between friends and family, exchange of ideas and share of information and following news, they also attract the attention of cyber criminals and been a very fertile ground for the them (CBA, 2014).

The information security breaches survey 2014 conducted by PwC, 2013 witnessed the increasing importance of social networks for large organisations. However, most organisations were struggling to find the best way to control the risks associated with the use of social networking sites.

Large organisations only tend to restrict use to corporate communications rather than just blocking access to social networking sites. Figure 23 illustrates how respondents prevent staff misuse of the web and social networking sites.

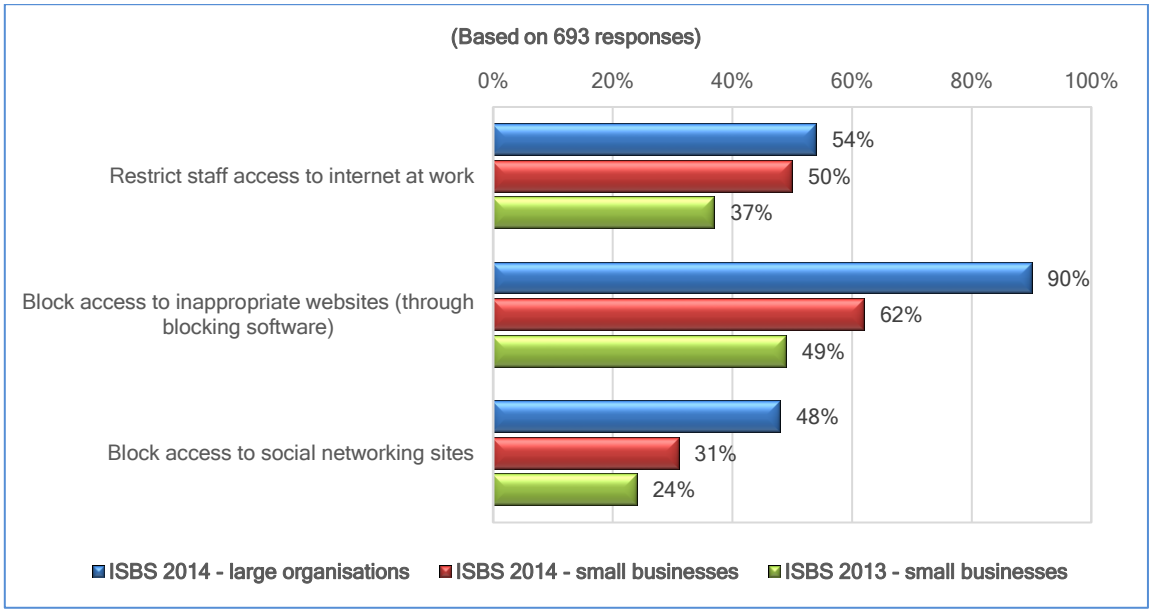

Figure 23: Preventive ways for staff misuse of web and social networking sites (PwC, 2014)

According to PwC report 2014, 16% of large organisations identified a security breach involving social networking sites in the previous year. However, the case appears better for small businesses, as only 5% detected a security breach related to social networking sites. This could be because fewer small businesses consider social network important for them and that they often have less detection capability compared to large organisations.

With regard to the misuse of social networking, PwC 2014 raised a story that took place in a small IT company located in London which did not take any steps to control the use of social networking sites. This led to multiple breaches relating to the misuse of social networking sites by staff that year. Unfortunately, these multiple breaches were not detected in a timely manner due to the lack of focus on the use of social networks (PwC, 2014).

With respect to increasing security awareness regarding the misuse of social networking sites, Canadian Bankers Association has joining the campaign of the Cyber Security Awareness Month in October 2014. Canadian banks have united their effort to take part in this international effort to help consumers protect themselves and their computers from cyber-crime. They have presented some helpful tips that the customers should follow in order to protect themselves against the risks that the use of these types of websites may introduce, these including the following:

- Users must be careful about what information included in their profile details. Users should not post sensitive information to profile and limit any online information about themselves, on social networking sites and in chat rooms, including phone numbers, addresses, date of birth, or other personal information, where this information could be used to impersonate the user identity and conduct fraud. In addition to alerting them to that never include or post any bank account information, or even their bank name (CBA, 2014); (RBC, 2014).
- Users must exercise caution when they add "friends" on the network. Users may not know who is behind some of online accounts, as it could be anyone; a new "friend" can be criminals who are out there to trick you into disclosing your personal or financial information.
- Users should check the privacy and security settings of the social networking site. Users are advised not to just accept the default settings, which normally set to allow more access that users want or realize. The normal setting access for the social website could be including a very large audience, the same can be applied to the discussion forum where the user may post things like their opinion which could be reached by everyone through the use of well-known search engines such as Google.

- Users should read carefully the privacy policy for the site they are using. Users advised to ensure that privacy policy does not include clauses that give the social network the right to use information posted on the site, which may mean selling contact information or email addresses.

As raised within aforementioned discussion of security issues related to the use of social networks, and their inadequacy in educating users about the underlying inherent vulnerabilities. There are many steps that should be taken in order to raise IT security awareness of end users whether on the operating system level, within a network monitoring level or at the point where a new user would like to join these social networking websites. There are also opportunities to raise IT security awareness at the web browser level whenever the user is typing the name of the website or before signing in. This is where context-sensitive security awareness can help and raise the awareness of the users about the security risks associated with the use of such websites.

3.7.5 Opening Unverified Email Attachments

Emerging computer communication technologies have fundamentally changed the way in which people communicate and exchange information (Torrubia et al., 2001). Electronic mail is one of the most widely used services on the Internet and has become such an important part in modern life that people now prefer to use it as a main tool to communicate rather than to make a phone call. Electronic mail is offering many advantages of speed and efficiency to stay in touch with friends, communicate with colleagues, receive e-bills from utility service providers or order confirmations when shopping online, read electronic newsletters, in addition to exchange of highly personal information, such as medical and financial data. However, lack of using e-mail safely

promotes many security risks which present themselves as the main source of rich information for cyber criminals (GetCyberSafe, 2014a).

Email is one of the easiest methods used by cyber criminals to target ordinary users (GetCyberSafe, 2014a). This security problem comes from security risks inherent in the use of e-mail service. However, to address this problem, there are many tools and methods available to protect users from hackers and malicious software. This includes anti-viruses protection solutions, anti-spyware and anti-malware solutions in general. Additionally, the email service providers contribute to protect users by introducing filleting techniques and give the user ability to block unwanted emails.

However, according to information security breaches survey 2014 conducted by PwC despite the availability of these wide ranges of protection tools and techniques provided by email providers, business disruption breaches involving staff misuse of emails or the Internet are most disruptive to businesses (PwC, 2014). For example, a small technology company specializing in the field of online security had their systems infected by a virus via email concealed as false certificates. This virus is not detected by a number of commercial anti-virus solutions and caused minor business disruption and damaged the reputation of the company. Similarly, a small financial services company lost a half-day of work after one of their staff downloaded a file containing malware from his personal webmail. As a result, several files shared between staff have been encrypted. This incidence took a week of work to deal with and resolve. As a result, the company made changes to their email usage policy and reconfigured the structure of their system to prevent this happening again (PwC, 2014).

3.7.6 Email Scams (Phishing Emails and Phishing Links)

There are many e-mail scams that have been tried by cyber criminals and these scams represent a real danger for users of e-mail. While these email scams have been recognized long time ago, cyber criminals continue to achieve the results that they are looking for. Email scams are now becoming very shrewd as well, using spoofing to make the email looks as much legitimate as possible which confuses users and makes it hard for them to notice and as a result make them open these scam emails.

Here are some examples as presented in the Public Safety Canada website to raise security awareness for users with respect to the current email phishing scams (GetCyberSafe, 2014b):

- **Fake business opportunities:** If a user receives an email with an opportunity to make a lot of money with inadequate effort in short time, or there are lack of information about the actual business, there is a great chance that this is a scam.
- **Lottery wins and prizing or "Jackpot" scams:** Users being asked to supply credit card information in order to claim prize or pay for shipping, users should be cautious of the source.
- **Health and diet scams:** The promise of the magic diet pills or quick weight loss can be very attractive for some people, encouraging them to follow these links by clicking on them without thinking or verification from the source. If the recipients of the email observed words like "quick" and "discount" in the same e-mail, it is very likely to be a scam.
- **Discount software:** Downloading software is also a trick used by email scams by offering a big price reduction with an unrevealed source, which is usually illegal. The software is likely pirated and potentially comes with Trojan horses or the likelihood is that the user will not get anything never in return for the price paid.

- **Advanced Fee Fraud:** These schemes provide a large amount of money should user get involved. They are carefully arranged, and provide false documents to give the appearance of legitimate business proposal and even invite users to meetings in their country. At some point, users may be asked for money to pay fees or other expenses and then all communication will be cut off.
- **'Pump 'n' dump' stock scams:** These are spam emails from an "investor" with confidential information, claiming that a particular stock is about to become very profitable. This will then raise the stock price, at which point the individuals behind the scheme sell - and the price collapses.

As mentioned earlier, Email service is among the preferred methods for cybercriminals to target users. To protect users, many techniques and tools have been developed to keep users from being victims of cyber criminals. However, all of these solutions deal with the technical side including software and hardware level. All these techniques and tools have not done enough in terms of increasing security awareness of users by informing them about potential risks with email links and attachments, before they make actions like downloading e-mail attachments or clicking on links with unknown e-mails. Increasing awareness of users will give users a chance to think before taking any actions that will make them victims and infect their systems.

For example, the Microsoft Outlook webmail service has filtering techniques to identify phishing emails. However, in the following screenshot, although it has been detected that phishing e-mail as shown in Figure 24, it fails to provide enough information for the user before or while making decision to unblock the email content. For instance, if the user tries to activate these links a window will appear as shown in Figure 25. This window does not contain sufficient explanation to raise security awareness for the user about the risks associated with this e-mail. It is only informing the user that parts of this

email have been blocked for their safety. It does not provide any explanation for the user that this e-mail is expected to be a phishing e-mail and what the potential risks are if the user proceeds to unblock these links, nor provides any information such as why was the e-mail or link has been blocked. Security awareness of potential risks should be raised for users and what users should do if they do not trust this email and this should be provided at the point when it is needed.

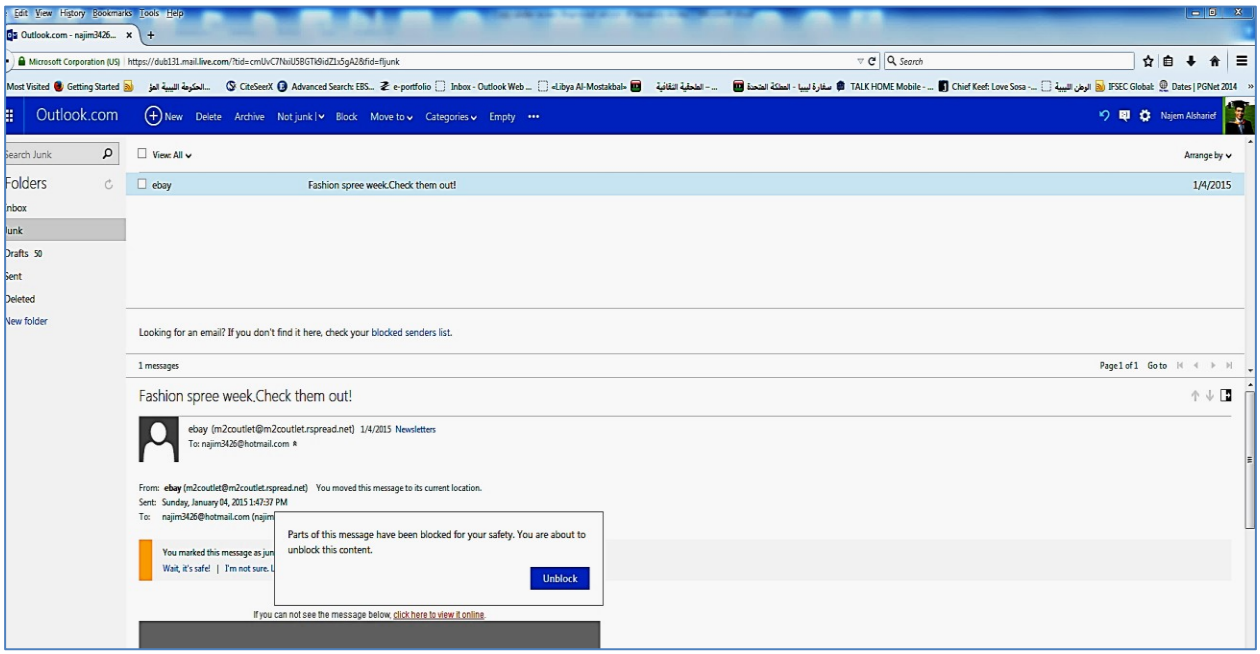

Figure 24: Detecting phishing email Microsoft Outlook webmail

Figure 25: Warning message when trying to unlock phishing links in MS Outlook

3.7.7 Using Uncertified Removable Media Devices

Removable media and removable devices have offered a great assistance for users of computer systems used for backup, store data, or to transport data from one computer

to another, as well as having the ability to be installed and removed from computer systems easily. These removable media or removable devices include USB flash drives, External hard disk drives, Optical discs, Memory cards, Floppy disks, In addition to other devices that are common today which include Digital cameras, Smart phones, tablets Wired or Wireless printers as well as other external/dock-able peripherals that can be easily removed from a system.

However, uncertified removable media devices are also considered as one of the main causes of spreading malicious software between computer systems if the files stored in them are infected with malicious software (Kaspersky Lab, 2014).

According to information security breaches survey 2014, removable media devices have rapidly become a key area of exposure. For example, over 10% of the worst security breaches in 2014 were due to portable media bypassing defences, which is more than double the level seen in 2013. Although, organisations increasingly are making more effort to develop security policy and controls regarding the use of mobile phones and tablets, these security measures do not always take into account the usage of removable devices such as USB sticks, removable hard drives, CD or DVDs (PwC, 2014).

Mobile devices are now a trend that cannot be stopped as many organisations are making risk based decisions on how to facilitate the use of such devices into the organisation. Slightly more than half of large organisations and three-quarters of small organisations have implemented a Bring Your Own Device (BYOD) culture. Most organisations are now using a variety of combinations of techniques to protect themselves from mobile threats, using both policies and technical defences. This is a positive sign as recently businesses have become increasingly aware of the potential

risks and the importance of adopting protection against cyber risks associated with the use of mobile devices (PwC, 2014).

There is a wide range of developed solutions to protect computer systems form being infected by malicious software including anti-viruses protection solutions like anti-spyware and anti-malware solutions in general as well as security warnings provided by operating systems to raise the security awareness for users. However, the problem of getting infected because of transferring malicious software through removable media still exists.

For example, staff at a scientific institute was inadvertently involved in spreading malware across their systems by using infected USB devices. It took more than 50 days to recover because of the ineffectiveness of their contingency plan. This incident led to changes made to their systems and measures to make contingency plans more effectively. Similarly, a government agency had a security breach because of the inappropriate use of mobile devices previous year. A security policy was issued as a result of this incident on the use of mobile computing and only allows access via approved devices.

Data shows that the use of mobile devices continues to grow and this means that the risks associated with mobile devices is on the rise. There were 9% of large organisations who had a data or security breach related to the use of smartphones or tablets, the same level as seen in 2013, although it is not clear whether all breaches are being detected currently. Only 38% respondents said that they encrypt the data held on mobile phones and only 42% of respondents said that they train their staff on the threats associated with mobile devices. In addition, there were 16% of the respondents who did not take any steps to address the risks associated with mobile

devices, which is very alarming, in relation to the increasing popularity of the use of mobile devices in daily business operations among all organisations (PwC, 2014).

As mentioned above, users dealing with removable media devices should be made aware of the potential risks before transferring data from these devices, especially if these devices are not certified. Despite the presence of security measures and controls to protect computer systems against these threats, users also need to be made aware of the potential risks associated with the use of removable media devices, especially if they are not certain about it. In the absence protection software or the protection software not being updated, the result of dealing with infected device will lead to the infection of computer system with malicious content. Implementing context security interventions will give the users a chance to think before taking any action.

3.7.8 Downloading Files from Untrusted Sites

Downloading a file means that this file will be transferred from the Internet to computer system. There are a wide variety of most commonly downloaded files such as programs, updates or other kinds of files such as game demos, music and video files, or documents (Microsoft, 2015). However, there is a risk that the file may contain a virus or a program that can damage computer systems or information stored in it. Downloading files from the Internet is potentially unsafe exposing computer systems to get infected with malicious software if the computer system is not protected, or the website is not trusted. There is no doubt that the worldwide web is the main source of malware software (Kaspersky Lab, 2014).

One of the most common ways in which computer systems become infected with malicious software is that users actively cause the malicious software to run not realizing that the file being opened or downloaded from untrusted web sites could

contain malicious software. Downloading files from untrusted sites is of one of the ways to distribute infected files with malicious software. There are some precautions users can take into account to help protect their computer when they download files from the Internet, such as installing a good anti-virus program on their computer systems. Users also advised to configure their anti-virus program to scan all files that they work with in real time. Most virus scanners can also be configured to scan emails as it arrives and quarantine infected messages. Moreover, because new viruses are discovered almost daily, users need to be sure to keep their anti-virus program up to date. Most anti-virus software has an automatic update facility that can help with this. Users should also use Microsoft's Windows update feature to be sure that they have Microsoft's latest fixes and security patches for their version of Windows. Windows update also has an automatic update facility that can help keep computer systems up to date (WinZip, 2014).

The rate of getting infected with viruses is high although all these security measures and controls have been widely available for long time for users dealing with computer systems. It is essential that user's security awareness should be raised and getting best advice on the associated risks before they proceed to download any type of files from the Internet. There is a wide variety of protection solutions like anti-viruses protection solutions, anti-spyware, and anti-malware to keep users and their systems safe as well as security patches provided from operating systems developers. However, if users fail to update the protection software or ignore security patches for their system their systems are defenceless and prone to be infected by malicious software.

Despite the fact that there are security warnings that operating systems normally provide for users to inform them about the potential risks as presented in Figure 26, these security warnings in some cases may not be sufficient in terms of providing

enough information to users about the potential risks, nor doing much to raise security awareness for end users of what has happened and most importantly why this happened. With time, users may become familiar with these security warnings and intend to ignore these messages and think that nothing bad will happen by doing so.

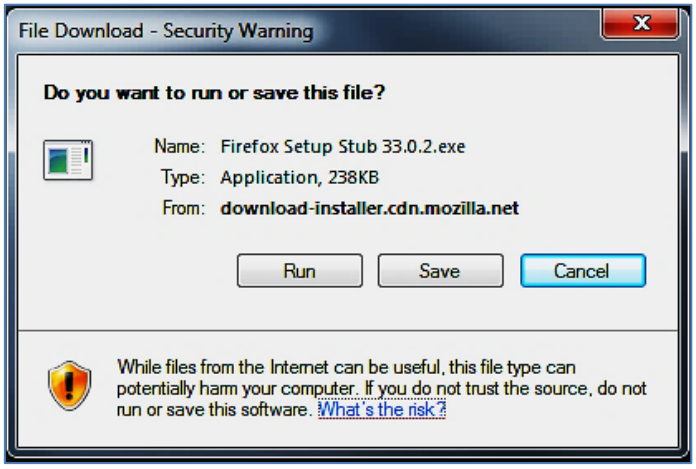

Figure 26: Security warning when downloading a file from the Internet

3.8 Conclusions

This chapter has primarily focused on various examples in which targeted security awareness-raising approach is implemented, and explored opportunities in which targeted security awareness could be adopted. It has also demonstrated one of the very important issues regarding the application of targeted security awareness-raising approach, is that despite the implementation of this approach by some prominent software developers in their applications, other leading developers still do not yet realise the advantage of this approach and adopted it in their widely used applications, instead they continue releasing applications that provide inadequate security guidance, which will not help users to understand the security necessities to protect their systems, and may affect a large population of users who are using such applications.

Furthermore, this chapter exposed that despite the existing use of such approaches, the popularization and proliferation of security interventions, which alerts users before

making their decisions about security risks remain limited in some applications, especially in terms of providing adequate security information and guidance to users in order to make informed security decisions.

Additionally, this chapter has provided a broad discussion regarding the problems related to security warning messages. Therefore, to address the aforementioned challenges, developing an innovative method to raise the security awareness for the end users in a timelier manner becomes an imperative issue. One of the promising and effective methods to address the warning messages issues is to provide support to users while dealing with IT systems in a timely manner. With the use of a comprehensible and simple explanation regarding the potential risk. This can be achieved by utilising existing security features such as security meters/indicators, and in the same time avoiding the provision of complex technical information at the first instance in the initial warning that novice users may not comprehend. Furthermore, additional access to more information regarding the risk should be by default offered to users to acquire further information in the case that the initial warning message is perceived as insufficient. This will also help when the users feel that they need more information in order to understand the risk. This approach has great potential to act as an effective way to ensure that users would not ignore security-warning messages and instead act to avoid potential security issues.

Finally, with current obstacles to effective information security and the use of existing security awareness-raising methods, as well as barriers to training and the possibility that users over time may forget what they have been trained on, the adoption of a targeted security awareness-raising approach to address these issues has become an imperative matter.

Chapter 4

The Effect of Targeted Security Awareness

4.1 Introduction

The human factor is normally described as the weakest part of security systems, and users still remain and are long recognized as the weakest link in the information security chain (Patrick et al., 2003; Ifinedo, 2014; Kegel, 2015; Tioh et al., 2017). However, in many cases they are ill-positioned to follow good practice and make the necessary decisions. Part of the reason here is that, even if security awareness, training and/or education have been provided, some of the key points may have been forgotten by the time that users find themselves facing security-related decisions. A potential solution in this context is to ensure that security guidance and feedback is available at the point of need, providing effective information to help users to make the right decision at the right time and avoid security risks.

This chapter examines the issue of targeted security awareness raising and presents the results of an experimental study conducted to test the effectiveness of the approach. This experiment was based around the scenario of connecting to Wi-Fi networks, to determine whether participants could make informed and correct decisions about which networks were safe to connect to. Four alternative interfaces were tested (ranging from a version that mimicked the standard Windows Wi-Fi network selection interface, to versions with security ratings and additional guidance). The aim of the experiment was to determine the extent to which providing such information could affect user decisions when presented with a range of networks to connect to, and help to move them more effectively in the direction of security. The findings revealed that,

while users exhibited far from perfect behaviour in terms of selecting more secure networks in preference to less protected ones, there was a tangible improvement amongst the users that had been exposed to the interfaces that offered and promoted more security-related information. In common with findings from other security contexts, these results suggest that users' security behaviours can be positively influenced purely through the provision of additional information, enabling them to make better choices even if the system does not provide any further means of enforcement.

4.2 Security Threats Inherent in Insecure Wi-Fi Networks

Wi-Fi is known for being fast, convenient and reliable; on the other hand, free Wi-Fi hotspots are increasingly seen as an IT security risk. In an era where data breaches make the main news almost daily, it would be justified for businesses to place a firm restriction to access their systems from the outside world. However, it is also apparent that modern businesses demands are often prioritized over security. For such businesses, the benefit of having their employees able to access email and corporate data on the move far outweighs possible IT security risks. As a result, just over half (51%) of mobile users stated that their companies allow them to use personal devices to access corporate data via public Wi-Fi hotspots (iPass, 2016a).

For the most part, people make security decisions and choices daily without fully considering their security implications. Organisations depend on their staff to frequently make security decisions when carrying out different tasks, both whilst in the workplace and on the move. An apparent example is the use of insecure public Wi-Fi hotspots to work remotely (for business purposes). It is believed that more than one billion workers are working remotely and this constitutes more than a third of the total workforce worldwide. The choice of using an insecure wireless network, when reliable networks or 3G/4G networks are unavailable, can become problematic as users use many

devices (perhaps their own devices) to access and potentially transfer sensitive information. When faced with time pressure, staff members tend to make hasty decisions that leads them to access unknown Wi-Fi hotspots. This behaviour poses a serious risk to the security of the device and its data, as these Wi-Fi hotspots provide many opportunities for cyber-attacks, including spoofing and man in the middle attacks. There are many techniques of manipulating and influencing wireless network selections, some of which are as simple as changing the name of the network. Helping users to choose networks that are safe and appropriate for their tasks, whether on personal or company-owned devices, is imperative to maintain a high standard of security. Indeed, choosing a secure and trustworthy Wi-Fi connection is one of the top 10 security behaviours that are encouraged on sites like www.staysafeonline.org (Turland et al, 2015). Nonetheless, many studies have found in general that users are impetuous about security risks related to the use of Wi-Fi hotspots (F-Secure, 2014). This has increased the need for further investigation of the attitudes of Wi-Fi users towards security risks related to the use of unknown Wi-Fi networks (in particular, the use of unknown Wi-Fi networks within public areas). To further evidence the problems, Table 7 gathers findings from various sources to demonstrate the tendencies of users on connecting to insecure Wi-Fi and accessing sensitive information.

Table 7: Evidence of users' trends towards using insecure Wi-Fi networks

Source	Key findings
(Kaspersky Lab, 2016)	• 71% of the surveyed users use insecure public Wi-Fi. • 15% of questioned consumers stated that they use public Wi-Fi to shop, bank, or make payments online without additional precautions. • People are still using their devices without equipping their devices with security solution and acting negligently. • As a result, 29% have been affected by online threats. • Consumers continue engaging with the online world at every opportunity, with 42% using free but potentially insecure public Wi-Fi, and only 13% using a secure VPN connection. • Kaspersky Lab concluded that the figures indicated a lack of security awareness among consumers in this regard. This places their valuable data at risk. Consumers share data insecurely, conduct important transactions on public Wi-Fi and treat their passwords without additional precautions. In addition, while these habits continue, only 60% of consumers protect themselves with a security solution on every device they own.
(iPass, 2016a)	• The report highlights that although mobile data services are available to users on the move, these services still cannot surpass the quality that the Wi-Fi hotspots provide in terms of speed, cost, convenience and performance. • 63% of respondents will choose a Wi-Fi hotspot over mobile data services. • Worryingly, employees know the security risks of public Wi-Fi; nevertheless, many are still used it anyway. • 66% of respondents stated they were concerned about the security of Wi-Fi hotspots. However, only 28% of respondents said they use a VPN all the time, and more than a third 38% never do. • The iPass report concluded that mobile users expect to remain connected and productive always working as they see fit, not based on the type of the communication method used to connect to the Internet. • Mobile users do not want to waste their mobile data on draining business/personal applications or use slower connectivity options which may not provide the reliability and performance they require. They want to use Wi-Fi first.
(iPass, 2016b)	• 94% of organisations see public Wi-Fi as a threat. In the meantime, 88% of organisations admitted that they find it difficult to consistently implement a safe mobile usage policy.

	• Businesses are struggling to create security policies that provide mobile users with the flexibility they demand. • The report also highlights that many employees still choose high-risk connectivity options despite knowing the potential security risks. • 66% of mobile users said they were worried about data security when using free public Wi-Fi hotspots, yet 42% still access company data using public Wi-Fi hotspots.
(F-Secure, 2014)	An independent investigation was conducted by the Cyber Security Research Institute and the German penetration testing company SySS on behalf of F-Secure company. • It found hundreds of people are regularly logging onto a "trojanized free Wi-Fi hotspot service that was created to carry out their experiment. • The research also revealed the presence of significant weakness in the Wi-Fi system which allows the usernames and passwords for users who use email accounts on the POP3 protocol which is widely used to be easily discovered when users send emails through Wi-Fi hotspots. This vulnerability can be exploited by any criminal offering and controlling a Wi-Fi hotspot to gather account information that would allow them to impersonate the user through their email account. • The experiment highlighted that people pay no attention to computer security when they are on the move.

While using unknown Wi-Fi networks, users should be made aware of the security risks that are associated with the use of such networks and its security policies. Users' awareness should be raised before they get access to these networks. This ought to be done at the operating system level or the operator of the network should offer this opportunity before the users proceed to join the network. This perhaps will help users to know the security risks and hence have their chance to better decide whether to use or abstain from the offered Wi-Fi connection.

There is a lack of investigation into the existing systems in terms of whether the users are getting best support and advice before they get connected to unknown Wi-Fi hotspots. In response to these issues and to achieve a comprehensive study, an

experiment has been conducted to assess users' attitudes towards the use of unknown Wi-Fi networks in a public environment using four different user interfaces.

The findings of the research will enable the identification of the level of guidance that is required to help Wi-Fi users when performing routine online tasks without unduly interrupting or overloading them with vast amounts of information.

4.3 The Limitations of End-User Recommendations of Selecting Wi-Fi Network

Most existing platforms seem to not provide adequate security recommendations and security guidelines that nudge users towards selecting appropriate Wi-Fi hotspots based on their need and to mitigate user's security risks of connecting to insecure Wi-Fi hotspots. The only available option that the existing platforms are providing to users are the padlocks, which indicates that the wireless network (Wi-Fi hotspot) is protected with a password.

Apple's iOS is beginning to take steps in this direction. However, the currently used feature does not seem as adequate. When the user is exploring available Wi-Fi networks that have no protection, a text appears beneath the network name (i.e. security recommendation), where the user can then click on more information, and then a new window appears providing the following message "Unsecured Network Open networks provide no security and expose all network traffic. If this is your network, configure the router to use WPA2 personal (AES) security type." In addition, a link is provided which leads to a new page offering support from Apple. This page however is not quite what users are expecting, as it is firstly, titled "*Recommended settings for Wi-Fi routers and access points*" and secondly, the target audience for this page is clearly inconsistent with the typical users' scenario "*this article is for network administrators and others who manage their own networks*".

Providing these tips would probably help in mitigating users behaviours that might put their data and devices at risk by connecting to insecure Wi-Fi networks rather than telling them the settings of wireless networks which they have no control of which are probably in public areas. The screenshots in Figure 27 illustrate the message that users get when exploring Wi-Fi hotspots and the message they get when trying to connect to any insecure Wi-Fi network using Apple iOS.

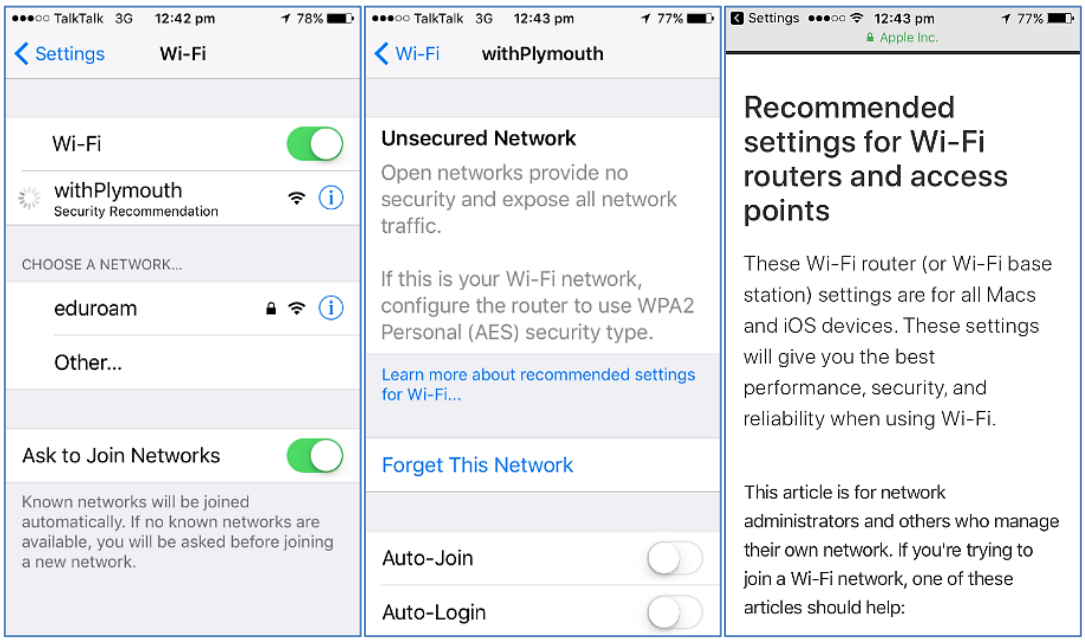

Figure 27: Selecting Wi-Fi network using Apple iOS

In comparison, the Android platform has taken no concrete steps in this direction as shown in the screenshots illustrated in Figure 28. The only message that told the user about the level of security was a subtitle with "*None*" beneath, which probably would not be adequate to provide an answer for the user of why the security of this Wi-Fi network is "*None*". Furthermore, it does not provide security guidelines and advice of what sort of activities that users can do if they are connected to the Internet using this Wi-Fi network.

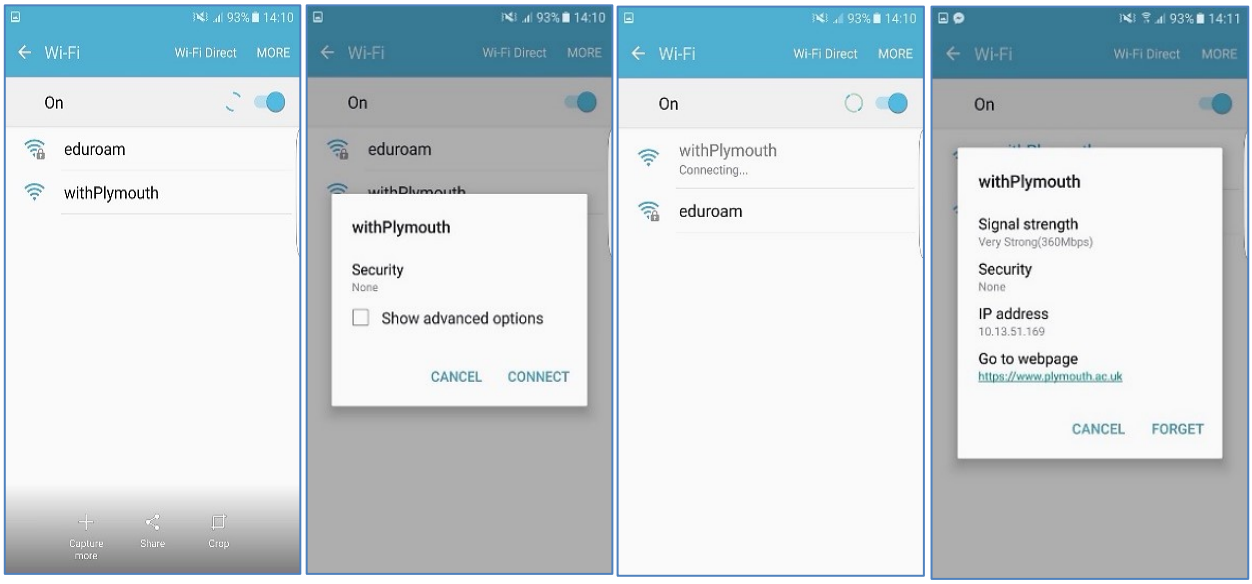

Figure 28: Selecting Wi-Fi network using Android mobile operating system

Additional example is that when a user is trying to look up for available wireless networks within the Microsoft Windows 7 platform a window will appear as per the screenshot shown in Figure 29.

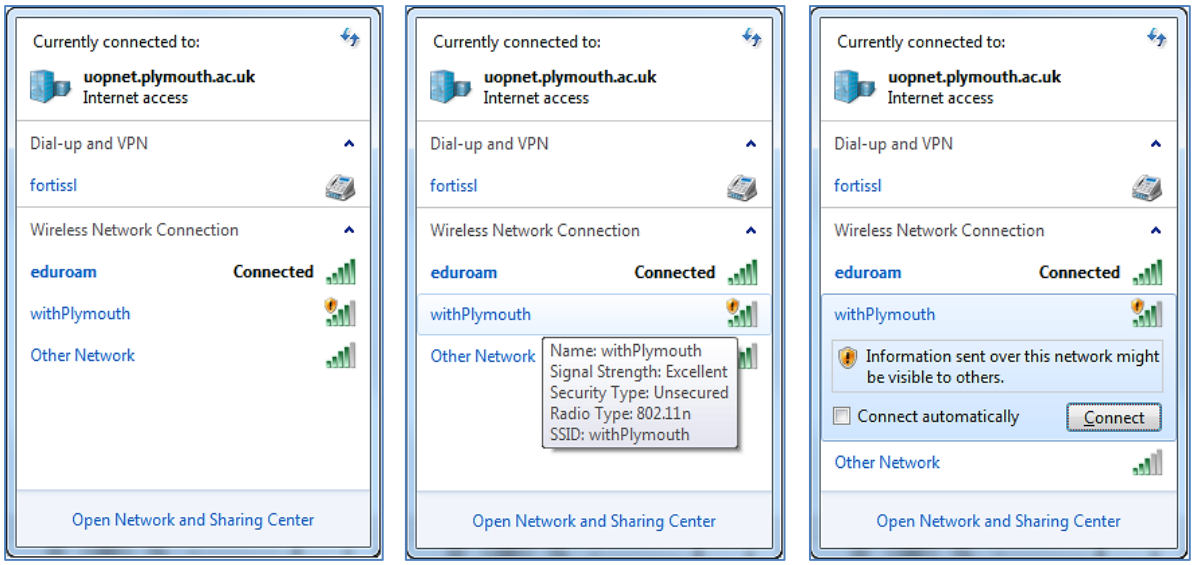

Figure 29: Selecting Wi-Fi network using Microsoft Windows 7

Although this window is to inform the users about the available Wi-Fi networks within their area alongside with their signal strength and the name of these Wi-Fi networks, users can also get additional information about these available wireless networks by

pointing the pointer at the name of any of these networks. However, this information may not be sufficient in terms of providing sufficient security guidance to users to whether these networks trustworthy or to give them the chance to better decide or abstain from these Wi-Fi hotspots. Users perhaps would not understand abbreviations and technical terms such as “Security Type: WPA2/ WPA2-PSK”, what users need at this point is some advice like whether these networks are trustworthy or not, whether to use any of these networks or not and perhaps what can the network be used for. Additional information that have the potential to support the users decision may include some characteristics of these networks, such as informing the user whether the network is using or providing encryption protocols or if it is not using them at all, also giving users more advice and security guidance of the sort of activities that they can carry out, or the sort of activities they should not carry out based on the characteristics of these networks and the security considerations if the user connect to it. This type of security advice may have the potential to be very useful in supporting the user’s decisions at the point when needed (i.e. in making a decision whether to use the Wi-Fi or not) and consequently nudging them towards better security decisions.

4.4 An Experimental Trial of Alternative Wi-Fi Selection Interfaces

The main aim of this research work is to utilise different user interfaces of Wi-Fi networks in order to evaluate their usability and the security, to overcome some of the information limitations presented by existing user interfaces. The purpose of the user trials is to investigate the usability, security, and clarity of different user interfaces and to determine whether they have an effect upon user decisions.

4.4.1 Experimental Methodology

Four prototypes were developed, an existing interface used in MS Windows platforms; an improved user interface with warning message; and an advanced interface with a

security meter (Design 1) and (Design 2), these were developed to simulate the user interface of Wi-Fi networks in order to address the main objectives of the proposed experiment.

The aim of this research experiment was to identify whether users will connect or will continue to connect to unknown Wi-Fi networks in public areas if they have been provided with adequate security information about the available networks.

All interfaces contained two known Wi-Fi networks to participants namely the eduroam and withPlymouth, which users normally expect to see during their Wi-Fi interactions on the university campus, and two unknown Wi-Fi networks namely BellaCostaCafe and eduroamhighspeed. Eduroamhighspeed was named purposely to test if this name will affect participants' selection as to whether they will be attracted to the name as it implies a high speed network by including the wording of a high-speed with the existence of the known and trustworthy network eduroam. BellaCostaCafe was named to test if users will recognise that this name is not known to them within the university campus environment and hence they would abstain from connecting to it.

The design of the experiment was to examine whether users would connect or continue to connect to unknown Wi-Fi networks if they have been provided adequate security information about the presented Wi-Fi networks. To achieve this, the first and second interfaces were designed to analyse whether the user is tempted to connect to unknown Wi-Fi network in case a trustworthy network would be inaccessible. In contrast, the third and fourth interfaces present a padlock, on the trustworthy network, to indicate that an authentication is required. However, when clicked it connects the user without requiring authentication. This was to investigate whether users would recognise this flaw on the network and its potential threat.

The participants were divided randomly into four groups and asked to try one of the four interfaces, to choose an appropriate Wi-Fi network and to perform the task that was stated in the following given scenario:

> *"Experiment Scenario*
>
> *Consider yourself at the university campus, and you are connecting to a Wi-Fi hotspot to browse the Internet in order to use applications such as emails, online banking, and social networking services.*
>
> *You are requested to use the wireless network selection interface to choose an appropriate network from which to conduct these activities.*
>
> *Please note that you only need to select and connect to an appropriate network; you will not actually be required to send emails, or perform any of the other tasks mentioned above.*
>
> *You will then be asked to comment upon the usefulness or suitability of the interface that was used."*

The study involved 100 participants who were 18 years of age and older, divided randomly into four groups (25 participants for each interface), with all data and responses treated anonymously. The users were involved in only one session of the study. This means trying only one of the proposed four interfaces for approximately 15 minutes.

The experiment procedure required participants to use the prototype software that simulated the process of viewing available Wi-Fi networks and asked them to connect to the most appropriate network in a given scenario as mentioned earlier.

After completing the session, users were also asked to fill out an online survey that took approximately 15 minutes. The survey was used to investigate users' acceptance of the developed interfaces from both the aspect of security and usability.

All users' interactions in the four groups with the four interfaces were captured and stored on the computer that was used for the experiment to collect the results for later analysis and to examine if the improvements of the interface were helpful in making users change their behaviour of connecting to unknown Wi-Fi networks in a public environment. In addition, there was a screen recording for the user interaction with the interfaces to assist in analysis and revision at later stages.

4.4.2 Experimental Prototypes

The prototypes were implemented as an application to run on the Microsoft Windows platform, and the trial design considered four different user interfaces for selecting Wi-Fi networks. The first interface was designed to simulate the Wi-Fi dialog window that is used in the Microsoft Windows platforms, when a user is searching for Wi-Fi networks. Windows 7 operating system was chosen over the later versions of the OS because participants were most likely to be familiar with this version on the basis that (a), it was the version of the OS used on campus at the time of the study and (b) it was the most prevalent version of Windows in general use at the time of the study and remains so at the time of writing (Netmarketshare, 2017).

The screenshots presented in Figure 30 illustrate the designed first interface that was used in the experiment. This interface is defined as "*Existing interface used in MS Windows platforms*".

The second interface was also designed to simulate to the Wi-Fi dialog window that is used in the Microsoft Windows platforms. Furthermore, it also has some improvements

and changes, which include a dialog window that appears when the users click the connect button, as shown in the screenshots below, to alert the users and allow them to choose either to "*Accept*" or "*Reject*" the connection. It also has the padlocks which are no longer used in recent Microsoft Windows platforms to indicate to the user whether the network requires a password to access it or not (see the screenshots in Figure 31). This interface is defined as "*Improved user interface with warning message*".

The third interface was designed differently compared to the previous interfaces, with improved information security panels that have security information about the explored Wi-Fi network and recommended usage. This interface also had security meter indicators for each available Wi-Fi network, which presents the extent of the security level that the Wi-Fi network had as illustrated in Figure 32. This interface also had the advantage of featuring a "*Click for more information*" link opposite each security meter. When a participant clicked, a dialog window was presented as shown in Figures 33, 34, 35 and 36 to alert participants and give them more security information about the Wi-Fi network that they are exploring and allow them to make their decision based on the security information and recommended usage. This interface is defined as "*Advanced interface with security meter (Design 1)*".

In order to influence the security behaviour of users in terms of making more security-oriented decisions, four security meter settings were used. The first security level (Excellent) was specified with the colour code green, the second (Good) with yellow, the third (Fair) with amber and the fourth (Poor) with red. The security panels were also designed to have a traffic light design where green was used to indicate that the setting(s) are (Enabled) for the security protocols or for the encryption protocols for the presented Wi-Fi networks in the interface and red to indicate that the setting(s) are (Disabled). The green colour was also used in the start-up time setting to indicate that

the Wi-Fi network was in operation for a long time and red was used to indicate that the Wi-Fi start-up time is very recent. Moreover, green was also used in the settings of previously connected to indicate that the Wi-Fi network has been used previously and red to indicate that it has not been used before. Finally, yellow was also used to indicate that there was a change in the setting(s) of the presented Wi-Fi network and green to indicate that there were no changes. Users also have the feature to hover the pointer over the traffic lights to gain more information about the traffic lights by providing a brief explanation of why it is yellow, amber, or red.

The fourth interface (illustrated in Figure 37) was designed to be similar to the third interface with the only difference being that users will see the security panels that have security information about the explored Wi-Fi network and recommended usage if they either clicked on the link "*Click for more information*" or if they clicked on the button "*Connect*" and in the latter case users would have the choice to either "*Accept*" or "*Reject*" connecting to the selected network. This will ensure that users have the chance to know about the security information and the recommended usage for any network they select before they make their decision to gain access. Figures 38, 39, 40 and 41 illustrates the improved information security panels with two buttons to allow the user to either "*Accept*" or "*Reject*" connecting to the selected network. This interface is defined as *"Advanced interface with security meter (Design 2)*".

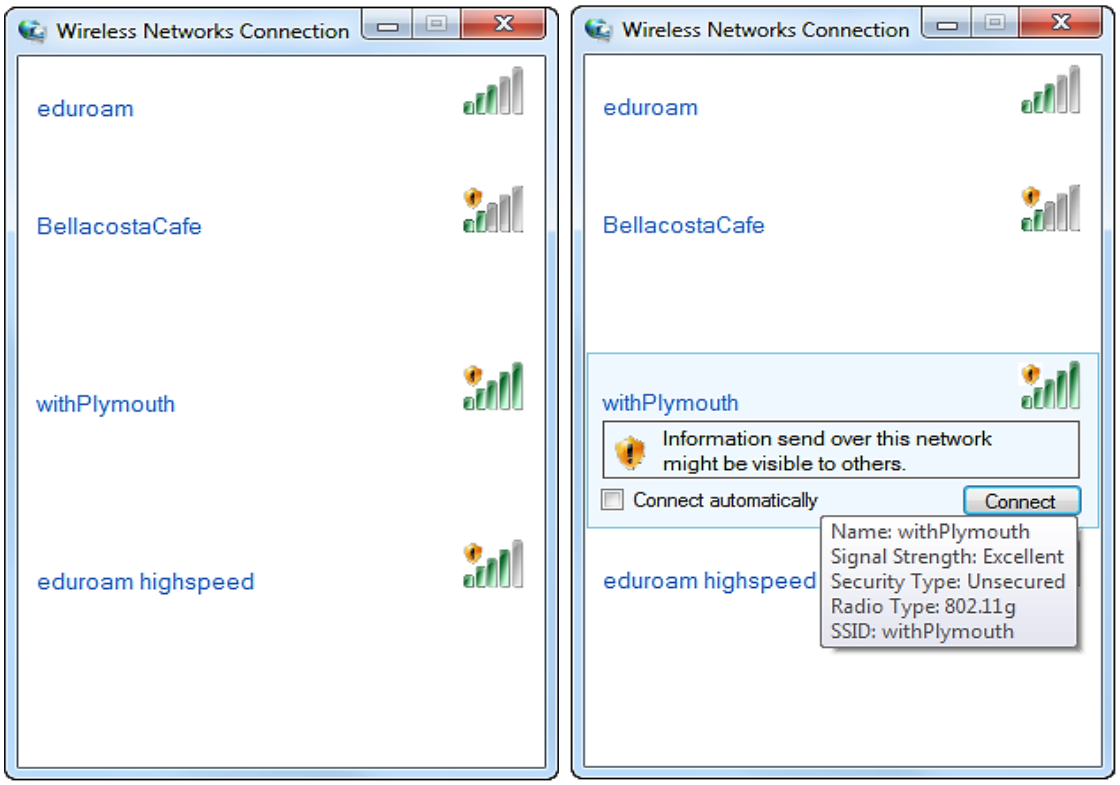

Figure 30: Second Wi-Fi interface - Improved interface with a warning message

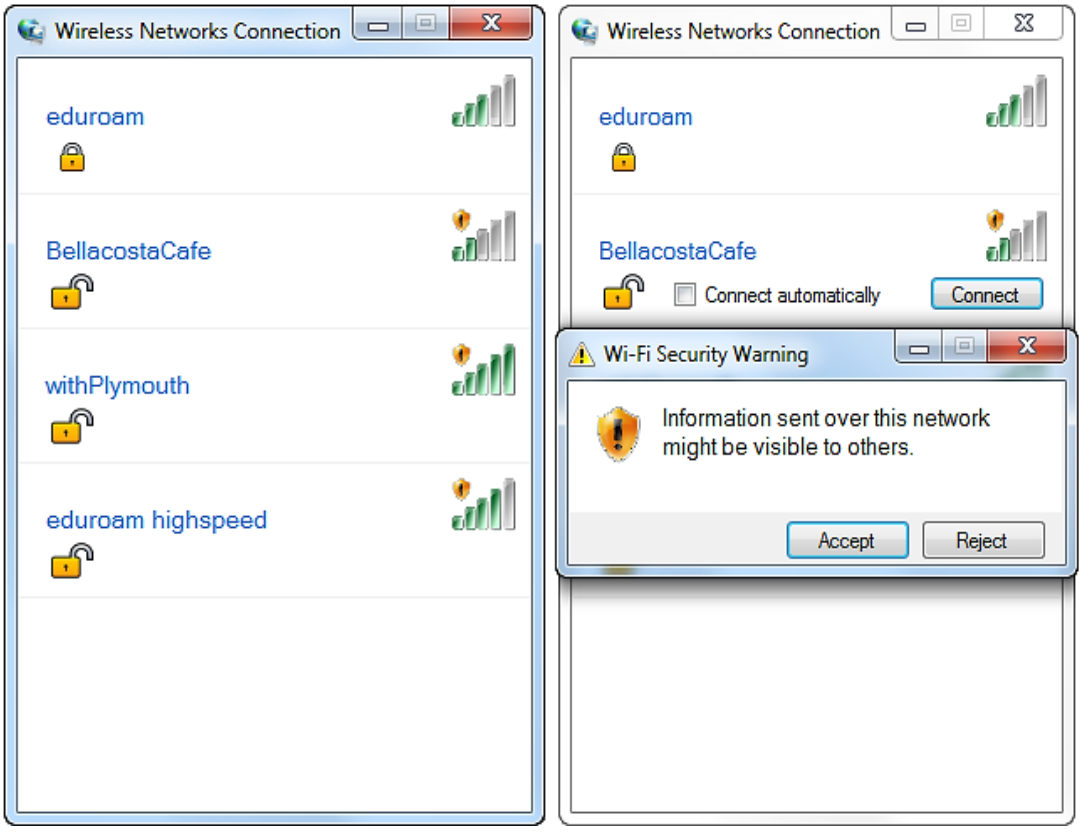

Figure 31: First Wi-Fi interface - Simulating existing interface in MS Windows platforms

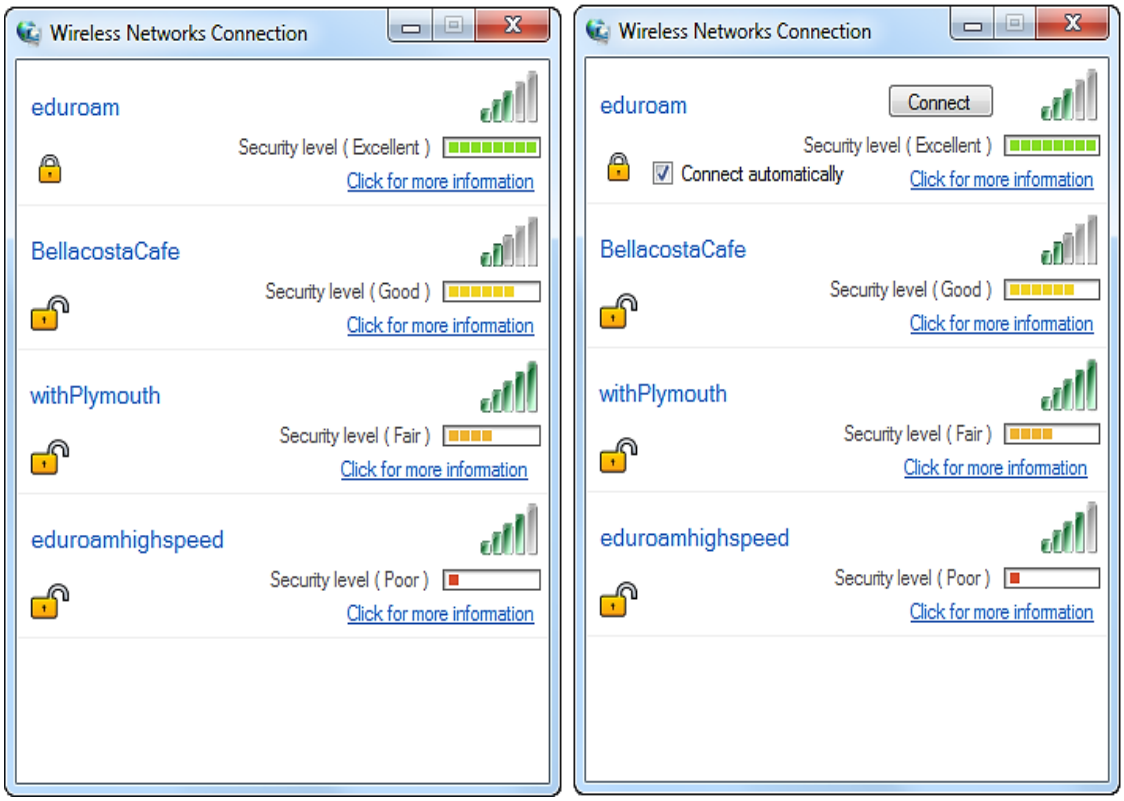

Figure 32: Third Wi-Fi interface - Advanced interface with security meter (Design 1)

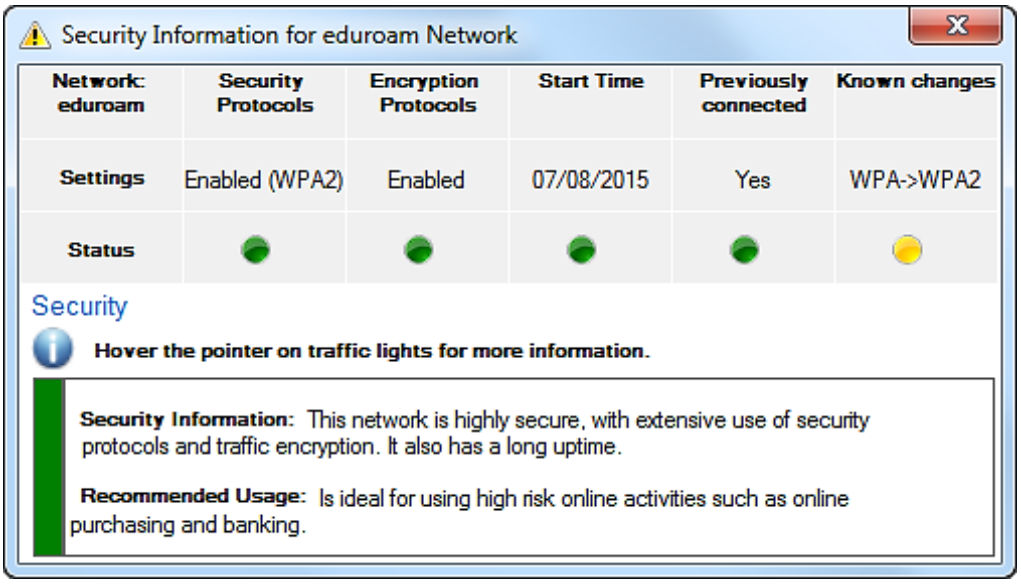

Figure 33: The security panel for the first Wi-Fi network in the third interface

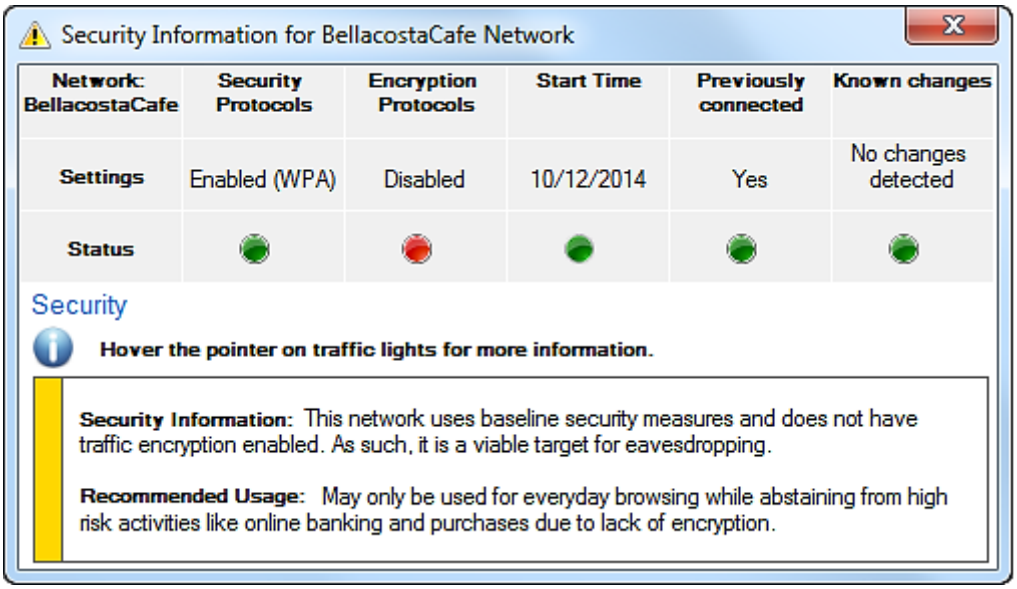

Figure 34: The security panel for the second Wi-Fi network in the third interface

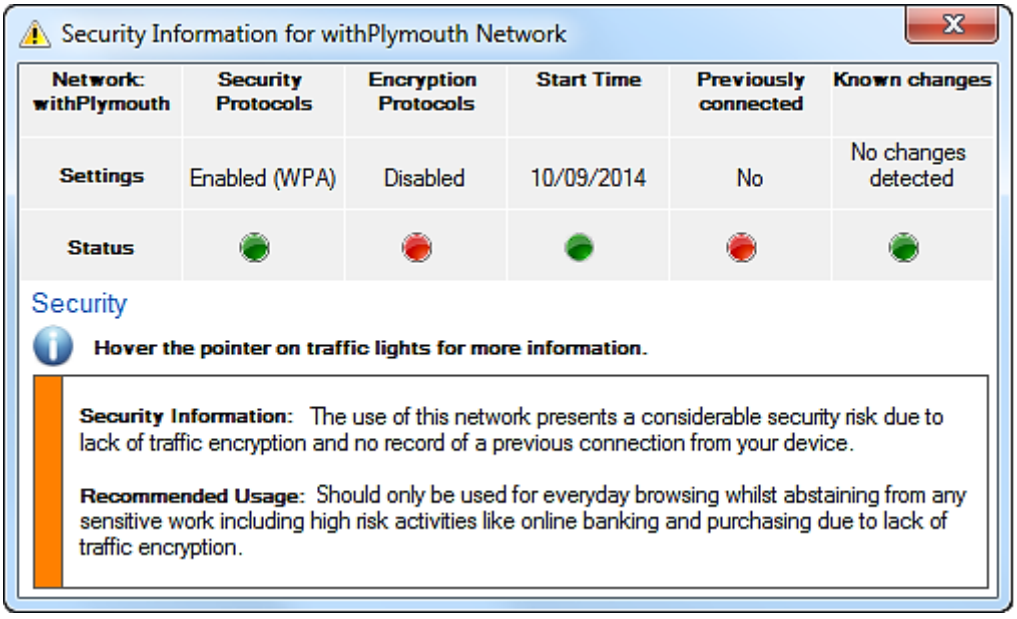

Figure 35: The security panel for the third Wi-Fi network in the third interface

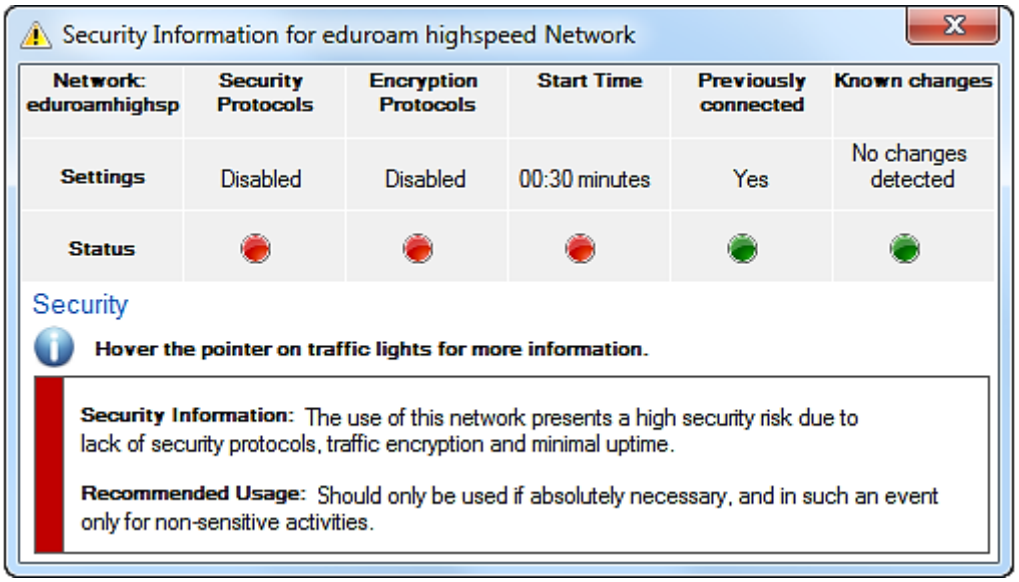

Figure 36: The security panel for the fourth Wi-Fi network in the third interface

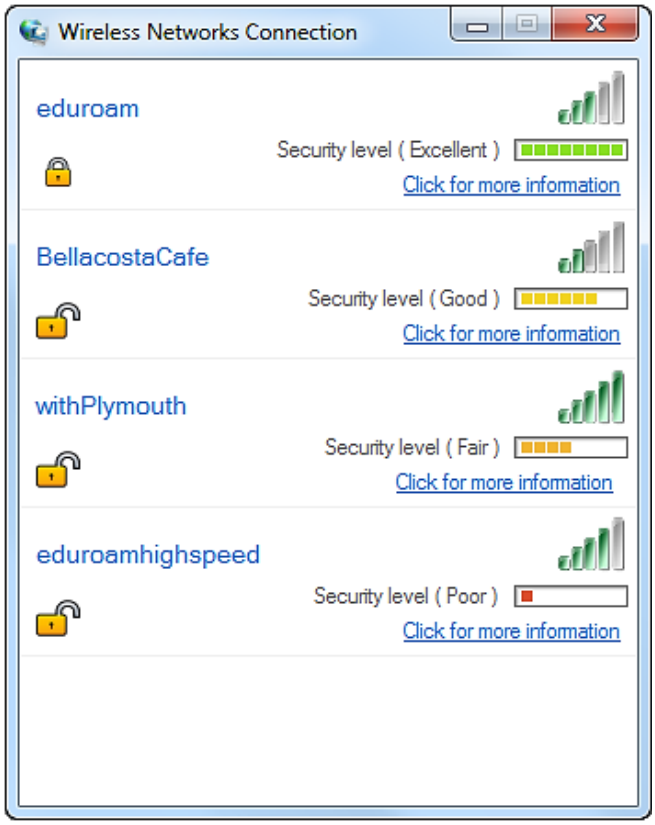

Figure 37: Fourth Wi-Fi interface - Advanced interface with security meter (Design 2)

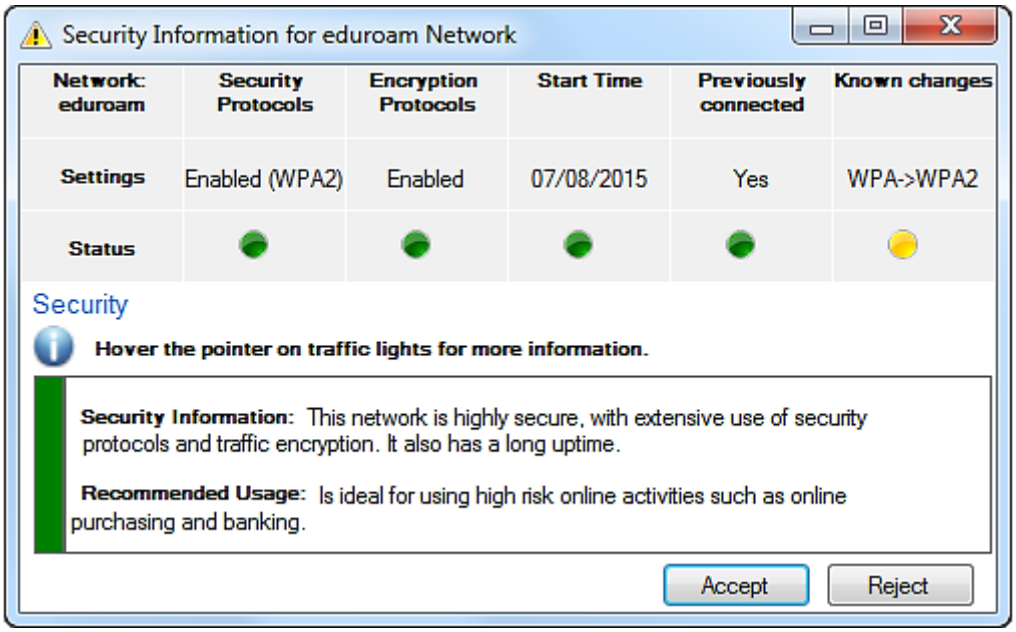

Figure 38: The security panel for the first Wi-Fi network in the fourth interface

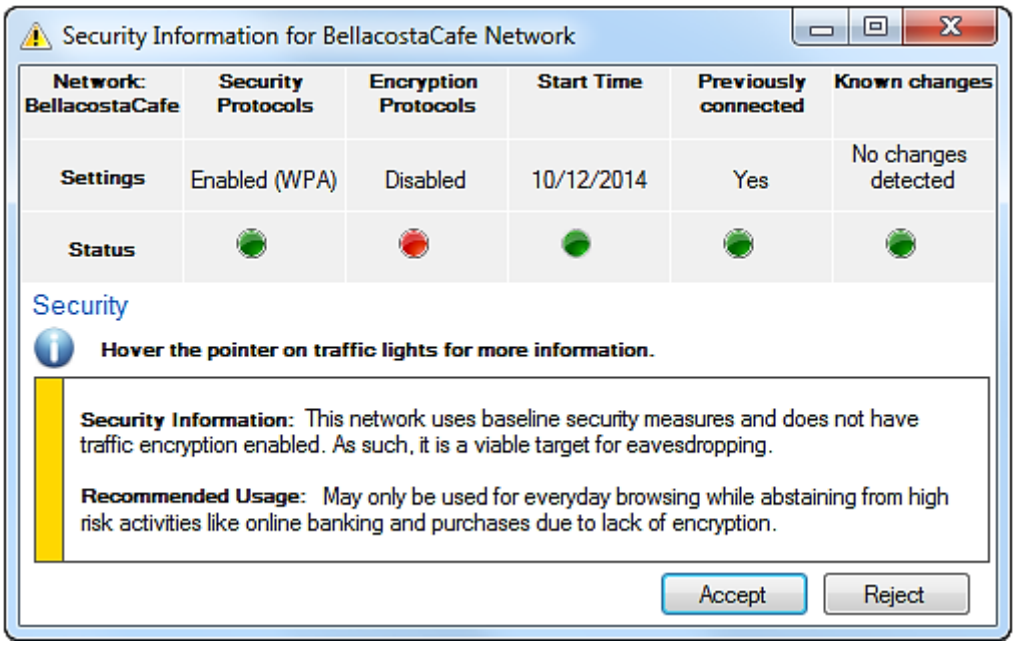

Figure 39: The security panel for the second Wi-Fi network in the fourth interface

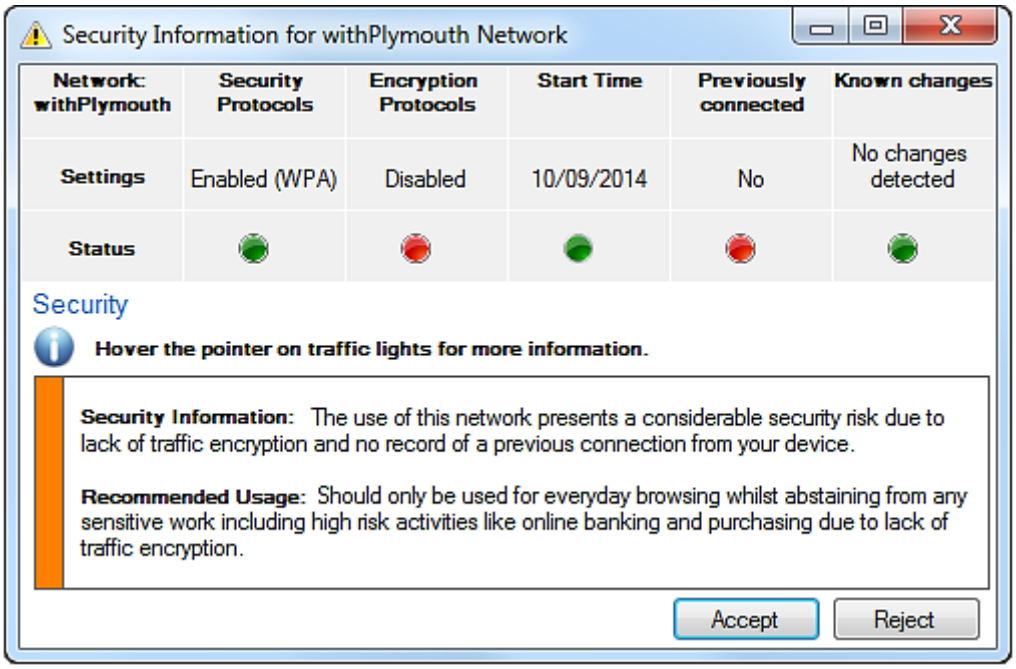

Figure 40: The security panel for the third Wi-Fi network in the fourth interface

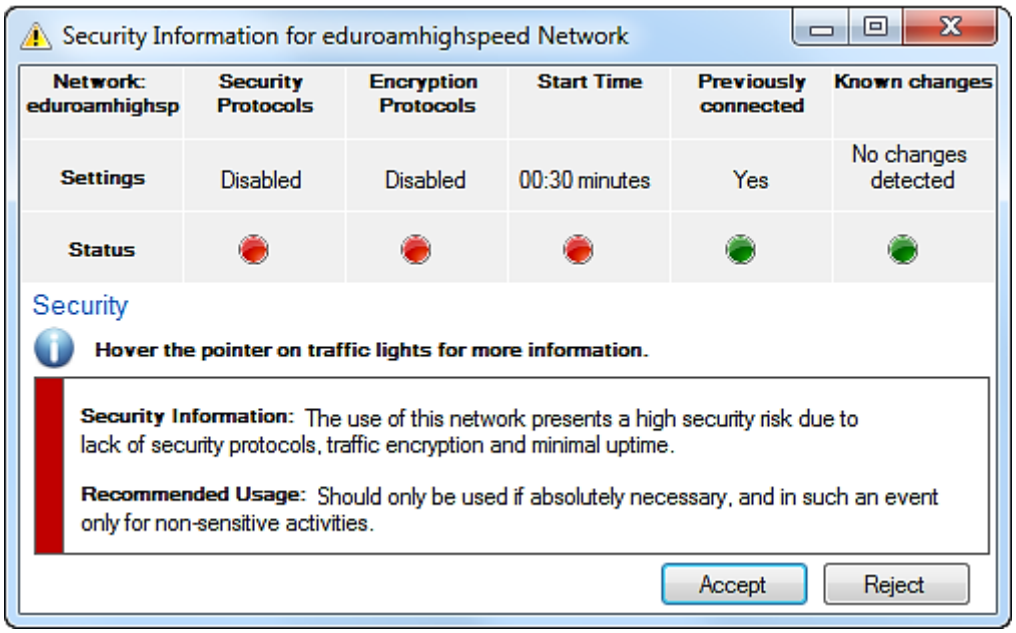

Figure 41: The security panel for the fourth Wi-Fi network in the fourth interface

4.4.3 Results

The participants' selection choices of the Wi-Fi networks of the four interfaces are presented in Figure 42. For the first interface, given that most participants are students and that the experiment was carried out within the university campus, it is not surprising that 60% of them selected the eduroam Wi-Fi as their first choice, as this is the network managed by the university.

Despite being unknown, 8% of the participants chose BellaCostaCafe after being unable to connect to eduroam with their credentials.

Because of its name, it was expected that the withPlymouth network would be within the main selection of the participants. The network is also managed by the university; however, it is intended for guests and therefore it only provides four hours of connection each day at no cost or authentication. It must also be noted that this connection does not use any encryption protocols, making it less secure than eduroam. Nevertheless, 20% of the participants chose this network as their first choice, whereas 24% of them selected this network after being unable to connect to eduroam.

Despite being unknown to participants and not within the networks managed by the university, the eduroamhighspeed network attracted 16% of the participants as their first choice and 28% of the participants as their second choice. The implied speed of the network clearly measured as a great factor on the influence of the selection, as participants chose this network on the basis that it is a high-speed connection, due to its nomenclature.

On the second interface, 76% of the participants selected the eduroam network as their first choice for the same reasons described previously. In contrast to the first interface, the warning message seems to make participants hesitant on connecting, as only 4%

of them chose the BellaCostaCafe as their second choice, compared to the 8% on the first interface. From these results, the impact of the design on the decision of the users can be recognised, as the warning message made the participants think more before selecting the network. Nevertheless, 4% of the participants chose this network as their third and fourth choice, raising some concerns on a small portion of the participants not paying enough attention to the warning message.

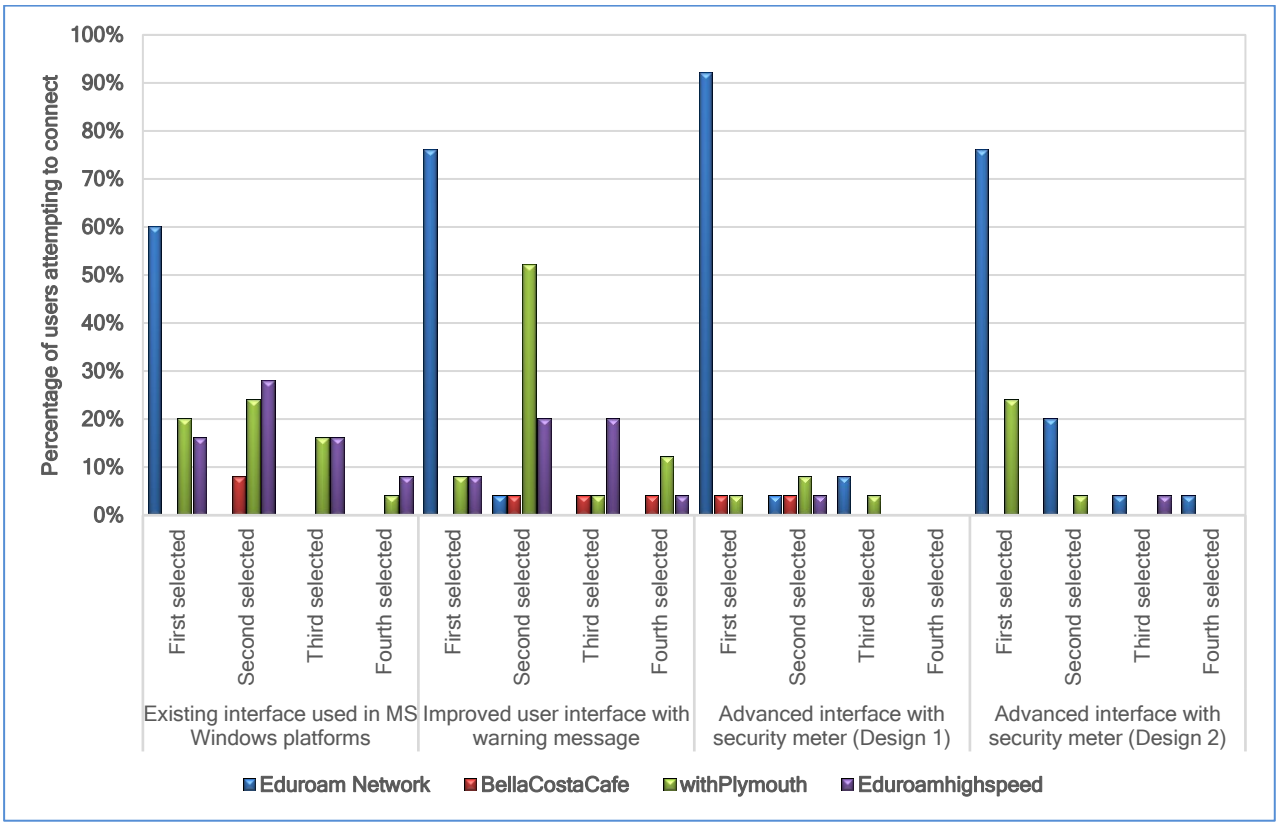

Figure 42: User's Wi-Fi network selections for the four interfaces

Likewise, 8% of the participants chose the withPlymouth network as their first choice and 52% selected as their second choice after being unable to connect to eduroam. As mentioned earlier, this network is within the main selections, as it is known to most of the participants.

Similar to the BellaCostaCaffe network, the eduroamhighspeed selection also showed signs of improvement, as only 8% of participants chose it as their first choice, as

opposed to 16% on the first interface. Despite this, 20% chose it as their second choice and third choice, compared to 28% and 16% on the first interface respectively, raising concerns over the name high speed influencing the choice of the user.

With regards to the third interface, 92% of the participants chose eduroam as their main choice. This is not surprising, as the full green security meter and the encouraging security information motivated participants to choose this network. On the other hand, this raises some concerns as the interface was designed to allow access without any authentication. The padlock was only to demonstrate that the network is secured, and to test whether users would recognize this flaw and the abnormal behaviour. Surprisingly, only one user detected this, whereas others did not recognize the flaw and continued to connect without any perception.

Regarding the BellaCostaCafe, the security meter and the advice message influenced the users on deciding to connect to the network and, as a result, only 4% made it their first and second choice equally. The impact of the security meter along with the security advice proves to be a better approach, as participants hesitate more to connect to unknown networks although the security meter shows that this network is the second-best network in terms of its security compared to the other presented networks, as opposed to the previous interfaces.

The withPlymouth network attracted 4% of the users to choose it as their first choice, 8% as their second choice, and 4% as the third choice. Alarmingly, this demonstrates that a small portion of participants trust the network by the name and therefore ignore the security warnings, despite being told that the connection is insecure. Looking at the results of eduroamhighspeed, none of the participants chose it as their first, third or fourth selection and only 4% selected it as their second choice. Although it highlights a big improvement compared to the previous interfaces, there are still reasons for

concern, as some users still selected it as one of their choices, despite being an unknown network and alarms being raised regarding its poor security.

For the fourth interface, 76% of the participants chose eduroam as their main choice compared to 92% in the third interface. Although the design of the fourth interface is quite similar to third interface, there were some users who selected withPlymouth over eduroam because it has a better signal taken into account that they are both trustworthy because participants are familiar with both networks.

With regards to the BellaCostaCafe Wi-Fi network, none of the participants selected this network although the security meter shows that this network is the second best network in terms of its security features based on the security information provided in the security information panel. This demonstrates that some participants tend to make their choices based on the familiarity of the network name but not of the security features the network.

In addition, 24% of the users made the withPlymouth network their first choice, whereas 4% made it their second. None chose it as their third or fourth selections. This shows a significant improvement over the previous interfaces, nevertheless, there is still some reason for concern, as many users still chose this network despite the security warnings, since they are familiar with the network name.

Regarding the eduroamhighspeed Wi-Fi network, there were a few participants who selected this network as their third choice and none of the participants chose this network as their first, second or fourth choice. Although this is a great improvement compared to what has been seen in the first and the second interfaces, it arguably shows that some people will ignore whatever advice is given.

4.4.4 Discussion and Findings

From the results described above, it was perceived that the name of the network has a significant impact on the participants when choosing an appropriate network to access the Internet within a known environment like the university campus. Results obtained from the experiment revealed that in the absence of security information, users are very prone to connecting to names that look like a known name.

As presented in Figure 42, a considerable number of the participants in the first, second, third and fourth interfaces have chosen to connect to the eduroam Wi-Fi network as their first choice. This was driven by the recognition of the Wi-Fi network, as it is the mainly used Wi-Fi network in the university campus. When participants were asked what their reasons were for choosing the eduroam as their first choice, their answers were because they are familiar with the name within the university campus and considering the network name, it indicates that it is run and managed by the university and therefore it is trustworthy. It seems that the users greatly trust the location as an assumption that there is a correlation between the network name and location. For example, students and staff within an academic environment have become accustomed to the fact that the eduroam Wi-Fi network is run and managed by the university and hence it is a trustworthy network. However, it is well known that the network name can be modified to any name or spoofed which indicates the confidence of the users in the network name could be interpreted as a lack of knowledge of this security issue.

This reflects the lack of security awareness for the participants regarding the possibility of falling victim of a spoofed network. In a wider setting, in places such as shops and shopping malls, restaurants and cafes, where the user will focus only to get access to a free Wi-Fi and will be looking to any network that has partly or totally the name of the

place within the users range like the name of a shop, restaurant or cafe, this increases the possibility of the users falling victim to deception and getting access to spoofed Wi-Fi networks.

In addition, it appears that claimed signal strength is also a persuading factor, especially if the Wi-Fi network name includes an indication that it is a high-speed Wi-Fi network. This explains the selection of 16%, 28% and 16% of the participants to eduroamhighspeed network, who tried the first interface as their first, second and third choice respectively. Similarly, with the second interface 8%, 20% and 20% of the participants who tried the second interface choose this Wi-Fi network as their first, second and third choice respectively. The large proportion of the participants who have selected the eduroamhighspeed network, as seen in the first and second interfaces, reflects the extent of the danger which could be exposed to these users because of their lack of knowledge in the associated risks of unknown Wi-Fi networks, and the extent of the damage that they may be subjected to when connecting to fraudulent Wi-Fi networks. More importantly, this proves that the first and the second interfaces have limited capabilities in providing the required security guidance and feedback to participants to allow them to choose the most appropriate Wi-Fi network.

However, as few as 4% participants chose the eduroamhighspeed Wi-Fi network as their second choice with the third interface and same chose this Wi-Fi network as their third choice with the fourth interface which proves that the advanced interfaces with security meter (Design 1 and 2) have educated users and made them aware of the security risks associated with use of this unknown Wi-Fi network. This proves that users are influenced if suitable security guidance and visible feedback is provided at the point of need to help the users to make the right decision at the right time to avoid security risks associated with risks of using unknown Wi-Fi networks.

This has also highlighted the fact that some participants access Wi-Fi networks that provide greater speed rather than focusing on the security aspects of the Wi-Fi networks. This demonstrates that the need for internet speed, in the eyes of a few participants, sometimes outweighs the security concerns.

Moreover, it was also observed during the experiment that the participants interacted with the second interface with disinterest when the warning message popped up, as some of them read the warning message without giving it enough consideration and then clicked either the "*Accept*" or the "*Reject*" button, while others dealt with it quickly without reading its content or without paying any attention to the message. This perhaps is due to the fact that it was the first time participants perceived such a warning message when they tried to connect to Wi-Fi network using the MS Windows platform.

It was also perceived during the experiment that since it is often difficult for users who have a limited knowledge of computer systems to understand the security issues and concerns of Wi-Fi networks, most users will simply connect to the network with the greatest signal or the greatest speed and will not look into the security details. Additionally, participants' interactions with the four interfaces showed that they intend to connect to the next best network in terms of speed or best signal if they could not access the more secure one. For example, one of the participants commented: "*I wasn't able to connect to the preferred secure network, so I connected to the network with the best signal that was unsecured*".

The new design of the interfaces with the security meter and the information security panels that provides information and recommended usage for the users about the Wi-Fi networks, has proven to be a promising approach in providing adequate information for the users before they make their decision, educate and make them aware of the security implications before connecting to insecure Wi-Fi hotspots in public areas. Only

4% of the participants who tried the third interface selected the network that has poor security “eduroamhighspeed” as their second choice and only 4% of the participants who tried the fourth interface selected this network as their third choice. Participants made their decision on the basis that it is a high-speed Wi-Fi network as its name implies.

Moreover, it should also be mentioned that the name of the network is still a vital fact that keeps influencing the participants when selecting the network especially if the name of the network is known to the users and is seen in the environment they are familiar with. This is obtained from the results of the third and the fourth interfaces. For example, the network named “withPlymouth” is well-known to the participants within the university campus and it has been designed in the experiment to have a fair level of security in the third and fourth interfaces, however, 8%, 52%, 4%, 12% of the participants who tried the third interface selected this network as their first, second, third and fourth choice respectively. Similarly, with the fourth interface, 24%, 4% of the participants who tried the fourth interface selected this network as their first and second choice respectively.

4.4.5 Post-Experiment Participant Feedback

To evaluate the four tested interfaces in the experiment, it was essential to create four questionnaires. However, there are some questions, which apply to the full population of participants and other questions vary according to the specific subgroups from the variants of the trials. Therefore, some of the questions are designed to conform to the interface used. For example, the first interface is designed to simulate the interface used in Microsoft Windows 7 platform. The second interface is designed to include some of the differences and improvements, such as, when the user clicks the “*Connect*” button a warning message will be raised which tells the user that “The

information sent over this network might be visible to others" and allows the user to either "*Accept*" or "*Reject*" the connection based on this message. The third interface, which is the most different and improved in terms of containing a security meter indicator that shows the extent of the Wi-Fi network security and also gives the user a chance to click on a link to acquire more information to see the "*Security information*" and "*The recommended usage*" of the selected Wi-Fi network and the fourth interface which is designed similar to the third interface with the only diverse that users will see the security panels if they either clicked on the link "*Click for more information*" or if they clicked on the button "*Connect*" and in the latter case users would have the choice to either "*Accept*" or "*Reject*" to connect to the selected network. To properly analyse the results, participants were divided randomly into four groups, group (A) which have used the Existing interface in MS windows 7 platform, group (B), which have used the improved user interface with a warning message, group (C); which have used the Advanced interface with a security meter (Design 1), and group (D), which have used the Advanced interface with a security meter (Design 2).

4.4.6 Participants Feedback and Analysis

Our subjects consisted of males and females as Figure 43 shows. The vast majority were students from Plymouth University excluding the School of Computing, Electronics and Mathematics, as the target was only users with average computer skills.

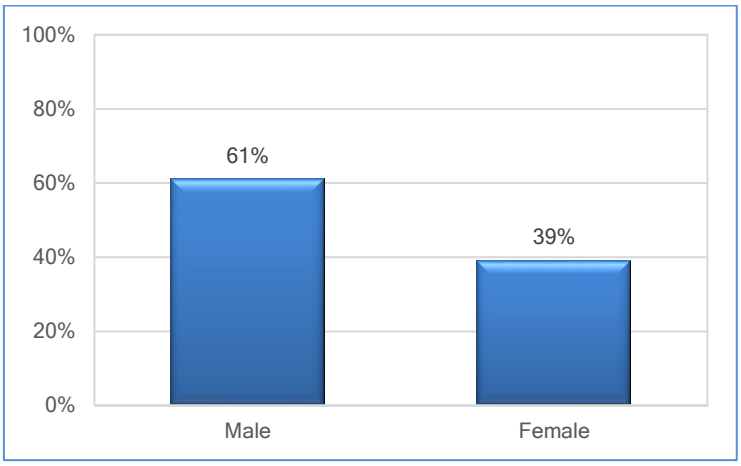

Figure 43: Participants gender

Figure 44 presents the age groups of the participants. The vast majority of population of the participants were aged between 18-59 years old.

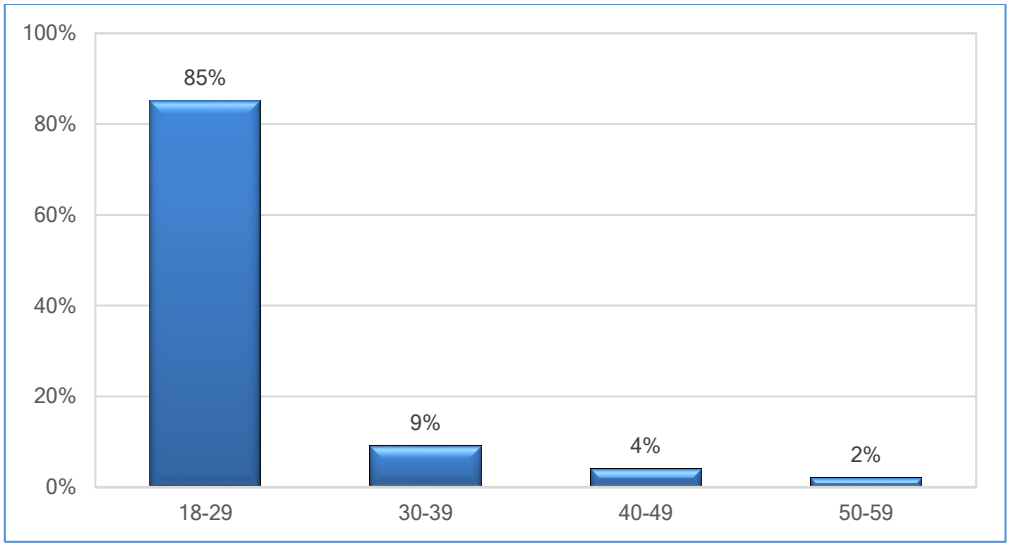

Figure 44: Age groups of the participants

Participants were asked whether the instructions for conducting the experiment were suitably clear to ensure that the participants understood the experiment and participated in the experiment correctly. Figure 45 shows the participants' agreement on the clarity of the instructions provided for conducting the experiment. The results reveal that a substantial proportion of the participants understood the experiment

procedure which demonstrates that the experiment procedures were carried out with minimal errors.

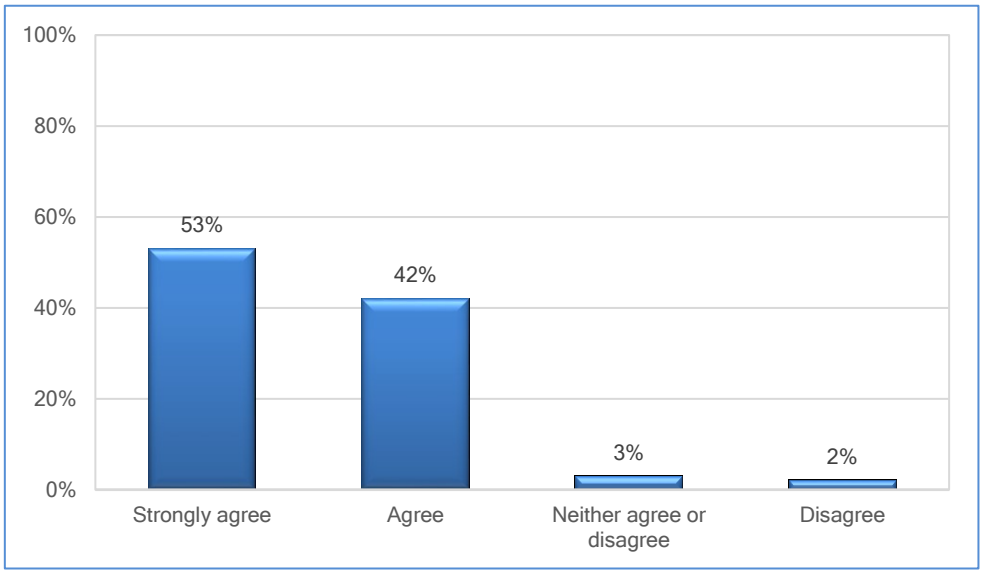

Figure 45: Participants agreement of the clarity instruction provided for the experiment

Moreover, participants were asked to what extent they feel that they followed the instructions. Figure 46 shows the extent to which participants followed the instructions for the experiment. The results demonstrated that the most of participants followed the instructions fully or moderately to conduct the experiment. This can be interpreted as a direct result of their understanding of the procedures of the experiment.

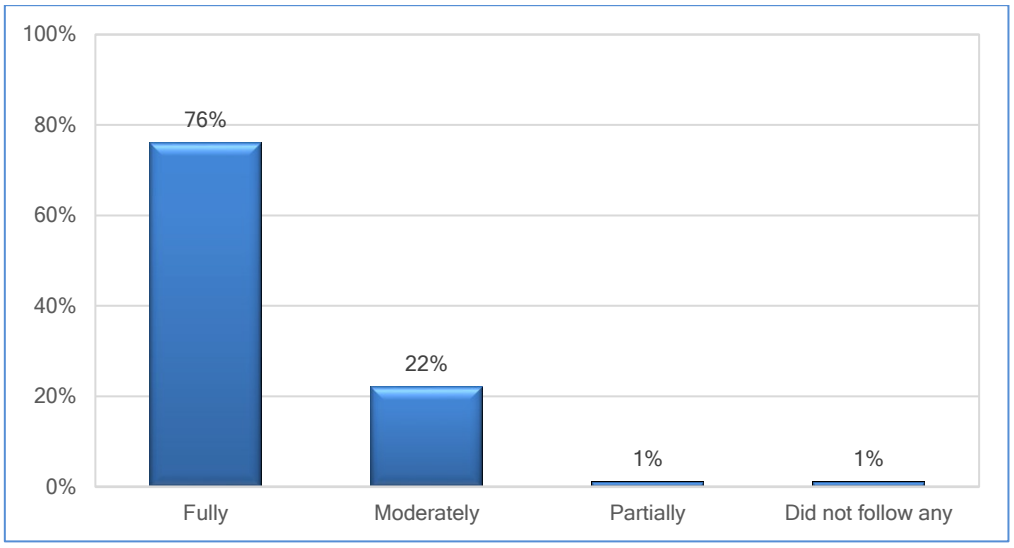

Figure 46: The extent of participants following the instructions in the experiment

The entire population of the participants were asked regarding the use of Wi-Fi at home, public areas and at work. Figure 47 shows the frequency of using Wi-Fi by participants at home, public areas and at work. The fact perceived here is that there is a considerable proportion of the participants (36%) who are using public Wi-Fi hotspots in the public areas on a daily basis, and this reflects the popularity of using Wi-Fi in public areas. This is perhaps because of the high demand of accessing the Internet and online services while people are on the move. This also reveals that a considerable number of the participants are opting for public Wi-Fi as an inexpensive alternative or sometimes free connection to *3G* or *4G* connectivity. The increasing use of Wi-Fi hotspots at the expense of wireless networks would further complicate the security landscape of mobile IT for businesses and individuals equally. Furthermore, this highlights the imperative need to educate and make the users aware of the existing security implications of using unknown Wi-Fi hotspots in the public areas that have no security features or no protection at all. The results published by (Kaspersky Lab, 2016; iPass 2016a and iPass 2016b) show that people use Wi-Fi in public areas without proper precautions, increasing the risk of theft of their confidential information by cyber attackers.

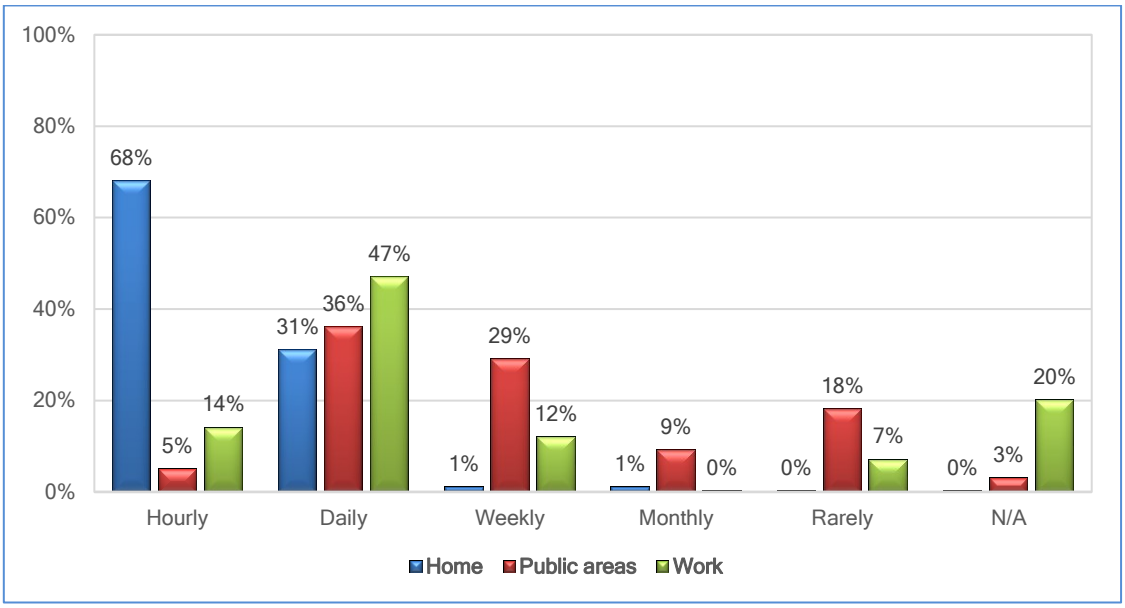

Figure 47: The frequent of using of Wi-Fi at home, public areas and work

Considering the use of Wi-Fi at different places including home, public areas and at work, all participants were asked how frequently they perform a range of tasks and activities including checking email, online banking, social networking, bookings, buying/selling goods, and other uses. Figure 48 presents the range of tasks and the frequency of performing these tasks by the participants using Wi-Fi at home. It is not surprising, that almost all the participants would use and trust the connection at home because they own the routers that are supplied by ISPs and the Internet connection is protected with a password. The Wi-Fi connection at home is protected and equipped with security features such as security and encryption protocols to protect customers from cyber threats to potentially penetrate customers' home network.

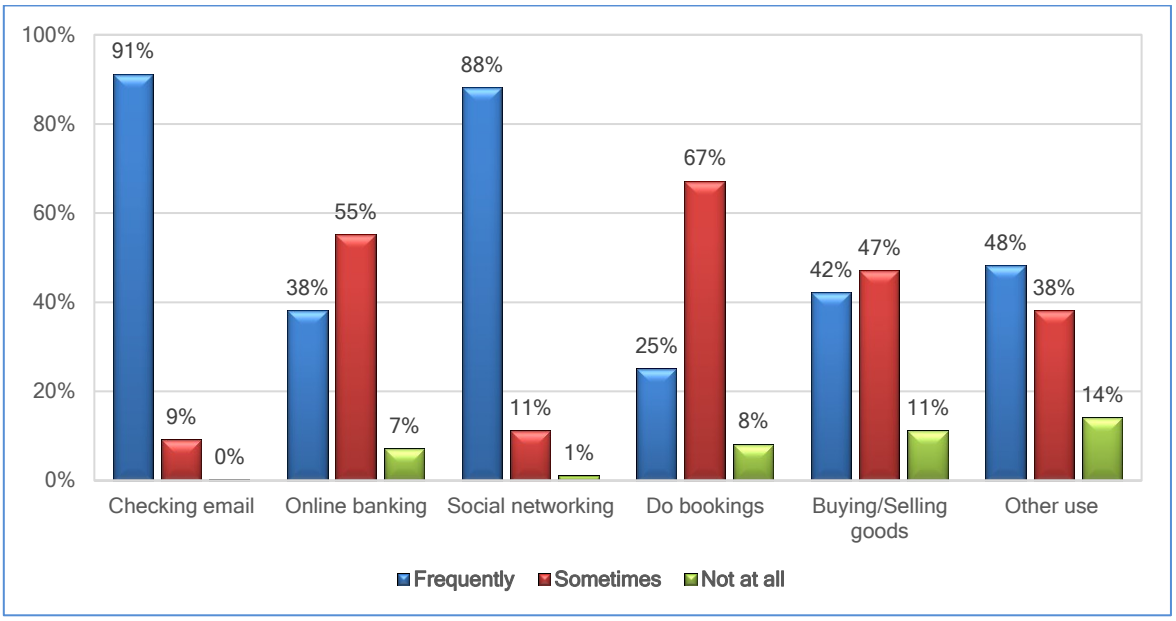

Figure 48: The range of tasks participants perform using Wi-Fi at home

The results in Figure 49 show that a large number of participants are using the Wi-Fi hotspots in the public areas to access their emails, which indicates that participants are unaware of the security risks and the security implications that are associated with the use of unknown Wi-Fi hotspots in the public areas to access their emails, which mostly are not using encryption features leading them vulnerable for interception. This emphasizes the need to increase the security awareness of users with respect to providing security advice to them regarding the security risks associated with the use of Wi-Fi networks in public areas especially unknown ones before they connect to any Wi-Fi network in a public area. Particularly, the Wi-Fi networks in public places cannot be trusted, in addition to the inability to verify them and users cannot know who manages these Wi-Fi networks.

Similarly, regarding the usage of Wi-Fi in public areas for accessing online banking, it is very worrying that relatively large number of the participants stated that they are using Wi-Fi at public areas for online banking, which will increase the probability of these participants to become victims of spoofed Wi-Fi networks.

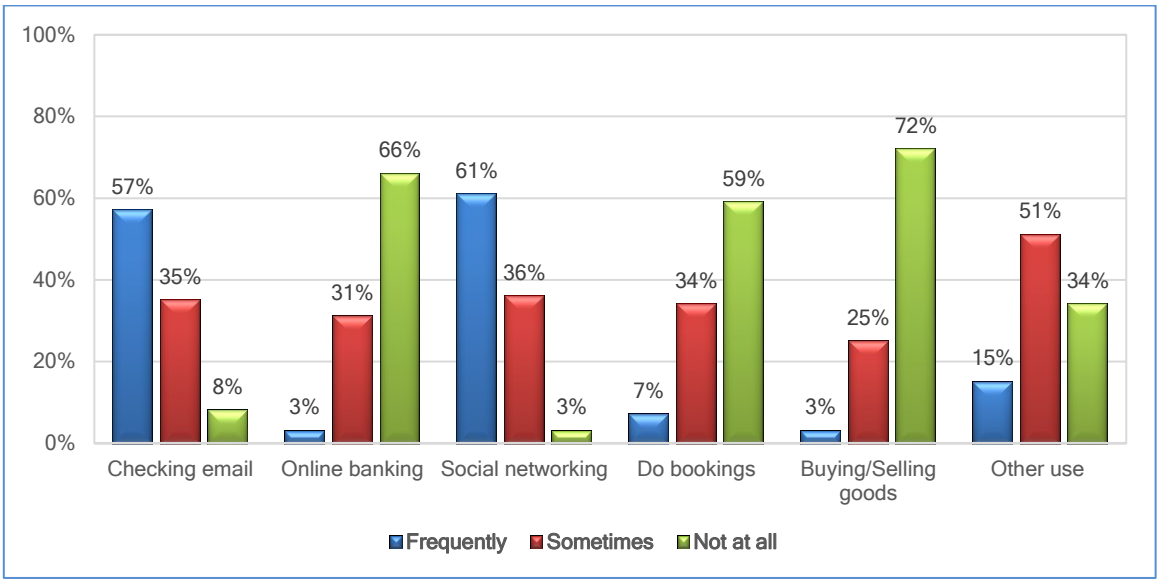

Figure 49: Type of tasks participants perform using Wi-Fi at public areas

Figure 50 presents the range of tasks and the frequency of performing these tasks by the participants using Wi-Fi at work. As witnessed before, it would not be surprising that participants would use and trust the use of Wi-Fi connections at their work place since it the Wi-Fi hotspots would be managed by the company they work for. However, the security implications would still exist if the Wi-Fi connection is not protected with a password and proper precautions should be taken by users if the Wi-Fi connections is not protected in their work place.

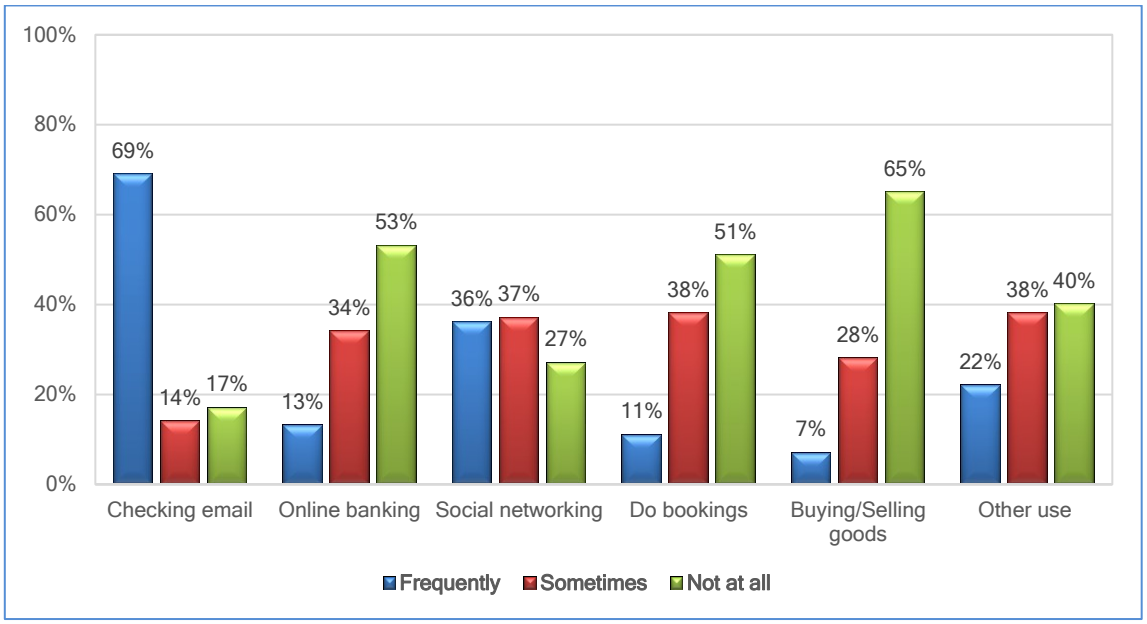

Figure 50: Type of tasks participants perform using Wi-Fi at work

Moreover, participants were asked if they know the difference between secured and insecure Wi-Fi networks as shown in Figure 51. The chart demonstrates that only 40% of the participants stated that they know the difference between secured and insecure Wi-Fi networks and the other portion, 61% of the participants, are either uncertain about the difference between the secure and insecure Wi-Fi network or have no adequate information about the differences between the secured and insecure Wi-Fi networks. This large proportion of participants highlight the possibility of a large number of users to become victims of spoofed Wi-Fi networks. This increases the importance and need to provide adequate security information about the security implication of the use insecure Wi-Fi networks to users before they decide to connect to any especially if the Wi-Fi network is unknown to them.

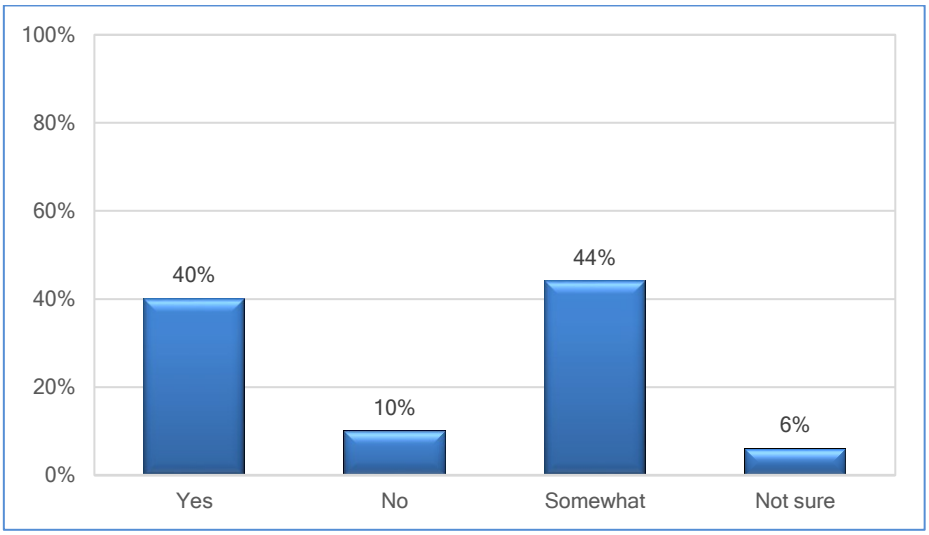

Figure 51: Participants' knowledge of the difference between secured and insecure Wi-Fi networks

Statistics in Figure 52 presents the level of the participants' awareness of the security risks associated with the use of insecure Wi-Fi networks. The results here, corresponding to previous findings, demonstrate that 61% of the participants are either uncertain about the risks, have no adequate information, or impetuous about security risks associated to the use of Wi-Fi networks. This illustrates the imperative need to provide a new way to increase the security awareness of users about the security risks associated with the use of Wi-Fi networks, especially if it is unknown and specifically if it is in public areas. Participants who have tried the second interface (Group B), the third interface (Group C), or the fourth interface (Group D) were asked if they think the full implementation of the software can be used to facilitate users in choosing the appropriately secure Wi-Fi network, as shown in Figure 53.

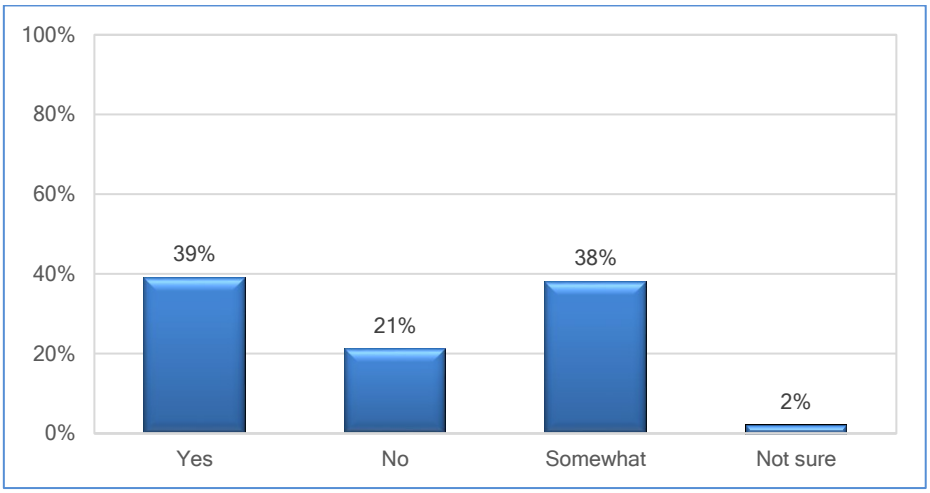

Figure 52: Participants' awareness of the security risks associated with insecure Wi-Fi networks

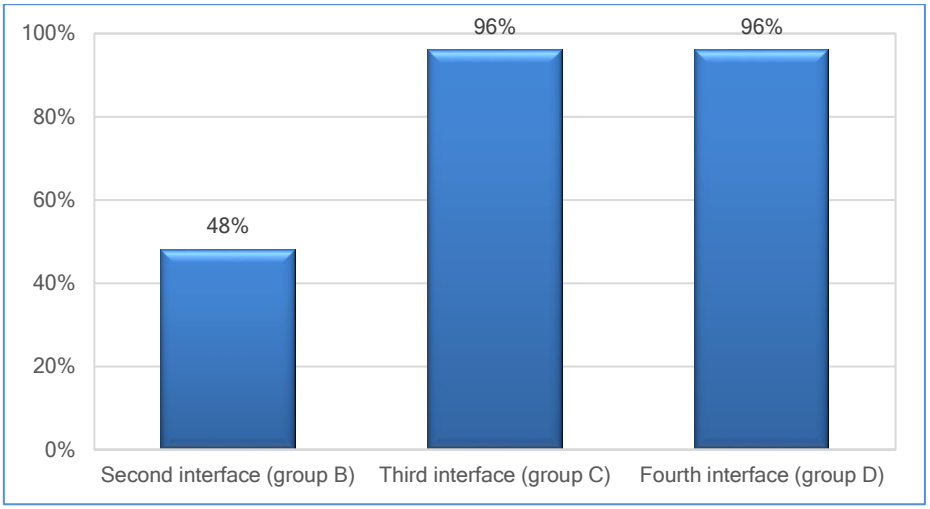

Figure 53: Participants agreement with user Wi-Fi network selection in view of full software implementation

In comparison, between the three interfaces, it appears that the third and fourth interfaces excel the second interface. Although the participants are not the same, presumably the features of the third and the fourth interfaces, such as the security meter, the panels with the security information and recommended usage, make the difference as more participants agreed on that the full implementation of the software can be used to facilitate users in choosing the appropriately secure Wi-Fi network, as opposed to the percentage of users that used the second interface. Participants who have tried the first interface were not asked this question because the first interface

was designed to simulate the existing Wi-Fi that is used in MS Windows platforms and has no additional features compared to the other three interfaces.

Participants were also asked if they considered the security aspects of the Wi-Fi network when they made their decision. Results in Figure 54 demonstrates that the number of participants who tried the third and the fourth interfaces, who considered the security aspects of the Wi-Fi network when they made their decision, is higher compared to number of participants who tried the first and the second interfaces. Probably this is due to the fact that the new design of the third and the fourth interfaces provided more presentable security information that is adequate, easier to understand the key security characteristics of the Wi-Fi networks, compared to the design of the first and second interfaces, which consequently helped towards nudging participants to consider the security aspects when connecting to Wi-Fi networks.

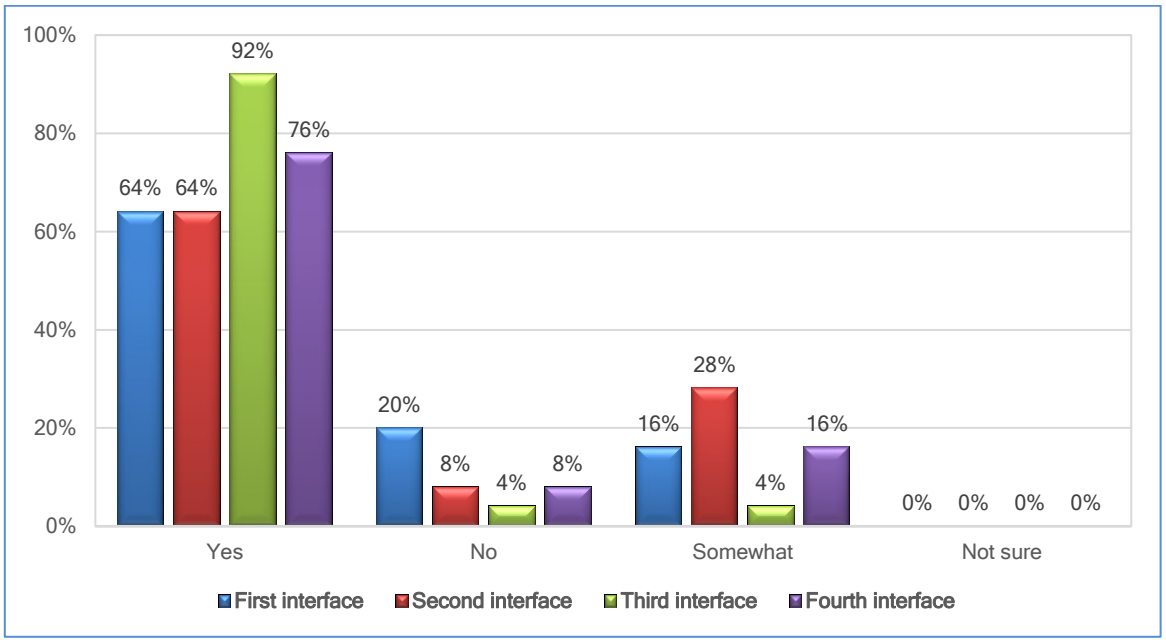

Figure 54: Participant Wi-Fi network selection considering security aspects

All participants' who answered the above question with "Yes", were also asked accordingly if they felt that they had enough information to make a decision about

whether the network was safe/trustworthy or not. Figure 55 shows the results for each group according to the interface they tried. It is not surprising, that most of the participants who tried the third and the fourth interfaces stated that they had enough information to make a decision, compared to the participants who tried the first and the second interfaces. As observed earlier, perhaps this is due to the features that the third and the fourth interfaces have such as the security meter and the security panels with the security information and recommended usage, which makes the difference clear here in terms of participants' satisfaction with the availability of adequate information that helped them make their decision.

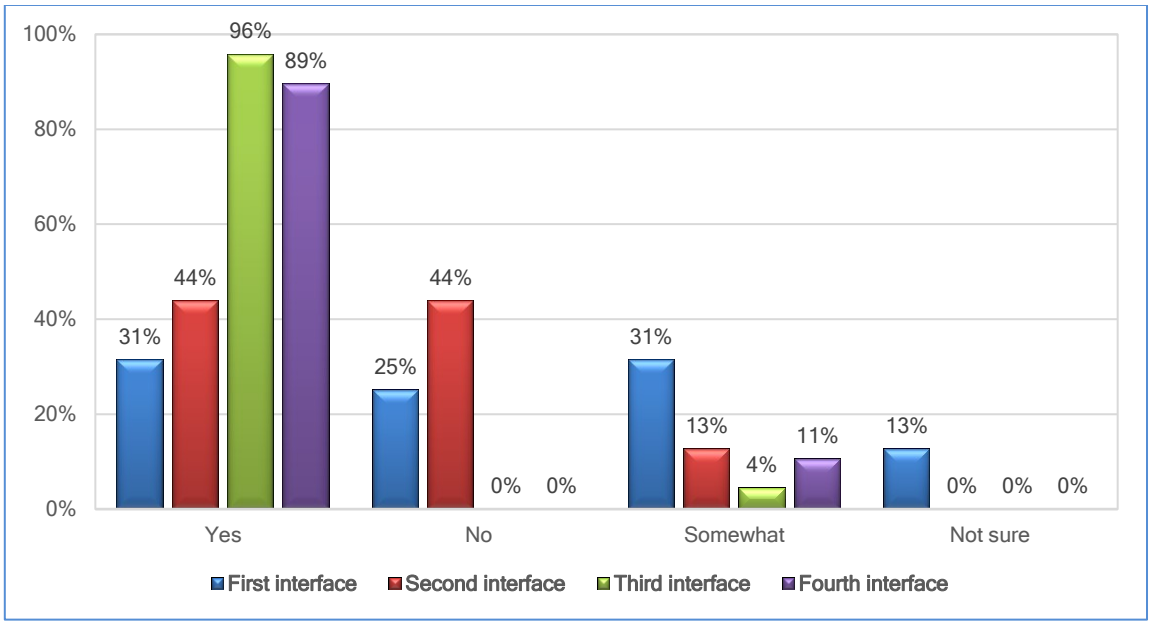

Figure 55: Participants' opinion on network being safe/trustworthy

Participants were also asked what are the features they looked at when making their decision. This question was structured according to the security features of the networks that each interface is presenting to the user when exploring the available Wi-Fi networks. For example, the first interface is only presenting a pop-up window that has a basic information when the user points the pointer at the explored network, similar to what is currently used in Microsoft Windows 7 platform. The second interface is also being designed similarly. Therefore, Figure 56 is only presenting the results of

the participants who tried the first or the second interface. The results show that the name of the network was the most important security feature in the view of participants who have tried either the first or second interface. As per earlier findings, in the absence of the security guidelines and information in the Wi-Fi networks, it is not surprising that users will be very inclined to connecting to known names. This also confirms that in the absence of sufficient and important security information that is easy to understand, participants will rely heavily on the name of the network when choosing instead of others, even if this network is less secure or it has no security features that protect user data and information. In contrast, there was smaller number of participants who stated that they looked at the security feature of using the security protocols and the security features of using the encryption protocols. In addition, it is very worrying, that there were 16% of the participants who tried the first interface and 20% of the participants who tried the second interface, stated that they did not look at any of the security features of the Wi-Fi network when they made their decision. This indicates that a reasonable portion of users paying no attention to the security at all and perhaps unfamiliar with threats posed while on the move. This is a major security challenge and an obstacle to using Wi-Fi networks securely for both individuals and companies while on the move.

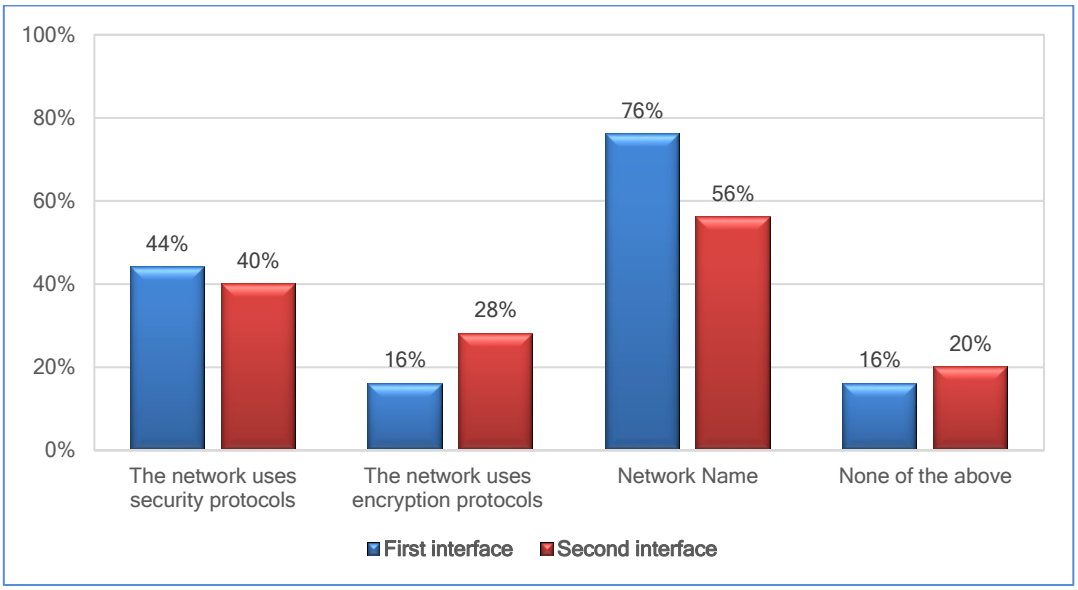

Figure 56: Types of the security features participants' looked at when deciding on Wi-Fi networks selection (the First or the Second interface)

Similarly, participants who tried the third and fourth interfaces were also asked what are the security features did they looked at when they made their decision. Figure 57 shows the results. Both interfaces were designed with improved information security panels that have security information about available Wi-Fi networks and recommended usage. In addition, both interfaces are also having security meters that determine the security level for each presented Wi-Fi network within the interface. For this reason, the participants who tried these interfaces were asked about additional security features as presented to them with the third and the fourth interfaces. In other words, in both interfaces, the security panel was designed to display additional security information about the explored Wi-Fi network such as the start time of the network and whether it has been previously connected. Compared to what is seen in the first and third interface regarding the importance of the network name for the participants, the network name was less important to participants who tried the third or the fourth interface, which indicates that the new design has influenced the users' perceptions when connecting to Wi-Fi networks. In addition, there was a larger number of

participants who tried the third and the fourth interface and stated that they looked at the security feature of using the security protocols and the security feature of using the encryption protocols, compared to what is seen in the first and the second interface. This shows that the new design provides improved security information and advice, which helps in persuading and encouraging users to look at the important security aspects of Wi-Fi networks when selecting Wi-Fi networks. In regard to the security feature of whether the network has been connected, over a third of the participants for both interfaces indicated that they looked at this feature. This is noticeably indicating that participants will appreciate seeing the history of whether the network has been previously used or not. Furthermore, this perhaps will nudge users towards thinking securely when connecting to a new/unknown network and will consequently make them less vulnerable of falling victim to deception, and getting access to spoofed Wi-Fi networks. Nonetheless, the start time has not been given enough appreciation by the participants as a security feature that they should look at. This can be interrelated as participants did not experience this feature in all platforms that are accustomed to use, whether computers or mobile phones. This also evidences the fact that participants do not realize the existence of deceptive Wi-Fi networks or are unaware of the potential of falling victims to portable networks that can be easily constructed and fully controlled by cybercriminals and deployed in the public areas. This generally raises serious concerns about the risks that can be exposed to the users of unknown and potentially insecure Wi-Fi networks that are widely spread nowadays in public places.

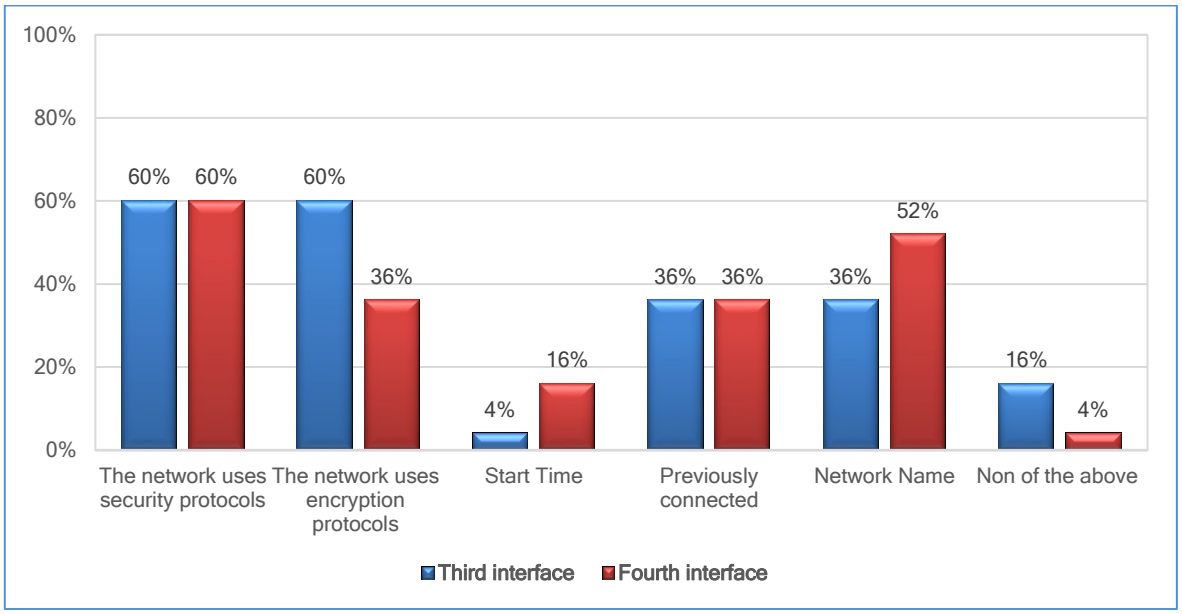

Figure 57: Security features reviewed by participants selecting third or the fourth interface

Figure 58 shows the results of the answers of participants whether the Wi-Fi connection they selected was secure or not, according to the interface they tried. Results demonstrate that most of the participants who tried the third or the fourth interface were quite confident that they know whether the Wi-Fi connection they selected was secure or not. In contrast, participants who tried the first or the second interface were less confident. This is perhaps due to the security guidelines, the security information supported with the security meter that the third and the fourth interface provided to the participants, which was simple and easy to understand with less technical terminology that most users would not necessarily understand. This perhaps helped the participants to comprehend the security level of the networks displayed within the interface and increased their confidence in knowing whether the Wi-Fi network they selected was secure or not. On the other hand, in the lack of the availability of security guidelines and the security information in the first and second interface led to users finding it difficult to see whether the Wi-Fi network is secure or not and hence hindrance to making a better security driven-decision and what is the kind of activities should they use it for if they decide to contact with it.

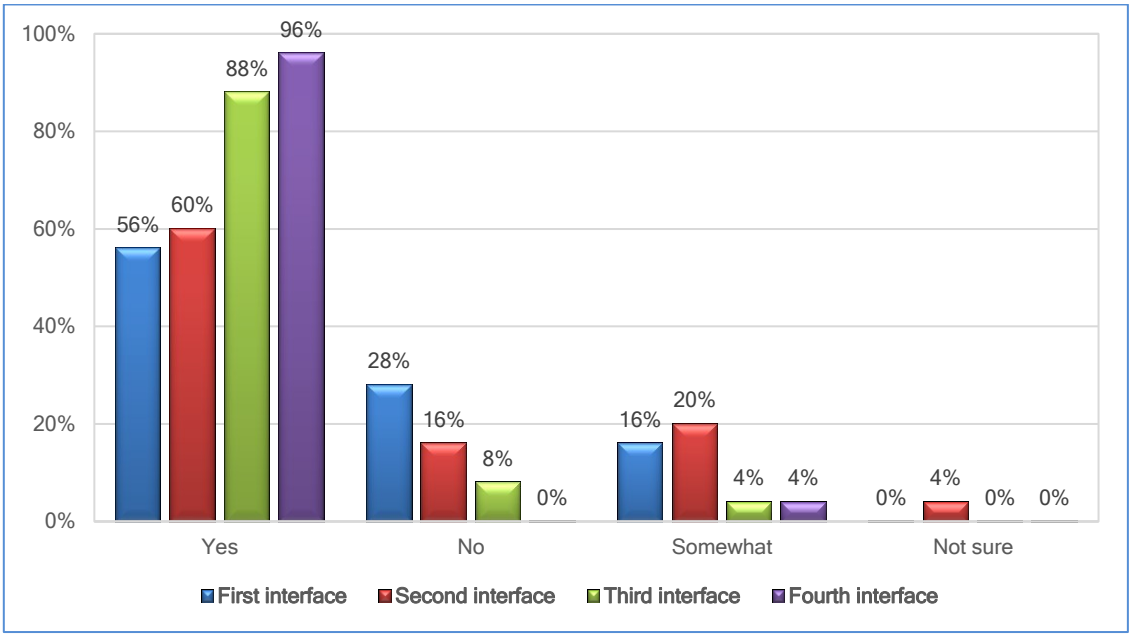

Figure 58: The level of participants' knowledge about Wi-Fi connection security

All groups of the participants were asked how concerned they are when connecting to unsecured Wi-Fi, the results in Figure 59 illustrate that 43% of participants were slightly or not at all concerned when connecting to unsecured Wi-Fi hotspots. These results demonstrate that a relatively substantial number of Wi-Fi hotspot users either pay no attention to the security problems associated with using Wi-Fi hotspots in public areas or unaware of the existence of these problems. This emphasizes the urgent need to deploy solutions that helps in making users aware of the security implications of connecting to insecure Wi-Fi hotspots. This can be achieved by developing better solutions that provide security information, supported with a recommended usage to make users aware of the implications of connecting to insecure Wi-Fi networks, nudge users towards security and consequently help them to protect their devices and the data stored on their devices while on the move.

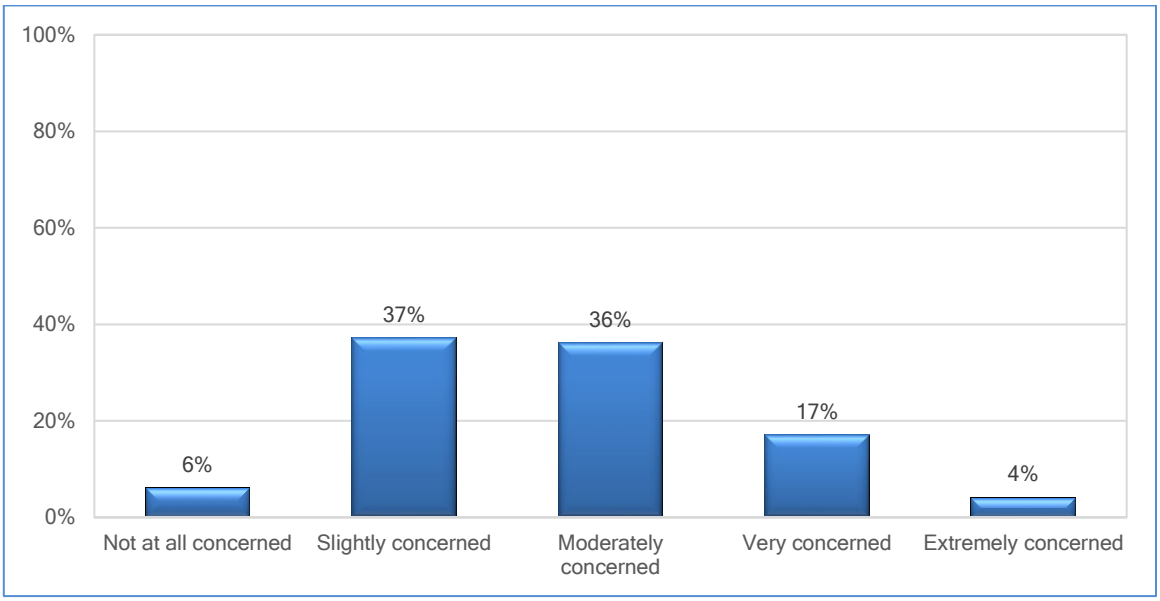

Figure 59: Particpants' Level of concern when connecting to unsecured Wi-Fi

All groups of the participants were asked to rank the security features that a user must take into account before using Wi-Fi hotspots, based on their point of view. This was including the security protocols and encryption protocols, in addition to the network name. Figure 60 presents the participants' opinions in this regard. There was just over 90% of participants who claimed that it is very important or important that network uses the security protocols, and more than 80% claimed that it is very important or important that the network uses the encryption protocols, while over 55% claimed that the network name is very important or important. Results also show that the participants' views on this aspect did not correspond to their interactions with the interfaces during the experimental study, especially for the participants who tried the first and the second interfaces, where it was observed that most of the participants' choices were influenced either by the network name, speed or signal strength. Nevertheless, the percentage of those who claimed that the network name is very important or important as a reliable security feature for the Wi-Fi network is still very high. This is worrying, as more than half of the participants are likely to be victims of a spoofed Wi-Fi network simply due to their reliance on the name of the network, where cybercriminals can deploy fake Wi-Fi

networks that be very similar or identical to the name of any known network in a known location to target users.

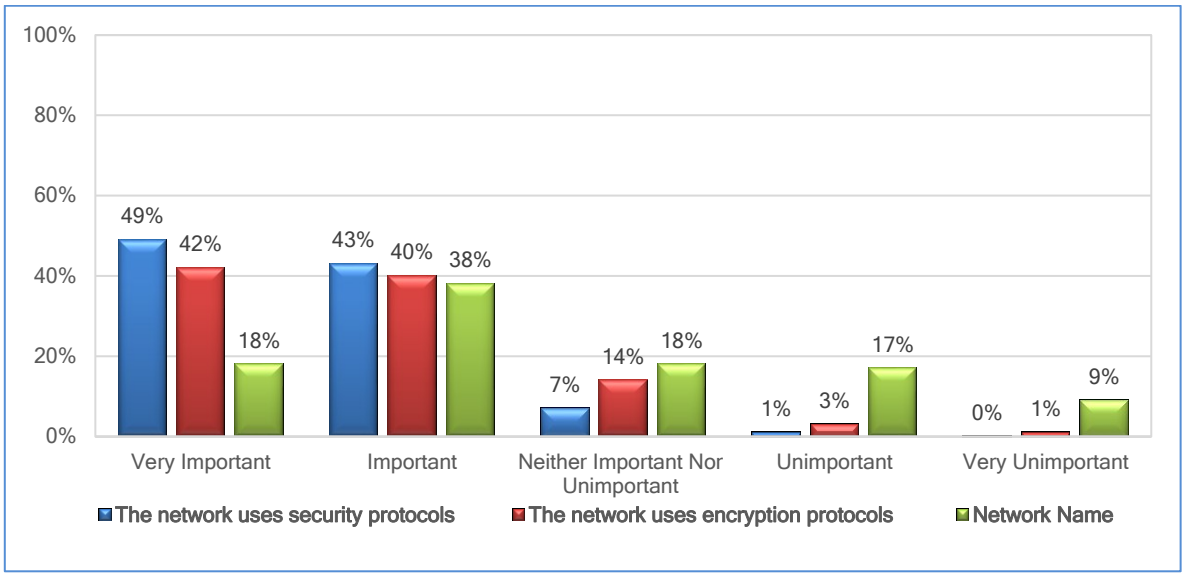

Figure 60: Participant importance: Security protocols, Encryption protocols, and the network name

Due to the substantial difference in the design of the third and fourth interfaces compared to the first and second interfaces, the participants who tried the third and fourth interfaces were asked about their view of the features that appeared in these interfaces, this was including the start time of the network, previously connected, in addition to the security level indicator. Figure 61 presents the participants' opinions.

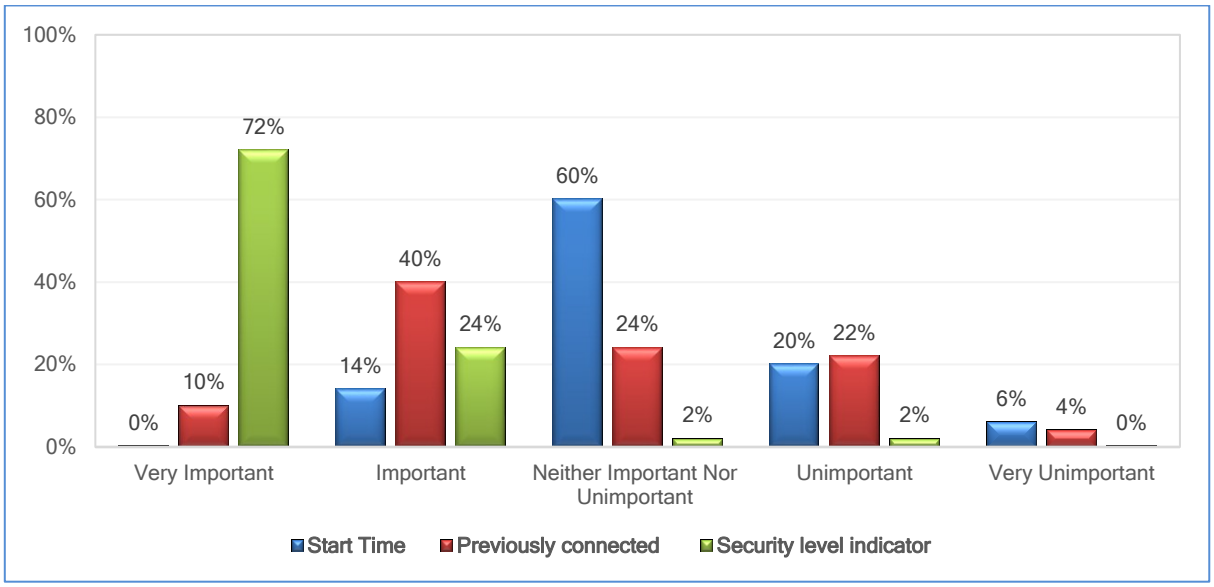

Figure 61: Participant importance: network start time, previous connection and security indicator

With the increase use of various types of meters/indicators in the IT field that are widely used to show the strength or risk of something, it is not surprising that over 95% of the participants who tried the third or the fourth interface claimed that the security level indicator/meter was very important or important. Effortlessly, the indicator/meter will attract users' attention and alert them directly to the security level of the network, by employing a variety of colour codes that can be easily interpreted. This result also highlights that the use of security level meter greatly influences the choices of participants who only tried the third or fourth interfaces. In terms of the new design, this reinforces the fact that the presence of a security level meter has enhanced the selection of participants to the most secure networks in the third and fourth interfaces, compared to the choice of participants for the less secure networks in the first and second interfaces in the absence of the security meter. In addition, this also emphasizes that users will appreciate the presence of the security meter which probably will help them to recognize the security levels of the available networks in a more appealing manner so they can decide to connect to the most appropriate Wi-Fi networks for their daily need when they are on the move. In contrast, there was only

50% who claimed that the feature of previously connected it very important or important, whereas the start-up time for the network was very much less appreciated by the participant, as only 14% of the participants claimed that it was important.

Figure 62 presents the level of the participants' confidence on connecting to the appropriate network for each interface. Due to the design that the third and fourth interface is providing, i.e., the visual appearance that can be easily interpreted and understood, and simple well-known tools such as the security indicator and colour codes, which demonstrate the security level of the network and employing traffic lights to determine the variations in the network characteristics status to reveal the relevant factors utilised to convey the relevant security information to the users in an easily perceived manner, supported with definite security guidelines with a recommended usage, it is not surprising that almost all the participants of the third and the fourth interface stated they are confident that they have connected to the appropriate network.

In contrast, the absence of an acceptable visual design, which does not explain the security level of the network in a good way, nor provides a visualization that can be easily interpreted and understood, it is not likely that users would be confident that they connected to an appropriate network. One of the apparent examples in this regard is the use of a pop-up window currently used in Microsoft Windows 7 when users are exploring the available Wi-Fi networks. The pop-up window is visible only for a few seconds and then disappears, which probably would not be sufficient to convey the security message to users about the security level of the Wi-Fi network and will not be enough to provide security guidelines to help users to understand the security level of the Wi-Fi network and then make the appropriate security decision.

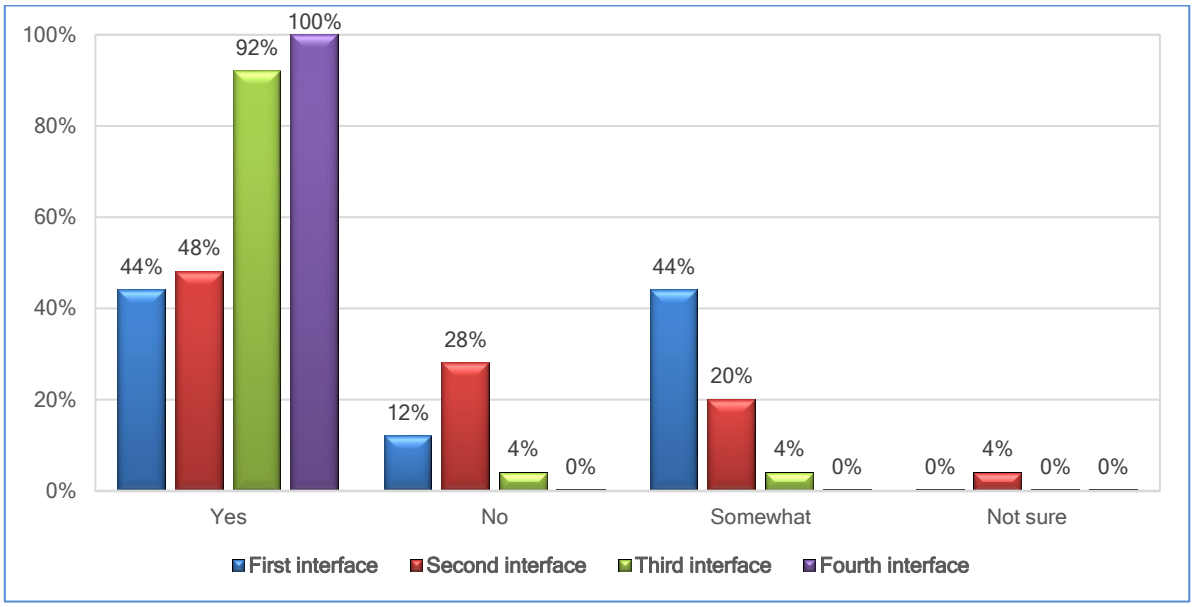

Figure 62: Participants' confidence about connecting to the appropriate network

Figure 63 shows the participants' view on whether they think the usability aspect can be improved in the interface they tried. Although the sample involved only users with average computer skills, who perhaps have no solid background to criticize software or computer interfaces in terms of the design, nevertheless their point of view should be considered as the sample of the study and because they are the most representative sample of the knowledge level for the largest number of computer users. Participants who tried the third or fourth interface showed their satisfaction with the usability of these interfaces, with only 16% of the participants of the third interface believing that the usability aspect of this interface can be improved, and only 8% of those who tried the fourth interface. In the comparison, participants of the first and the second interfaces were less optimistic in this regard, with 24 % of the participants who tried the first interface believing that the usability aspect of this interface can be improved, and the same percentage of the participants who tried the second interface. This view conceivably explains the participants' satisfaction with the security information and advice provided to them in the third and the fourth interfaces, and the dissatisfaction

with the security information and advice provided to the participants who tried the first and second interfaces.

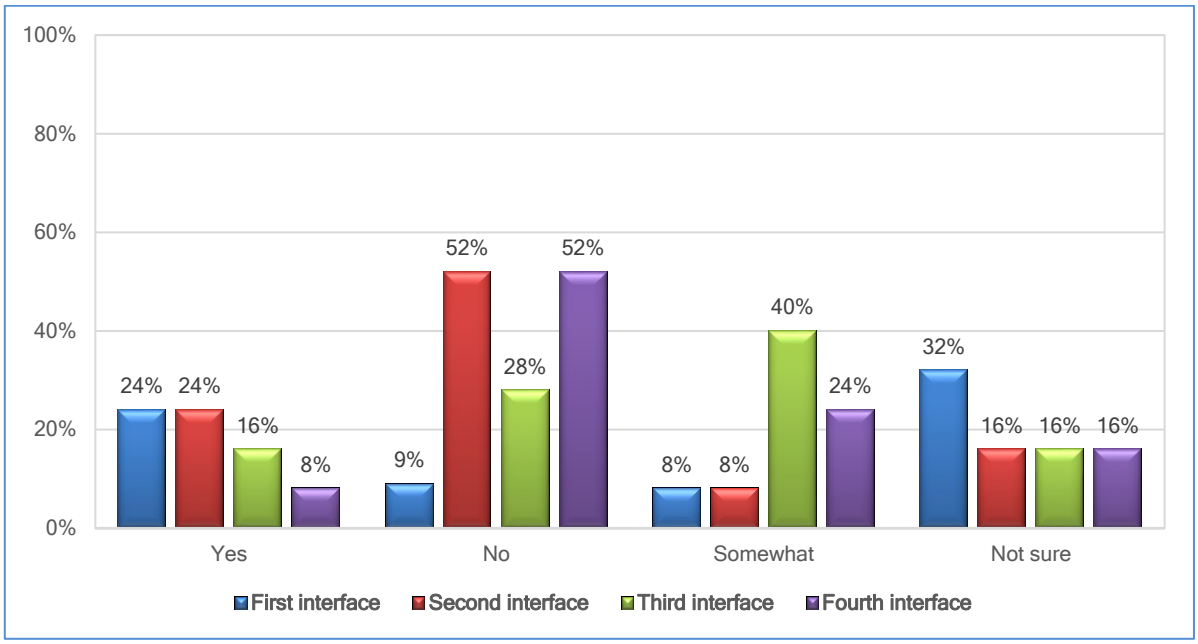

Figure 63: The participants' view on usability aspect of tried interface

Again, the results presented in Figure 64 suggests that the third and the fourth interfaces excel the first and the second interfaces in this regard, where just over three-quarters of the participants of the third interface claimed that they are either completely or very satisfied with the supported information about the presented networks, and over 90% of the participants of the fourth interface claimed so. In comparison, there were just over two-thirds of the participants of the first interface claimed that they are either completely or very satisfied with the supporting information about the presented networks and just over half of the participants of the second interface claimed so. Results suggested undoubtedly that there is advantage of using the security control panel and the security meter that is used in the new design for the third and the fourth interfaces, and that the third and the fourth interfaces are performing much better in satisfying the users by providing the required security information and provide a better support for the participants, compared to the design of the first and the third interfaces.

Linking this result to the previous results, it is undoubtedly that the new design has helped the participants of the third and the fourth interfaces in a simple manner without information overload of technical terminology to make appropriate security decisions when connecting to Wi-Fi networks.

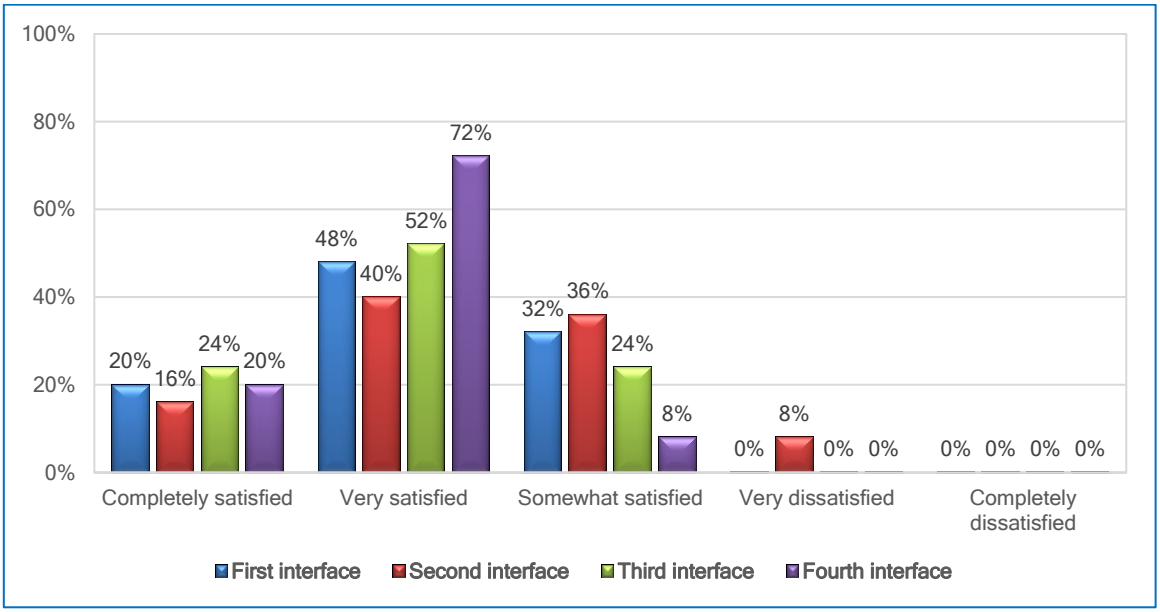

Figure 64: Participants' satisfaction: supporting information about the presented networks

Participants were asked after their experience with the interface they tried how likely their behaviour online would be changed depending on whether the Wi-Fi connection is secure or not. Figure 65 presents the participants' opinions for each interface in this regard.

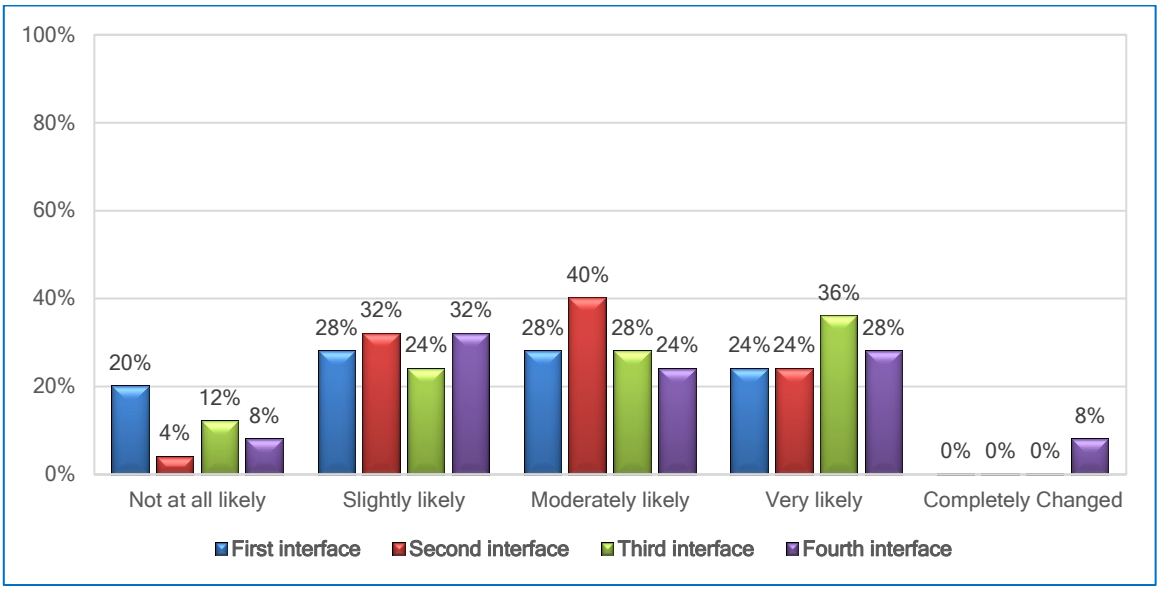

Figure 65: Post-experiment Views: Security consideration in selecting Wi-Fi

In general, one of the main motives of this experiment was to highlight the lack of adequate security information aiding in making appropriate security decisions and reducing end-user security compromises in different scenarios. The problem of connecting to insecure public Wi-Fi networks that are wide speared in public places was an example of such scenarios. In particular, the various interfaces and surveys have been introduced to appreciate whether this will make users aware of the issue and to educate them about the problem. Moreover, this was also to increase their awareness in this regard and to see if the users will change their behaviour towards the security related issues in general and towards connecting to insecure and unknown Wi-Fi hotspots after the experiment. The following section is presenting the participants' comments for each interface on whether on whether they will change their behaviour after their experience or not.

Comments of the participants who tried the first interface:

1. *I am cautious already with regards to using public networks. But certainly I will think more about the network I am connecting to. I believe the main problem would be that the general public are naive or just uneducated on the subject. It is largely the younger generation who take an interest into the internet and would have some knowledge about the type of networks they are connecting to.*
2. *I already don't use online banking services or payment while on an unknown public network.*
3. *If I needed to access something urgently (e.g. banking) then I would take the risk, however I would attempt to not do it so regularly.*
4. *If it is secure, I will do all tasks that I need to, however if insecure I will limit using things that involve money and confidential information.*
5. *It is something I haven't given much thought to it before, but thinking it through whilst completing this survey has made me consider there could be some risks.*
6. *If you require Wi-Fi to complete a task, you'll still connect to an unsecure Wi-Fi if a secure network isn't available.*
7. *Has made me think a little bit more about what it could do when I connect to unsecure networks, I would like to know the risks as they aren't clear. I think I might be a bit more reserved in the future when connecting to open Wi-Fi systems such as in shopping centres etc.*
8. *I'm already quite aware of internet security and rarely use Wi-Fi hot spots.*
9. *I'm generally cautious about unsecured Wi-Fi anyway.*

10. *When out and about, and I see a network I will be more cautious when connecting. I only use public networks for google searches or google maps. However even then there is a risk that when I have connected they could give me Malware etc.*
11. *I believe that I already have security measures in place i.e. using my own networks for banking and anything where I need to input information that could be stolen.*
12. *I already follow quite good security procedures when I use the internet.*

Comments of the participants who tried the second interface:

1. *It may make me think a bit more before just logging on.*
2. *I will still act the same as before as it is quicker and easier to use the Wi-Fi that works instead of the secure Wi-Fi which I don't actually understand.*
3. *More likely to check to see if the network is secure.*
4. *I should take more care when selecting a Wi-Fi connection.*
5. *I feel that I am already fairly careful when connecting to unsecured networks.*
6. *Will be more careful to check that my connection is secure.*
7. *I think I will actually look more closely at the details of each network to decide which would be the most appropriate and safest.*
8. *I may be more concerned when choosing a Wi-Fi network from now on.*
9. *Making you choose a network and then questioning you on your choice has made me think about what information is being shared over that network, but as I don't know the full extent of data sharing and the consequences of connecting to a network that is not secure I will probably still use unsecure networks more than I probably should.*
10. *I need to be more aware of what Wi-Fi network I choose to connect to.*

11. *I will be more aware of connecting to networks - not just choosing any old network.*
12. *I will look up what is an unsecured network so that I am more informed.*
13. *I would always choose the secure network first, however now I would also consider exactly what about the network is secure e.g. security and encryption. I am also likely to go away and find out more about secure networks and what information can be accessed from secure network.*

Comments of the participants who tried the third interface:

1. *I will definitely pay more attention to the security level. I was not aware of all the features previously that need to be taken into account while connecting to Wi-Fi hotspots.*
2. *I am generally cautious but this will make me look at bit harder at hotspots in particular.*
3. *Might double check rather than just connect.*
4. *I'm usually trying to keep an eye open to what I connect, so I don't think there's much to change.*
5. *I was cautious before, however, it has shown me how certain Wi-Fi networks may pose a threat to my personal information.*
6. *I would try and minimise the amount of detail I entered during that period when connected to an unsecure network.*
7. *I think I will be more aware of what I am connecting too. I never really thought before if a connection was secure before, but I think I will now.*
8. *Security was the main feature I was looking for and will be more likely to check security details of future connections.*

9. *I am not sure how I would apply the information given to me in the experience today to my real online activities.*
10. *I already know some of the risks of using an unsecured network.*

Comments of the participants who tried the fourth interface:

1. *I will most likely check to see if the Wi-Fi is secure next time I connect.*
2. *I am familiar with Wi-Fi security, however, this has reminded me that I should check more often than just connecting.*
3. *I would be more careful and wary when connecting to Wi-Fi networks, and not connect with the first Wi-Fi network I see. I would assess the Wi-Fi network based on their security level.*
4. *I think this will now make me check whether the Wi-Fi I connect to is secure or not.*
5. *I would be slightly more aware of it, but I don't think it will make a lot of difference in which network I select.*
6. *I think I'm likely to check security of the Wi-Fi before just connecting, maybe even encryptions.*
7. *I believe the knowledge of whether a connection is secure or not would influence the way I would use that connection or whether I would even use it at all.*
8. *As I already used to do what was recommended.*
9. *It would make too much of a difference as I can usually gauge the security level of a Wi-Fi connection. But the information did explain the risks and what each connection should be used for.*

Although the answers of the participants show no tangible difference between the interfaces in this regard, the comments of the participants showed that make users

aware of whether the Wi-Fi network is secure or not in a more apparent manner that can be easily comprehended would make a difference in the eyes of the users and nudge them towards changing their behaviour when connecting to unknown and potentially insecure Wi-Fi networks in public areas.

Participants were also asked whether the system has the functions and capabilities that they expect it to have. Figure 66 presents the results for this question for each interface. it could be argued that undoubtedly, the participants of the third and fourth interfaces had and benefited from the opportunity to compare the new design of these interfaces with the interface currently used in the Microsoft Windows 7 platform and thus, had the opportunity to understand the differences and improvements introduced to the new interfaces and were able to distinguish and became aware of the differences between the two designs. Therefore, on this basis, they built their view that the system they tried has the functions and capabilities that they expect it to have. On the other hand, however, it can also be explained that a high proportion of participants of the first interface as just over 90% and two-thirds of the second interface stated that the system has the functions and capabilities that they expect to have, despite the shortcomings that the currently used interface in Microsoft Windows 7 platform has, as discussed in the previous sections. This is probably due to the fact that the participants of the first and the second interfaces did not have the opportunity to see the new design and hence compared with the old design as the participants of the third and the fourth interfaces had, therefore their view here would not reflect the accurate state of the current design in which they were able to compare two different designs and the improvements in the new interfaces.

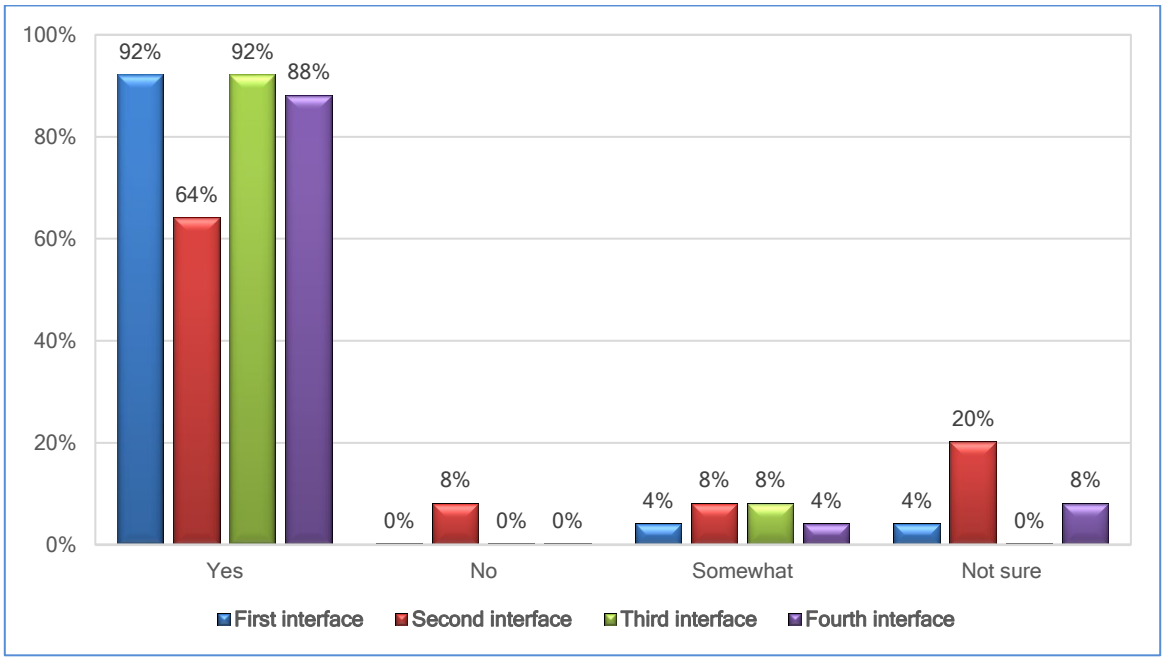

Figure 66: Post-experiment Views: Expected system functionalities & capabilities

Participants were asked in overall if they are satisfied with the software system (i.e. the interface) they tried. Figure 67 presents their opinion.

Although the answers of the participants here on this question also show no concrete difference between the interfaces in this regard, nevertheless results still demonstrate that overall satisfactions of the participants of the third and the fourth interfaces excel the first and second interfaces. It could be argued that if the participants of the first and the second interfaces have the opportunity to explore different interfaces then they would probably differentiate the features and express their satisfaction about whether they would be satisfied or not about the system they tried in more apparent manner.

The following section is presenting some of the participants' comments for the first and the second interfaces on why they were/were not or somewhat satisfied, however, none of the participants of the third and the fourth interfaces were somewhat or not satisfied, so there were no comments from the participants of these interfaces.

Comments of the participants who tried the first interface:

1. *A warning when logging on to an unsecure network, with info about what the risks might be could be useful.*
2. *I think that there could be some more details about security on the software so that it is clearer to people what they are signing up too.*
3. *The software system does not highlight to the user that the network is a danger to their devices and their information.*
4. *There was little opportunity for me to establish how secure the Wi-Fi networks were and so I am not satisfied.*

Comments of the participants who tried the second interface:

1. *It could be made clearer by using colours to draw your eyes to the recommended secure networks.*
2. *The warning that pops up needs to be more explicit in what it means.*
3. *It would be beneficial to have more information on the level of security provided my secure networks, but apart from this it was easy to use, navigate and understand. It also allowed the user to make an informed choice on the network they connected to.*

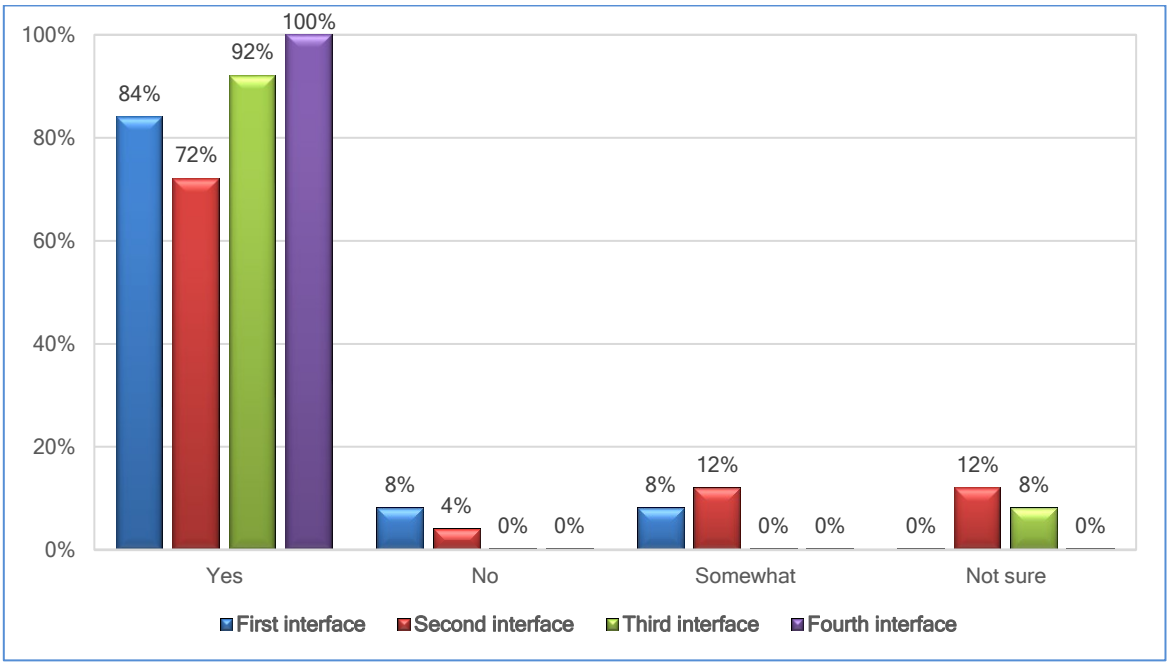

Figure 67: Participants' overall satisfaction of the tried interface

Participants were also asked if the information provided by the software was easy to understand. Due to the variation in the design of the four interface, Figure 68 presents the results for the participants' opinions based on the interface they have tied. Yet again, the results in Figure 68 indicate that there is no significant difference between the interfaces in this regard. Nevertheless, it could be argued that this is may be due to the fact that the views of the participants of the first and the second interfaces relied primarily on their experience with a similar interface currently used in Microsoft Windows 7 platform, so that they can expect and understand what the interface offered through their experience with that similar interface. On the other hand, distinctly the participants' opinions of the third and fourth interfaces were entirely based on their experience in dealing with the new design of the third and fourth interfaces. Therefore, their point of view reflects their understanding of the information and the security guidance provided by these new interfaces.

The following section is presenting some of the participants' comments on this question for each interface:

Comments of the participants who tried the first interface:

1. *The information is not always clear when provided, sometimes it can miss lead or not provide enough info.*

Comments of the participants who tried the second interface:

2. *A little message popped up, but I can't remember what it actually said, but it was easy to understand. Again, I'm not entirely sure what the meaning of the message meant in practice.*
3. *It could have given me more direction with what was best to do.*
4. *It needs to tell you to choose a connection and list the connections in order of strongest signal. It was only under assumption from the lock/unlock icons that I knew whether or not it was secured so there needs to be text.*
5. *When hovering over each Wi-Fi option, you could see the speed of the connection, whether it was secure and the name of the Wi-Fi which gives an indication of what you are connecting to. It was also very clear when you were about to connect to an unsecure server that it was just that - unsecure.*

Comments of the participants who tried the third interface:

1. *I had a harder time to understand some of the aspects of transferring the data between two parties, however otherwise the info was quite clear (encryption part).*
2. *It need for some improvement especially for how to connect to the choose network.*
3. *I did not know how to interpret this information.*
4. *Some of the computing ' jargon' may have been hard to understand to some. However, the examples of recommended use were helpful.*

5. *The information about a particular network's security seemed especially relevant and was quite easy to find.*
6. *Having coloured categories of important Wi-Fi features was helpful to quickly understand the most secure and strongest Wi-Fi connection.*
7. *Easy to read and had various colours where appropriate.*

Comments of the participants who tried the fourth interface:

1. *I didn't fully understand all the technical terms.*
2. *Very clear.*
3. *The information on a general note is friendly and ease to use.*
4. *Although it did explain to me the recommended usage of different security levels and the security information, I personally missed the security information as I didn't pay attention to this as I was only interested in the signal strength. The reason being that I was intending to use the internet only for browsing news websites and other non-sensitive websites.*
5. *I usually just connect to the Wi-Fi straight away, I don't read information, I just look at the bars and how fast the connection is. So reading any information doesn't usually matter to me.*
6. *It is easy to understand, and security information is quite helpful. But I'm not sure what encryption protocols mean and how it works. It takes a bit time for me to read the information and compare. I would expect less information provided in the interface and clearer sign or buttons. Just to reduce the time and effort in reading all the information.*
7. *It's perfect to understand the process that I go through the WIF I chose.*

8. *I wasn't very aware of what some of the words meant, like encryption for example. This is because I use computers but I don't necessarily know much about them. The information was clearly presented and had I understood the meanings of all the words I would say it was easy to understand. The diagrams showing bars for the connection strength and the level of security was helpful.*

9. *It could have more details for what some of the complex terminologies mean. Some people may not understand some of the words used. For example, what upstart time meant for the user.*

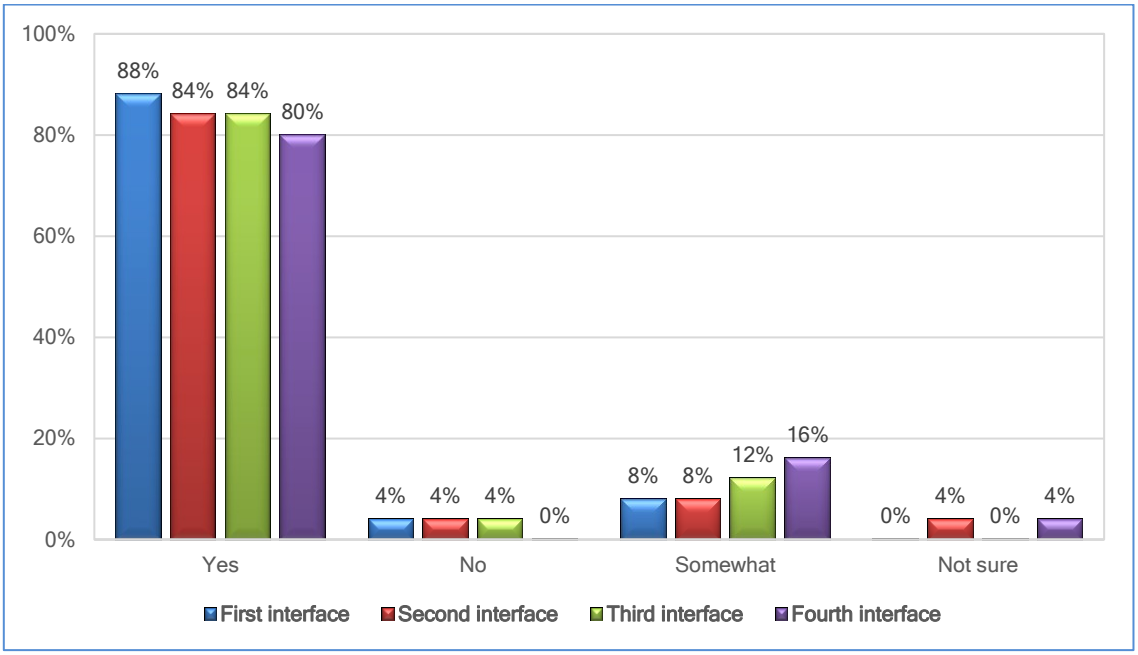

Figure 68: Participants' Views: Simplicity of information provided by the software

Due to the new variation of the design for the second, third and the fourth interfaces compared to the current dashboard that displays the wireless networks in the Window 7 platform, participants who tried these interfaces were asked whether the new design makes the information more presentable. Figure 69 presents the participants' opinions who tried the second, third and the fourth interfaces. It is not surprising that majority of the participants of the third and the fourth interface stated that the information more presentable in these interfaces than the current dashboard that displays the wireless

networks in the Windows platform. The third and the fourth interfaces were expected to be more presentable compared to the first and the second interfaces as discussed previously, because of the usage of the security level meter with coloured categories, which will attract users' attention and alert them directly to the security level of the Wi-Fi network and by employing traffic lights to determine the variations in the network characteristics status to reveal the relevant security information to the users in an easily perceived manner, supported with security information and a recommended usage, which was helpful to quickly understand the security level for each presented Wi-Fi network in these interfaces.

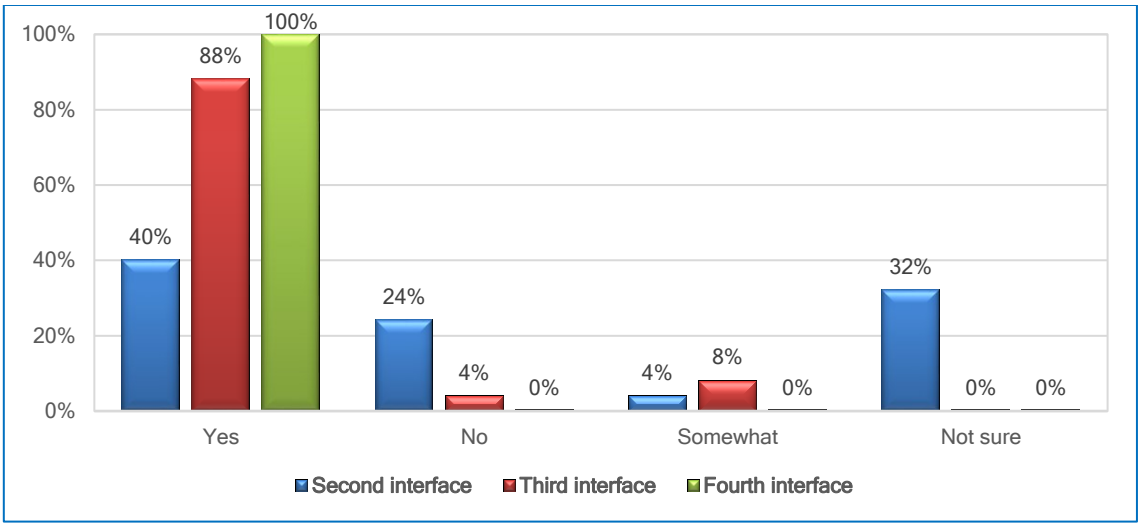

Figure 69: Participants' Views: Second, third and fourth interfaces vs. current Win 7 Wi-Fi dashboard

Participants were also asked if using software system (i.e. the interface) was convenient. This question was asked to the participants who tried the second, third and fourth interfaces and it was due to the new design of these three interfaces compared to the current dashboard that displays the wireless networks in the Windows 7 platform. Figure 70 presents the participants' opinions in this regard. In light of previous findings, it is not surprising that majority of the participants of the third and the fourth interface stated that using software system (i.e. the interface) was convenient. The third and the

fourth interfaces were expected to be more convenient compared to the first and the second interfaces, because of using the security level meter with coloured categories that will easily convince users and make them aware of the security level of the Wi-Fi network in an easily and an apparent manner, supported with security information and a recommended usage, which was not requiring exertion to understand the security level for each presented Wi-Fi network in these interfaces.

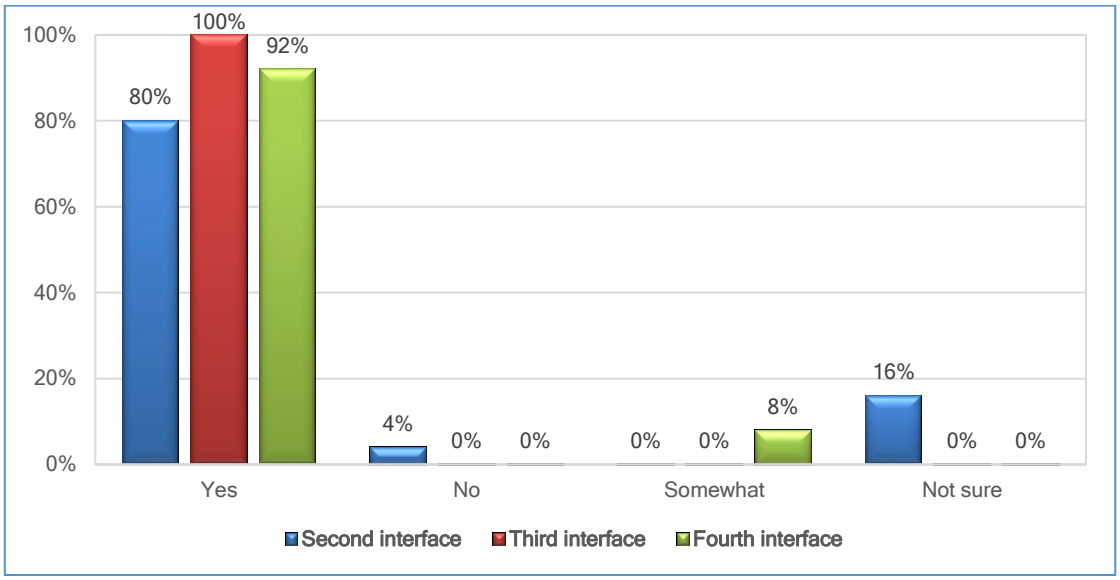

Figure 70: Participants' Views: Convenience of software system use

Participants were also asked if they think the full implementation of the software can be used to facilitate users in choosing the appropriately secure Wi-Fi network. This question was asked to the participants who tried the second, third and fourth interfaces, this was due to the new design of these three interfaces compared to the current dashboard that displays the wireless networks in the Window 7 platform. Figure 71 presents the participants' opinions in this regard. Results demonstrate that almost all participants of the third and the fourth interface agreed that the full implementation of the software can be used to enable users in choosing the appropriately secure Wi-Fi network and that it could help them straightforward to be more aware of connecting to insecure Wi-Fi networks. In comparison, there were less than 50% of the participants

of the second interface who agreed on this, probably due to the shortcomings of the second interface that impede users in choosing the appropriately secure Wi-Fi network.

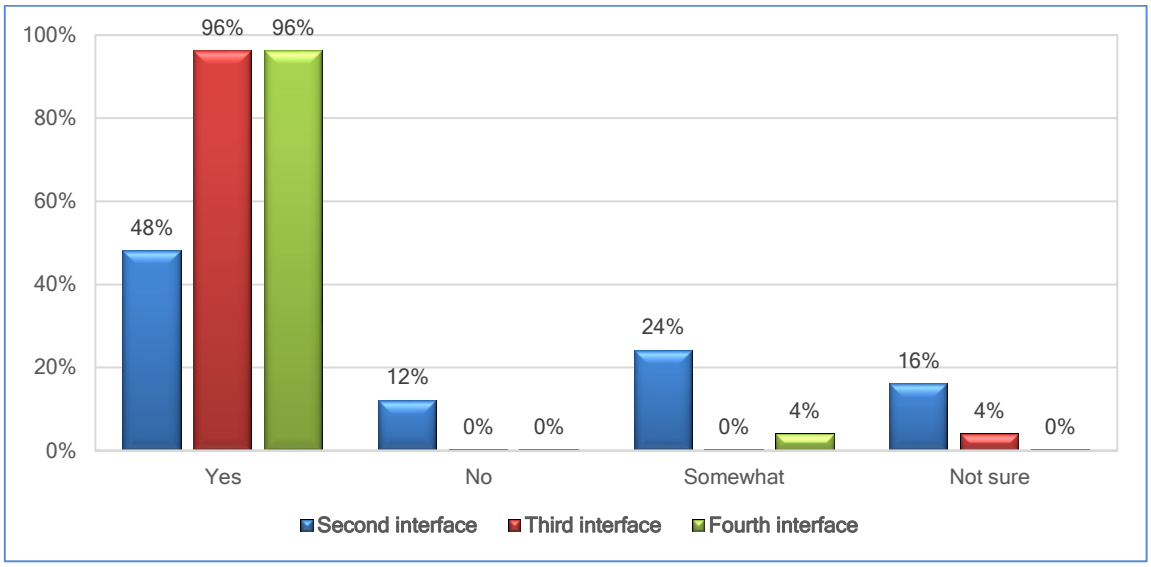

Figure 71: Participants' Views: Implementation of the software to facilitate secure Wi-Fi selection

Due to the substantial difference in the design of the third and fourth interfaces compared to the first and second interfaces, the participants who tried the third and fourth interfaces were asked if they are more confident in using Wi-Fi software that provides security related information because it helps them to decide whether it is safe to connect to an available Wi-Fi network. Figure 72 presents the participants' opinions in this regard. Almost the participants of both interfaces stated the same in this regard. Probably this is due to the fact they are designed very similar to each other and there are no concrete differences between them as mentioned in the previous sections. Results suggested that users are convinced and will be confident in using the tools or software that provides security related information to help them to decide whether it is safe to connect to an available Wi-Fi network. These findings also suggest that there is a high probability of positive response from users towards any tools or software that might be released by system developers to help users with the problem of connecting to an insecure Wi-Fi network and to highlight the risks of insecure Wi-Fi networks.

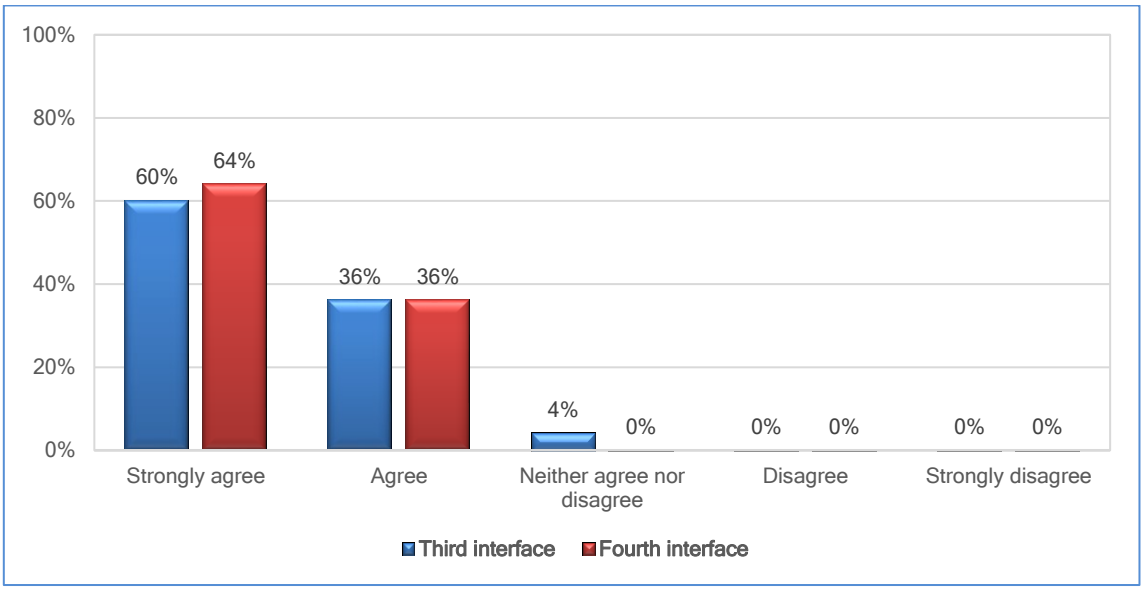

Figure 72: Participants' confidence in using software (Wi-Fi) providing security related information

4.5 Conclusions

This chapter has presented the results of an experimental study that examined the effectiveness of using targeted security awareness-raising approach. The study has shown that while users did not exhibit perfect behaviour, there was a tangible improvement with interfaces offering more security-related information. In common with other security contexts, results suggest that users' behaviour can be positively influenced purely through the provision of additional information and better choices can be made even if the system does not provide any further enforcement.

The results have also proven that the new design of the Wi-Fi interfaces has made an important improvement in terms of the security behaviours of the participants before connecting to insecure Wi-Fi hotspots in public areas.

Moreover, the results revealed that known Wi-Fi networks for participants are mostly treated as trustworthy networks, although the network name has the potential to be spoofed. This conceivably highlights the lack of knowledge of the participants regarding this security issue.

From the obtained results, it was also perceived that the network name has greatly affected some of the participants' decisions especially if its name implies that it has a high speed without paying any attention to security issues. This demonstrates that the speed in some cases outweighs the security concerns in the eyes of the participants.

One of the very important lessons learned from this experiment is that if leading developers such as Microsoft are prone to releasing software that gives insufficient security guidance to help users to understand the security and make the appropriate security decisions that lead to protect their data and devices, then what does this suggest is that this will likely not encourage other software developers to direct their attention to focus on the security in the software they release. If this occurs in the most important software developed by Microsoft, such as Windows, it affects a large population of users and sets a standard that others may consider acceptable in their own software.

Results of the surveys demonstrate that a relatively large number of the participants are impetuous about security risks related to the use of Wi-Fi networks. This illustrates the urgent need to provide a new way to increase the security awareness of users about the security risks associated with the use of Wi-Fi networks, especially if unknown.

Chapter 5

Design Principles and Guidelines for Targeted Security Awareness

5.1 Introduction

The need for developing security features and tools available in computer systems and applications, which are used to make users aware of security risks while the task in hand, has increased significantly over the years to accompany the increased range of cyber security attacks.

While many computer systems and applications provide and use a wide range of security features that users can use or rely on to protect themselves against these security threats, the current design of some of these security features is often blamed for shortcomings in making users fully aware of the security risks that they may face. This reduces the level of protection that can be achieved by using the current design of the security features and tools particularly for novice and other non-technical computer users.

The findings of the prior experimental work conducted during this research and described in chapter 4, have revealed that user's security behaviours can be positively influenced through the provision of additional information, enabling them to make better-informed security choices even if the system does not provide any further means of enforcement. Furthermore, results suggests that users will appreciate if adequate security guidance is provided before making a security decision to help them to understand the security risks, so that they can make appropriate and informed security

decisions that help to mitigate the security threats and protect their data and devices. Results also revealed that tools such as security level indicators (Security meters) with a combination of background colour codes, which demonstrate the security status and, supported by accompanying text to explain the security risks and proposed recommendations, have played a vital role by aiding users towards that end. Findings were used to identify design principles to assist targeted awareness raising. Seven valuable key security design principles were identified and proposed, each with underlying guidelines for system designers/developers to improve security features in their software to help to make users appropriately aware of the security threats they may encounter.

It can be argued that the existence of design principles and guidelines is imperative for the development of UI elements in a wide range of applications, for several reasons, including improving the usability of the IT systems, and user productivity through a user-friendly system. This should improve efficiency and reduce user errors. It can be achieved by producing consistent and less confusing UI elements of the applications. User confusion may occur because of the inconsistencies of UI elements of the same type of applications which will reduce the efficiency of these applications. Thus, the need to develop design principles and guidelines may continue as new issues arise, which need to be addressed by adhering to new design principles, to avoid confusion and provide applications of the same type in a consistent design.

The dominant objective of HCI is to facilitate the interaction between the user and the computer. Human-computer interaction field emerged as a part of intertwined roots in computer graphics, operating systems, human factors, ergonomics, industrial engineering, cognitive psychology, and the part of computer science systems. Human-computer interaction defined by Hewett et al. (1992) as "*a discipline concerned with*

the design, evaluation and implementation of interactive computing systems for human use and with the study of major phenomena surrounding them". The introduction of graphical user interfaces made computers easier to operate, contributing to huge growth in research in the field of HCI. As a result, a number of design principles have been created and developed (Johnston et al., 2003).

From a computer science perspective, human-computer interaction (HCI) deals with the interaction between one or more users and one or more computers using the User Interface (UI) of a program. The long-established HCI concepts can be used to design an interface or improve an existing one, taking into account aspects such as usability, which is used to determine the ease of use of a particular technology, the level of technology effectiveness according to the user's needs and user satisfaction with the results obtained using a particular technology to perform specific tasks (Muñoz-Arteaga et al, 2009).

With the development of computer software, the imperative need and the importance of creating design principles and guidelines for the development of applications have emerged. More specifically, for the development of UI elements for various types of applications so that they are easy to use, leading to reliability in these systems. It was noted that there should be specific design principles and guidelines that applications developers can rely on when developing their applications, which will reduce confusion for users, and ultimately increase their efficiency.

With the development of software applications and the emergence of new requirements aimed at increasing the security of information systems, there is a need for specific design principles that contribute to increasing the efficiency of these systems while providing protection to IT systems through adhering to new design principles and guidelines.

5.2 The Need of Design Principles for Targeted Security Awareness

Usability is arguably one of the most important focusses in the field of cybersecurity today. Supported by the need for confidentiality, integrity, availability; these features have become common components of IT systems that require use by novices and experts alike. As security features are exposed to wider categories of the users, it is essential to ensure that these functions are highly usable. This is mainly because poor usability in this situation often translates into an inadequate application of cybersecurity tools and functionality and, as a result, ultimately limiting their effectiveness. In order to achieve this objective of highly usable security, there have been extensive studies in the cybersecurity literature focused on identifying security usability problems and proposing guidelines and recommendations to address them (Nurse et al, 2011).

Over time, requirements have changed, and new ones emerged with a more focused set of design principles and guidelines that have become necessary to address more specific issues and achieve specific objectives. For example, creating design principles and guidelines for designing UI elements which addresses issues related to the security of the IT systems.

Security HCI (HCI-S) was introduced to reflect the need to explicitly support security in the development of UI elements in the IT systems field. The HCI-S concept built mainly upon modifying and adapting traditional HCI concepts to focus on security aspects in order to improve the security of IT systems by improving the elements of their user interfaces (Muñoz-Arteaga et al, 2009). The term HCI-S was first introduced and defined by Johnston et al. (2003) as "*The part of a user interface which is responsible for establishing the common ground between a user and the security features of a system. HCI-S is human computer interaction applied in the area of computer security*" (Johnston et al., 2003).

Users interact with computers and technology through various user interfaces. These interfaces are designed to help users understand IT systems and increase productivity in using them. For example, a well-designed user interface assists the user to become skilled in operating the software in a short period of time. This helps to increase the user's efficiency in completing a particular task, thus the user feels in control and satisfied with the technology. Conversely, if the interface is poorly designed, it can frustrate the user and hinder on completing the task successfully, which will result in decline and uncertainty about the use of specific technology in the future. Generally, users experience security functionality through the user interfaces. The interface notifies the user of the available security functions and how to use them. A user may not be aware of the security feature or may be using it incorrectly. The interface should ensure that the user is appropriately guided in order to minimise the potential for the user to be the 'weakest' link (Johnston et al., 2003).

As such, Johnston et al. (2003) principles have come to balance the usability of systems while increasing their protection by adhering to new design principles to increase system protection without compromising usability at the same time. Although these principles exist for user interfaces are purposely oriented on the security environment, there is still a need to introduce new principles or develop existing ones to adapt to the new requirements such as increasing the users' security awareness through the security features that are included in the user interfaces of the existing applications.

Although Johnston's security-related design principles have been widely cited in the literature, there is currently a need to introduce new principles to adapt to new requirements. For instance, in the case when users are exploring Wi-Fi networks and wanted to know the security concerns of the available Wi-Fi networks and what to use

it for. In addition, in the case of spotting phishing emails using email applications. In these examples, there is a lack of design of the interfaces of these applications, which does not provide adequate security information to users about the type of security threat faced by the user during their daily use or interactions with these applications, as well as not providing recommendations to users to help them stay safe.

One example is connecting to insecure Wi-Fi networks. Kaspersky reported that 71% of the surveyed users use insecure public Wi-Fi (Kaspersky Lab, 2016). The interfaces currently used to select Wi-Fi networks do not provide sufficient security information to make users aware of the security risks associated with the use of unknown and potentially insecure Wi-Fi networks. As a result, it is not surprising the percentage of users who connect to insecure Wi-Fi networks is at these high levels.

Another example is the number of victims of phishing email attacks. 76% of the surveyed Infosec professionals reported that their organisation experienced a steady or higher volume of phishing attacks in 2017 compared to 2016 statistics (Wombat Security Technologies, 2018), despite the availability of security awareness programs, which aim to increase the security awareness of users of this type of attacks and despite the availability of protection software. By examining the interfaces currently used in some email applications, it can be seen that these applications are inadequate to make the user aware of this type of security risks and there is a lack of information provided to increase security awareness of the users before taking any actions that may lead to compromise their systems.

In the two examples described above, there is a design flaw of the user interfaces of these applications in terms of properly making users aware of the potential risks, as with their current design, they do not provide adequate information or suitable recommendations to users to take appropriate actions or make proper and informed

decisions. Ensuring that users are aware of the potential threats they may face, whether through phishing email or using an insecure Wi-Fi network, is the difference between the occurrence of a security breach and completely avoiding the risk. To mitigate these risks, there should an adoption of new methods to increase users' awareness of such risks.

Nonetheless, despite the existence of security awareness programmes, many companies are unprepared to deal with cyber-attacks. 48% of the 9,500 executives in 122 countries surveyed by the 2018 Global State of Information Security Survey (GSISS) stated that they do not have an employee security awareness training program (PwC, 2018). Often, staff compromise security unintentionally. The Cyber security breaches survey 2017 reveals that 72% of reported security breaches occurred after they received a fraudulent email. Only 20% of the staff surveyed attended any form of cyber security training (IT Governance, 2018). Users are also prone to forgetfulness and therefore over time, users may forget their training. It is therefore imperative to ensure that user interfaces in applications provide the necessary security information to increase awareness of users.

Perhaps a part of the problem can also be blamed on the shortcomings of the current interface design of some applications. Whitten and Tygar (1999) stated that user errors contribute to most computer security failures, nonetheless user interfaces for security still tend to be inconvenient and confusing. They posed a question whether this is simply due to failure to apply some standard UI design techniques to security and whether the general user interface design principles are adequate for security. They argued that effective security requires, in contrast, a different usability standard and that the effective security will not be achieved through the user interface design techniques appropriate to other types of consumer software. Furthermore, they stated

that user security interface designers should not assume that users will be motivated to read the manuals or to search for security controls that are designed to be not easily observed or noticed. Moreover, if security is very difficult, irritating or disturbing, users may completely abandon it. From the results obtained from their work, they conclude that the standard model of user interface design, particularly the once represented by PGP 5.0 (their area of study) is not sufficient to make computer security usable for people who are not already knowledgeable in that area.

From their work which was focused on evaluating PGP 5.0's usability, the standard principles of user interface design, is not sufficient to make computer security usable for users who have a lack of understanding and limited skills in that area. Their conclusion was precisely stating that user interface design for effective security remains a problem that needs to be further investigated, and argued that this problem remains open and unresolved (Whitten and Tygar, 1999).

It is clear that there is a need for specific design principles that aim to increase the security awareness of users in their daily usage of IT systems and ensure that sufficient information is available to users when needed and providing them with the necessary advice and recommendations.

5.3 Related Work

There is an absence of published research on the need for design principles that directly focus on the problem of the design of user interfaces that serve the objective of "making users aware" of the security threats through improving the user interfaces of the applications. Since users are primarily dealing with IT systems through user interfaces and the vast majority of the users of IT systems often find it difficult to deal with existing security risks because of having inadequate skills, it is imperative to

investigate other existing design principles and compare them with the proposed design principles, to ensure that no essential design principles are ignored.

5.3.1 A General-purpose Usability Heuristics

Nielsen (1994) has developed 10 Usability Heuristics for user interface design by comparing several published sets of usability heuristics with a database of existing usability problems derived from a variety of projects in order to determine what the best explanation of actual usability problems is. Based on the analysis of the explanations, as well as the analysis of the heuristics providing a broader explanatory coverage of the problems, Nielsen has introduced a new set of ten heuristics. This was to increase usability and address the problem of user interface inconsistencies. Nielsen (1994) has also concluded that these heuristics seems to be excellent to explain the usability problems previously found. It continues to be seen to what extent it is also good for finding new problems, which is the main objective of heuristic evaluation (Nielsen, 1994). Nielsen's Usability Heuristics are presented Table 8 (Nielsen, 1995).

Table 8: Nielsen 10 Usability Heuristics

No	Criteria of HCI	Description
1	Visibility of system status	The system should always keep users informed about what is going on through appropriate feedback within reasonable time.
2	Match between system and the real world	The system should speak the users' language with words, phrases, and concepts familiar to the user, rather than system-oriented terms. Moreover, it should follow real-world conventions, making information appear in a natural and logical order.
3	User control and freedom	Users often choose system functions by mistake and will need a clearly marked "emergency exit" to leave the unwanted state without having to go through an extended dialogue. Support undo and redo functions.

4	Consistency and standards	Users should not have to wonder whether different words, situations, or actions mean the same thing. It should follow platform conventions.
5	Error prevention	Even better than good error messages is a careful design which prevents a problem from occurring in the first place. The system should either eliminate error-prone conditions or check for them and present users with a confirmation option before they commit to the action.
6	Recognition rather than recall	Minimize the user's memory load by making objects, actions, and options visible. The user should not have to remember information from one part of the dialogue to another. Instructions for use of the system should be visible or easily retrievable whenever appropriate.
7	Flexibility and efficiency of use	Accelerators – unseen by the novice user – may often speed up the interaction for the expert user such that the system can cater to both inexperienced and experienced users. It allows users to tailor frequent actions.
8	Aesthetic and minimalist design	Dialogues should not contain information which is irrelevant or rarely needed. Every extra unit of information in a dialogue competes with the relevant units of information and diminishes their relative visibility.
9	Help users recognize, diagnose, and recover from errors	Error messages should be expressed in plain language (no codes), precisely indicate the problem, and constructively suggest a solution.
10	Help and documentation	Even though it is better if the system can be used without documentation, it may be necessary to provide help and documentation. Any such information should be easy to search, focused on the user's task, such as a list of concrete steps to be carried out, and not be too large.

5.3.2 A Security-specific User Interface Design Principles

The HCI-S design principles were introduced by Johnston et al. (2003) and are intended to address how the security features of the GUI can be made as user-friendly and easier to understand and operate as possible. This results in making the system

easier to use, further improves the user experience, and makes less likely that the user will make mistakes or attempt to bypass the security feature, resulting in a more reliable system. The objective of HCI-S is to improve the interface in order to enhance the security. This makes the system more secure, robust, and reliable. HCI is focused on making the IT system as easy to use as possible. However, security features are occasionally seen to make the system harder to use. HCI-S addresses the issue and balances between security and usability. However, the HCI-S concept introduced by Johnston et al. (2003) did not specifically state that it was intended to make users fully aware of the security threats nor particularly addressing the issue of the end users lack of security awareness. Table 9 presents the design principles of HCI-S introduced by Johnston et al. (2003).

Table 9: Johnston et al. (2003) HCI-S criteria

No	Criteria of HCI-S	Description
1	Convey features	The interface needs to convey the available security features to the user.
2	Visibility of system status	It is important for the user to be able to observe the security status of the internal operations.
3	Learnability	The interface needs to be as non-threatening and easy to learn as possible.
4	Aesthetic and minimalist design	Only relevant security information should be displayed.
5	Errors	It is important for the error message to be detailed and to state, if necessary, where to obtain help.
6	Satisfaction	Does the interface aid the user in having a satisfactory experience with a system?

5.3.3 A Security Domain-specific User Interface Design Principles

Whitten and Tygar (1999) provide one of the seminal design principles of usable security with a focus on encryption and introduced many key issues facing novice and

non-technical users who have little initial understanding of security, particularly in the use of PGP 5.0 application. As a result of their investigation, they stated that security interfaces tend to be confusing, inadequate and inconsistent, thus hindering rather than helping users. In addition, they tend to suggest that to make security usable, there needs to be a development of domain-specific user interface design principles and techniques. According to them, the problem of usability is compounded by several implicit characteristics of the security. These characteristics are presented Table 10.

Table 10: Whitten and Tygar (1999) Criteria

No	Criteria	Description
1	The unmotivated user property	Security is usually a secondary objective for users. Users do not generally focus on security but rather they focus on achieving their tasks. It is easy for users to postpone learning about security, or to optimistically assume that their security is in place, while they focus on their primary tasks.
2	The abstraction property	Security is governed by the underlying abstract rules, such as security policies. Computer security management often includes security policies, which are abstract rules to determine whether to grant accesses to resources. Creating and managing such rules is an activity that programmers consider intuitive, but it may be atypical and unintelligible to an enormously wider user group. The security user interface design should take this into consideration.
3	The lack of feedback property	Providing quality feedback is difficult noticing security's complex nature. The need to prevent dangerous errors makes it crucial to provide good feedback to the user.
4	The barn door property	The proverb of the futility of locking the barn door after the horse is gone is related to the description of an important property of computer security: If a secret is left unprotected even for a short time, there is no way to be sure that it has not already been reached by an attacker. It is therefore very important to design the user interface for security and give a very high priority

		to ensure that users understand their security well enough to prevent potentially high-cost mistakes.
5	The weakest link property	It is well known that a security chain is as strong as its weakest link. If a hacker can take advantage of one mistake, the game is over. This means that users need to be guided to attend all aspects of their security, not leaving them to proceed through random exploration as they might with the normal application. Therefore, all users must understand this fact because it relates to the security of their systems.

5.4 The Proposed Security Design Principles and Guidelines

Although the usability problem was a major design goal of the previously introduced design principles, these principles do not attempt to address the issue of making users aware of the security risks they may encounter.

In this research, a series of related design principles and guidelines have been identified from the prior work described in chapter 4 and utilized in the surveyed interface design to devise these security features by providing an adequate security information and recommended usage, to support users to recognise the security risk and understand the required actions that they need to take in order to avoid security risks. These key security design principles and guidelines could also be used to inform the design and implementation of security-related tools and interfaces to support and make users appropriately aware of the security risks they may encounter during their daily use of IT systems. The new proposed security design principles and guidelines are described in the following section.

5.4.1 Principle 1: Severity of the Security Risk

Aim: To signify the severity of the security risk, with the aid of tools and techniques used by software and operating systems, on a given scenario.

Guideline 1.1: Consider the use of a meter to highlight the severity and/or risk of the action they are about to undertake.

Guideline 1.2: The use of a status mechanism should aid in enhancing the users' selections/actions in a clear and easy way without interfering with the usage of the device.

Signifying the severity of the security risk is the main key and the first step to make users aware of the security risk in any security scenario. There are a wide variety of tools and techniques used by the software and operating systems developers to demonstrate the severity of security risk that users may encounter during their daily use of IT systems.

An apparent example of these techniques and tools is utilizing the security indicators related to the application in use. Furthermore, the use of status mechanisms can keep users aware and informed about the state of the system (Katsabas et al, 2005). The experimental Wi-Fi selection study (see chapter 4) revealed that over 95% of the participants who tried the third or the fourth interface claimed that the security level indicator/meter was very important or important. This result also highlights that the use of security level meter helps significantly by making users aware of the security status of the presented Wi-Fi networks and contributed to making users differentiating the security level of each presented Wi-Fi network before selecting any Wi-Fi network. In addition, this has reinforced the fact that the presence of a security level meter has enhanced the selection of participants to the most secure networks in the new design

of the Wi-Fi interfaces compared to the choice of participants for the insecure networks in the interfaces those has no security meter.

Furthermore, this also emphasizes that users will appreciate the presence of the security meter in other IT security scenarios in which users may face security risks and need more help to recognize the severity of the threat in a more apparent manner, so they can better understand the severity of the threat they face before taking any actions that may lead to compromise the security of their IT system.

5.4.2 Principle 2: Security Visuals

Aim: Users should receive a clear indication of the current security status, including specific notifications and warnings for events of interest or concern.

Guideline 2.1: Consider the use of background colour codes to attract attention and signify severity. The use of background colour codes is a key factor in demonstrating and clarifying the security status of any application that users are dealing with.

Guideline 2.2: Use visual indicators to convey information about the type of incident (pictorial representation, supplemented with brief words or hover-over text). These tools and techniques are also well-known to users and have been in use for a long time by software developers in a wide variety of applications to demonstrate the different status of IT systems.

The experimental study of the Wi-Fi selection described in chapter 4 revealed that almost all participants who tried the third or the fourth interface stated they are confident that they have connected to the appropriate network. This is due to the fact that the design of the third and the fourth interface (see chapter 4) is providing more security visual appearance that can be easily interpreted and understood, and by

utilizing a simple well-known tools such as the security indicator and background colour codes that demonstrate the security level of the network and employing traffic lights to determine the variations in the network characteristics status to disclose the relevant factors utilised to convey the relevant security information to the users in an easily perceived manner, supported with definite security information with a recommended usage.

Security visuals are mainly built on the use of easily recognizable security warning signs, traffic lights and background colour codes (Red for dangerous, Amber for risky, Yellow to take precautions and examine, and Green for safe/secure) to help users grasp security risks from the first glance. In contrast, in the absence of an adequate visual design of the first and the second interfaces (see chapter 4), which does not explain the security features and risks of the Wi-Fi networks. In the absence of apparent and observable visualization design which can be easily interpreted and understood, it is not likely that users would be confident that they connected to an appropriate and secure network.

5.4.3 Principle 3: Simplified Security Explanation

Aim: To transmit the message to the users in a manner that would be clear and simple to understand regardless of their vocational inclination.

Guideline 3.1: The language used should be suitable for first-time as well as advanced users. This will help users to comprehend and correlate the presented security visuals with the security explanation of the security threats they are facing.

Guideline 3.2: There should be a balance between providing enough information without overwhelming the user. Furthermore, Katsabas et al, 2005 has found that

beginners will find it hard to comprehend the security threats if technical vocabulary and advanced terms are used profusely.

In addition to the security visuals, users also appreciate the presence of text that presenting the specifics of the security threat in everyday user language. This will help users to comprehend and correlate the presented security visuals with the security explanation of the security threats they are facing. The experimental study mentioned in the previous chapter revealed that users would appreciate if they will be provided with an adequate text that explains the security risk they are encountering with the least possible use of technological terminology. For example, participants of the first and the second interfaces stated that the information provided was vague or inadequate. In contrast, participants of the third and the fourth interfaces stated that the security information provided was comprehensible and useful in helping them understanding the security features of the presented Wi-Fi networks, make them aware of the security statues of the presented Wi-Fi networks and also helped them to make more informed decisions based on the information and explanations provided.

Nevertheless, the terminology used should be suitable for advanced as well as first-time users in which there should be a balance between the need to provide enough information for a first-time user while not too much information for an experienced user.

5.4.4 Principle 4: Proposed Recommendation

Aim: Users should have an action recommended in order to avoid/minimize a highlighted risk.

Guideline 4.1: There should be a supporting message with the appropriate recommendation for actions to be taken by the user to minimize/avoid the risk.

Guideline 4.2: The recommended actions should help to mitigate security implications and nudge users towards a better security behaviour and making better informed security decisions.

Guideline: 4.3: The proposed security recommendations should be intelligible and precise, without complexity, to allow users to take appropriate actions.

Providing the security recommendations to users will make it easier for them to make the most appropriate and informed decisions in different scenarios where no or inadequate recommendations are provided when dealing with IT systems. It also helps to mitigate implications and nudge users towards a better security behaviour and making a better decisions.

Due to the lack of knowledge of the security risks of novice computer users and users with average computing skills, the need to provide security recommendations to users is a vital factor in terms of the action that needs to be taken to prevent compromises. Novice computer users with limited computer skills are representing the largest population of computer users. Therefore, it would be inadequate to equip users with only security warning message without supporting this security message with the appropriate security recommendation for the users that need to be taken to avoid the risks.

Nevertheless, the proposed security recommendations should be very clear and precise as much as possible without any complexity to allow users proceed to take appropriate actions that should help them to make informed security decision rather than placing them into a guessing game of what is being recommended to them by the application to avoid the risk.

5.4.5 Principle 5: Minimal Intrusion

Aim: Interventions and/or alerts should not attempt to inhibit the user from completing their intended tasks.

Guideline 5.1: Users should not feel overwhelmed by the warning messages and their usage of a device should not be diminished due to the security measures implemented.

Guideline 5.2: The number of clicks should be as minimal as possible from the point when the security threat facing the user is presented (or identified) to the point where the user is provided with adequate security information and recommended usage about the security risk.

Guideline 5.3: The warning message should not interfere or affect the other components of the interface, i.e., it should not block, modify, overlap or make the interface harder to interact by the user.

The clear majority of users tend to accomplish everyday businesses when using IT systems as fast as possible especially with time pressure. It could be argued, it is clear that the number of security interventions and security warnings have a great impact on users, especially if the security interventions and security warnings are overwhelming, incomprehensible and or not as expected by users, in many cases, it would not be consistent with their tendency.

The number of clicks and navigation should be as minimal as possible from the point where the security threat facing the user is presented or identified to the point where the user is provided with adequate security information and recommended usage about the risk.

From the design point of view, if the number of clicks or the required navigation that the user needs to follow in order to know the security risk and make the decision is more than expected, it may lead to reduce the user's interest in the issue and hence persuade the user to act in a careless manner, leading to an increased risk of the users' data or IT system being compromised.

For instance, in the experimental Wi-Fi interface study mentioned in the previous chapter, only one link was offered to the users to acquire more information about each presented Wi-Fi network in the interface that leads to a security panel which provides more explanation of security features of the explored Wi-Fi network. However, there are still a number of users who selected the Wi-Fi network based on the status of the security meter and later after they made their selection, they click on the link "*Click for more information*" to acquire more information about the network that they had already selected.

5.4.6 Principle 6: Aiding the Decision Latency

Aim: To minimise the time the users spends assessing the information and making their decision without looking for further information.

Guideline 6.1: The process of making the user aware of the risk should be as simple and streamlined as possible. For example, the message should not contain more than 25 words length.

Guideline 6.2: The time required for users to spend assessing the information and making the decision, without the need to search for further information in order to understand the security risk encountered, should be as minimal as possible.

Simplifying and curtailing the process of making the user aware of the security risk to help the user to make an informed decision is a key factor here. The time required for users to spend on assessing the information and making the decision without the need to search for further information, is a critical factor, particularly when faced with time pressure where the chances are high that users tend to make hasty decisions that may lead to compromise their IT systems.

5.4.7 Principle 7: Level of Detail and Clarity

Aim: To provide a suitable level of detail and clarity to the user in order to ensure they are fully aware of the security issue encountered and able to make better-informed decisions.

Guideline 7.1: The user should be presented with enough information (ideally directly, but alternatively via a link) to know what is happening and (where appropriate) make an informed decision.

Guideline 7.2: The level of detail and clarity should assist the users without confounding them with unnecessary or superfluous details.

The detail and clarity about the security risk are vital in helping the user by giving full disclosure of the related information about the security risk encountered. However, the level of detail and clarity differs from once scenario to another. It could be argued that this principle is based on the amount of information that is required to inform that user and essentially making the user aware of the security risk, without overwhelming the user with superfluous information.

5.5 Use and Benefits of the Design Principles

As mentioned in the previous chapter, the use of security aids/tools/features, allows the user to make more educated decisions regarding their information security. Using the principles and the guidelines provided will allow developers to enter the mindset of using such features when designing their applications which would in turn assist user awareness via a more targeted approach.

The main objective of the introduced design principles and guidelines is to educate users and increase their awareness regarding prominent security threats. This can be achieved by applying the identified design principles and guidelines when developing the interfaces of applications, which can provide support to users at the point of need, so they fully recognise the encountered threat, in order to take the necessary security precautions and make informed decisions.

There is no doubt that consistency is a crucial and key issue for users. For this reason, one of the utmost important benefits of these principles, is that the UI elements suggested by the design principles and guidelines are based on the utilisation of existing tools and features of the IT systems that are used by developers. Furthermore, this helps eliminate any confusion that may occur to users with the use of unknown tools or features. For instance, they are intended to use notifications, signs and warnings or sounds for events of interest or concern, which users are familiar with. They are not intended to impede users from performing everyday tasks, but to give users the freedom to navigate and perform actions without hindrance or obstruct. It is no wonder that if the design is generally inconsistent, it will cause frustration which leads to poor user experience, and thus less user interest in security. Therefore, the design should always aim to eliminate confusion at every point when dealing with the system wherever possible.

The design principles identified are intended to provide recommendations and support that assists all type of users when they are unsure about decisions and their implications. It also focuses on educating users, making them aware of the security threat they face to prevent a problem from occurring in the first place. The aim is to prevent users from becoming victims by providing sufficient information to users before taking actions.

Another benefit of the principles is to ensure that only the relevant security information and advice are expressed to users with a suitable level of detail and clarity, and more importantly in users' language without the use of technical terminology, accurately indicate the threat, and constructively provide the appropriate advice to users, in order to ensure they are fully aware to make the necessary decisions they are required to make. This can be achieved by ensuring that security guidance and feedback are available when necessary, and to provide effective information that can help the user make security-focused decisions.

The design of security interfaces should aid to minimise the cognitive load of users when using IT systems. Numerous studies conducted over the years on human cognition have underlined limitations in working memory and the necessity to support users, and work within memory and thought restrictions. This may encompass the automation of security procedures, actions or configurations, the ease of setting up the security system, and ultimately the demands should be reasonable and within the memory capacity of the users (Nurse et al, 2011).

With the evolving threats in the security landscape and in many cases, by the time users tend to forget key points related to security of the system, even if security awareness, training and/or education have been provided. For this reason, the identified principles are intended to minimise the user's memory load whilst using the

system by making adequate and relative information easily retrievable whenever needed, recommend action to users to avoid the threats. However, since every extra information competes with relevant information and reduces their relative visibility, the presented information should not contain irrelevant or seldom relevant information.

Finally, these principles and guidelines are general rules of design and will mostly be valid to any platform. Furthermore, arguably, the successful implementation of all the principles will lead to making the user aware of the encountered security threat and consequently aid the user to make informed decisions.

5.6 Comparing Proposed and Existing Usability Interface Design Principles

To discuss the design principles, it is imperative to refer to the most important and well-established design principles in this field, namely Nielsen's usability heuristics (1994) and Johnston et al (2003). These two design principles are the fundamental principles proposed in the usability of IT systems literature to address both usability and consistency issues in the design of user interfaces in general, bearing in mind that the Johnston et al (2003) design principles are specifically for the security environment. Moreover, they are the essential design principles of the user interfaces referred to and appeared to be most commonly cited in the literature.

While the Nielsen's usability heuristics focus mainly on the usability problem, the identified principles and guidelines are to enable security awareness of end users and focusing on utilizing the existing tools and features to educate users, make them aware of the security threats they may face and subsequently help them in making informed decisions. Arguably, Nielsen's usability heuristics are reconciled to some degree with the identified principles in the way that both are focusing on the interface design or the UI elements but the ultimate objective for each one is different.

In comparison, while Johnston et al (2003) design principles address the design of UI elements to focus on the security environment in general as well, the identified principles address a specific issue which is to take into account the increased user security awareness and recommends specific principles that make the user aware of security threats through the development of user interfaces. This is to ensure that this should be taken into account by software developers during the development phase of user interfaces of the applications.

The identified principles also differ but some are intertwined to some degree when compared with those established by Johnston et al (2003). Although these are primarily established to assist in the development and design of interfaces used in a security environment, the identified principles are more security-focused. They also were established and derived from the prior experimental work for the security environment but more specifically are focused on making the users aware of the security threat they encounter. In addition, they have been broken down into guidelines to provide broader and more specific guidance on what and how to improve UI elements in order to increased users' security awareness.

Although both of the mentioned design principles address either the usability problem in general or the usability of the security systems, neither explicitly referred to the problem of security awareness of users. In contrast, the new principles provided broader details of how existing tools are invested and exploited so that they contribute effectively and increase security awareness of end users. Moreover, Johnston et al (2003) principles did not specifically address the lack of provision of adequate information about the security threats, nor the lack of providing recommendations that help users make better decisions which may lead to mitigating the security threats.

To avoid the reoccurrence of guidelines or mixing different concepts which may lead to confusion, it is useful to make a comparison between the mentioned principles. The comparison with the earlier principles and guidelines is requisite in order to inspect the identified principles and to ensure that no important aspect related to UI elements is ignored or neglected. Furthermore, it should be noted that only comparable and intertwined principles have been inspected bearing in mind that the ultimate motivation or objective may differ. Table 3 provides a comparison between the design principles identified from the previous experimental work, Nielsen's usability heuristics and Johnston et al (2003) principles.

Table 11: A comparison between the identified design principles, Nielsen's usability heuristics (1995) and Johnston et al (2003) principles

Source / Comparison criteria	The Identified principles	Johnston et al (2003) HCI-S principles	Nielsen's usability heuristics (1995)
Principle	**Security visuals**	**Visibility of system status**	**Visibility of system status**
Description	Aims to provide users with a clear indication of the current security status, including specific notifications and warnings for events of interest or concern.	It is important for the user to be able to observe the security status of the internal operations.	The system should always keep users informed about what is going on, through appropriate feedback within reasonable time.
Key differences	Although the descriptions are similar, the proposed identified principles are providing detailed description and mentioning to include specific notifications and warnings for event of either "interest" or "concern". They have also been broken down into guidelines for developers and focus more on how to best deliver products which raise the awareness of the user on a security perspective. For example, the colour coding to attract attention and alert the users of the extent of the risk they are facing.		
Principle	**Simplified security explanation**	**Aesthetic and minimalist design**	**Match between system and the real world**
Description	Aims to transmit the message to the users in a manner that would be clear and simple to understand regardless of their vocational inclination.	Only relevant security information should be displayed.	The system should speak the users' language, with words, phrases, and concepts familiar to the user, rather than system-oriented terms. Follow real-world conventions, making

			information appear in a natural and logical order.
Key differences	While the descriptions are also interrelated here, the proposed identified principle is explicitly stating the "target users" by focusing on all users' categories regardless of their skills or level of knowledge of the IT systems in terms of the language used. Moreover, it mentions to the "content" and states clearly that there should be a balance between providing enough information without overwhelming the user. They have also been broken down into two guidelines Guideline 3.1 and Guideline 3.2 to better deliver security features within their software products that help to raise the awareness of the user.		
Principle	**Level of detail and clarity & Proposed recommendation**	**Errors**	**Help users recognize, diagnose, and recover from errors**
Description	The first principle aims to provide a suitable level of detail and clarity to the user in order to ensure they are fully aware of the security issue encountered, and able to make better-informed decisions, while the second principle recommends an action in order to avoid/minimize the risk implicated to the security issue.	It is important for the error message to be detailed and to state, if necessary, where to obtain help.	Error messages should be expressed in plain language (no codes), precisely indicate the problem, and constructively suggest a solution.
Key differences	While the identified principles are clearly suggesting to provide a "suitable" level of detail and clarity to the user to make the users aware of the security issue encountered to make better-informed decisions, and the second principle suggesting to "recommends" an action in order to avoid/minimize the risk implicated		

	to the security issue, Johnston et al (2003) is talking about error messages which is something different because error messages are not the same as the warning message and Johnston et al 2003 further suggested that the message to be "detailed" and did not state to which level of details it should be as providing too much details to the users may not be understandable by all users categories. Whereas Nielsen description is suggesting to provide a constructive solution and this different when compared to recommendations. Nielsen and Johnston et al principles are not explicitly intended to increase the users' security awareness.		
Principle	**Minimal intrusion**	**Learnability**	**Flexibility and efficiency of use**
Description	Intervention and/or alert should attempt not to inhibit the user from completing their everyday tasks.	The interface needs to be as non-threatening and easy to learn as possible.	Accelerators -- unseen by the novice user - may often speed up the interaction for the expert user such that the system can cater to both inexperienced and experienced users. Allow users to tailor frequent actions.
Key features and differences	While both Nielsen and Johnston et al (2003) description is stating that it needs to be as user-friendly, as easy-to-learn as possible and interactive, the identified principles are also suggesting this, plus the fact that it must not interfere with the completion of the user's tasks. They have also clearly state that the number of clicks should be as minimal as possible from the point when the security threat facing the user is presented or identified to the point where the user is provided with adequate security information and recommended usage about the security risk. Furthermore, they have also been suggesting that the warning message should not interfere or affect the other components of the interface, i.e., it should not block, modify, overlap, or make the interface harder to interact by the user.		

5.7 Conclusions

This chapter proposed and discussed new design principles for security features that can be used to improve the security of IT systems by modifying application interfaces to increase the security awareness of users. This objective can be accomplished by educating users about the security threats they are facing and assisting them by providing security recommendations so they can make informed decisions.

The interface design of a system is crucial, especially when it relates to making security decisions in standard IT applications. The new design principles for security features are considered to greatly enhance the users' experience with the security issue and can be implemented to maximize the users' awareness of the security threats.

Furthermore, they can be used to provide the necessary security information and security recommendations without directing the user to make a specific choice. This will result in a system that is fundamentally reliant on making the user aware of the threat which should assist the user to make informed security decisions without any form of enforcement.

Additionally, they can also be used by software developers to ensure that the objective of making "users aware" is developed into the security interface or within the security features of the IT security system. The new design principles and guidelines can also be used to evaluate the interfaces of new security products. Moreover, they can also provide direction, from a security point of view, on how an interface can be improved in the way that helps to make users appropriately aware of the security threat encountered.

Chapter 6

Applying the Design Principles

6.1 Introduction

On the basis of the security design principles discussed and recommended previously, one of the current scenarios has been evaluated in order to determine its consistency with these identified design principles and to have scope for improvement, by using the targeted security awareness-raising approach. In order to support this view, revised versions of the user interfaces are designed for this scenario, which exhibited the shortcomings in this regard and the room for improvement to make the users fully aware of the security risk that they are encountering. It will also measure the new security design adherence to these new security design principles. This chapter discusses the new security design adherence to these new principles and provides an example of adhering to these principles with a view to improving the current design of this application. Moreover, it will discuss in detail this scenario and suggest the potential solutions that may help mitigate the security risks by providing adequate security information and guidance.

6.2 Background

There are several instances and scenarios in which the users find themselves facing security-related decisions. Whilst in such situations, the majority of them do not have adequate security guidance and advice to make the appropriate decisions, which would help them avoid or mitigate the associated security risks that may have to face when dealing with the IT system. One possible solution in this situation is to ensure that security guidance and feedback are available when necessary and to provide

effective information that can help the users make informed and right decisions at the right time to avoid the security risks and its implications. Targeted security awareness raising approach has the potential to be useful in providing the support to users at the point of need, for them to take the necessary security precautions and make informed security decisions. This promising targeted security awareness raising approach can act as the most suitable entity in helping users become fully aware of the security threats by providing security guidance, and recommendations during dealing with tasks in situations in which either inadequate support or help is provided to the users, or in which poor security information and guidance is provided to the users.

It should be noted that this effort is focused on making the users aware of the security risk in some security scenarios using the targeted security awareness approach, in which the existing security features of some applications were identified to have either flaws or shortcomings in making the users fully aware of the security risks. It has been identified that these applications have room for improvements in terms of the required design to provide the necessary and adequate security information and guidelines to make the users aware of the security risk. Therefore, it is beyond the scope of this research to discuss broadly other aspects such as the classification of the suspected blocked emails, the type of the advice that correlated to each type of the suspected blocked emails. However, the main objective of this project is introducing the new concept of using targeted security awareness to make the users aware of the security risks in some scenarios and explore the opportunities in which there is some visibility, in terms of the need to improve the currently used interfaces for some applications in order to help users comprehend the security threats in a better and more effective manner.

The following section will discuss in detail this scenario and suggest the potential solutions that may help mitigate the security risks by providing adequate security information and guidance.

6.3 The Problem and Challenges of Phishing Emails

According to ENISA the threat landscape report (2017), the dominant attack vector for malware infections was phishing. The human link is still considered as a weak link in the phishing infection vector. Therefore, it is imperative to increase security awareness measures to enhance user vigilance (ENISA, 2017). Moreover, according to Ernst and Young (2017), 64% of the surveyed organisations considered phishing to be the main threat that has most increased their risk exposure during 2017 (Ernst and Young, 2017).

Similarly, IronScales (2017) Email Security Report revealed that phishing is responsible for the vast majority of cyber-attacks worldwide. Furthermore, the report also revealed that, among all attack vectors, email is still the most exploited for a variety of reasons. Malicious email continues to easily bypass legacy SPAM filters, firewalls, and gateway security scans that still rely on signatures and scanning of the email content when analysing messages. Moreover, due to human nature, it only requires a few users who are unaware, or even those who are actively engaged in the awareness training programme, to unintentionally provide attackers access to sensitive corporate networks and data. In fact, such users are considered contributing factors as they are easily tempted to download an attachment or click on a malicious email link (IronScales, 2017).

Phishing generally has been a major security problem for a long time without an efficient solution in place (Vayansky and Kumar, 2018). In general, phishing is a practice that deceives users to give their sensitive information to attackers, and to date,

it has not been addressed by existing security industry. The impact of such attacks can be significant. The key to their success is the fact that they exploit what is often mentioned as the weakest link in the system – the end-user (Williams and Li, 2017).

Phishing has been identified by Anti-Phishing Working Group (APWG) as "a criminal mechanism employing both social engineering and technical subterfuge to steal consumers' personal identity data and financial account credentials" (Anti-Phishing Working Group, 2017). Phishing has also described and identified by Phishing.org as "is a cybercrime in which a target or targets are contacted by email, telephone, or text message by someone posing as a legitimate institution to lure individuals into providing sensitive data such as personally identifiable information, banking and credit card details, and passwords. The information is then used to access important accounts and can result in identity theft and financial loss" (Phishing.org. 2018). The problem with phishing is that there are no comprehensive solutions that protect users securely from being phished. While, the anti-phishing defences have been advanced, the phishing techniques have also advanced from simple to more complex methods. As a result, the need for innovative security methods to identify phishing scams is crucial. The problem with phishing is that attackers are continually searching for new and innovative methods and demonstrate the ability to make inventive techniques to trick users to believe that they are dealing or interacting with a legitimate website or email. Phishers have become more capable of producing phoney and fraudulent websites to look indistinguishable, even incorporating logos and illustrations in the phishing emails to make them all more persuading. Additionally, phishers have begun to build a psychology behind their emails which call for urgency, greed, or trust. Combined with the legitimate appearance and feel of the spoofed websites, even more cautious and aware users can be tricked into becoming victims of their attacks. Phishing impacts individuals globally and is conducted internationally, making it hard to track and

prosecute the criminals behind it. One basic method that phishers have used is called ‘fast flux’, where a substantial pool of proxies and URLs is utilised to keep the actual location of the phishing site concealed. By doing this, it is difficult to blacklist the site and the server being utilised takes more work to discover (Vayansky and Kumar, 2018).

More importantly is to increase users' security awareness of this threat, by providing them with a security feature that helps them identify phishing emails in an easy and uncomplicated manner, enabling them to recognise phishing emails to avoid malicious links.

It is irrefutable that the email is the primary method for organisations and individuals to communicate in the present-day. However, this is particularly also one of the most well-known primary methods of conducting cybercrimes, such as identity theft, spreading viruses and breaching users’ accounts. The need to improve the security awareness among computer users of these threats is evident in media reports (Kruger et al., 2007). Moreover, email is both a premium communication tool, and the best inexpensive way that companies are using in the present-day to inform customers about the latest products and services. However, email is often used to deliver unsolicited material that is at best, annoying and at worst, malicious causing considerable harm to customers and their computers (Get Safe Online, 2017). Phishing is also causing significant damage to businesses. For example, according to Forbes, phishing results damage costs US businesses alone around 500$ million every year (Forbes, 2017).

Phishing emails are reaming a popular method of compromising the security of IT systems and most recently are now the main delivery method for ransomware and other malware (Jonathan Crowe, 2016). According to the Verizon 2016 Data Breach Investigations Report, email attachments have become the number one delivery vehicle for malware, with email links coming in at number 3 (Verizon 2016).

Additionally, Clearswift surveyed 600 business decision makers and 1200 employees across the UK, US, Germany and Australia, who ranked phishing emails as the top threat when asked what they observed as the biggest cybersecurity danger to their organisation. In the UK alone, 59% decision makers highlighted email links as the biggest concern for their businesses, and they represent the greatest threat to companies of all sizes. Putting this threat above any other threat, its position reflects the impact that a single malicious email can have on the organisation. One of the key solutions, proposed by Clearswift to mitigate risks and improve email security, is to educate employees on how to recognize phishing emails and other malicious email based tactics used by cybercriminals that will ultimately help ensure the business stays safe. Clearswift also claimed that this needs to be further supported by looking into the processes, policies in addition to implementing and investing in the security technologies to add an extra layer of protection that ensures systems are protected from every angle. (Clearswift, 2018). Table 12 presenting a summary of the state of the phishing email attacks.

Table 12: Summary on the State of Phishing Attacks

Source	Key findings
(Wombat Security Technologies, 2017).	• Phishing attacks continue to grow in size and complexity, supported by more aggressive social engineering practices that make phishing more difficult to prevent. • The organisations surveyed reported that they suffered from malware infections (42%), compromised accounts (22%), and loss of data (4%) as a direct result of successful phishing attacks. • The report found that the most popular phishing attack templates with the highest click rates included items employees expected to see in their work email such as an HR document, or a shipping confirmation. For instance, employees were more cautious when receiving “consumer” emails about topics like gift card notifications, or social networking accounts. However, an “urgent email password change request” had a 28% average click rate.

	• Phishing continues to be a very effective attack vector that is increasingly responsible for a large number of data breaches in the market today. Despite continued investments in a few popular security technologies, phishing messages are still success in reaching end users and can cause serious damages to a company's important data and reputation. • 61% of the surveyed reported experiencing spear phishing. • The impact of phishing attacks can be highly destructive to organisations, with 38% of the surveyed suffered disruption of employee activities, 27% malware infection, 17% compromised accounts and 7% loss of data. • The report found that phishing is still a threat that is evolving, as 76.5% reported being a victim of a phishing attack in 2016 down 10% from 2015, 51% believed the rate of phishing attacks is increasing, which is 15% less compared to 2015, 45% believed the rate of phishing attacks is decreasing and 4% believed the rate has remained the same. • Research conducted in 2015 on the Cost of Phishing and Value of Employee Training by Wombat and Ponemon Institute found that the majority of costs caused by successful phishing attacks are the result of the loss of employee productivity and uncontained credential compromise, among other factors, which together cost an average sized company $3.77 million per year. • Wombat also stated that awareness is growing, however risky behaviours still exist. The survey of the general public revealed that more people are aware of the concept of phishing than it was estimated. However, these same people struggled to identify what ransomware is. Overall, this survey points to the fact that there is work to be done to teach people how to stay safe.
(APWG, 2017).	• APWG saw a steady set of phishing reports and confirmed attack sites in the first half of 2017. • Numerous hundred companies are frequently targeted, every few weeks, while fewer companies being subjected to irregular attacks. Over time, some companies are retreating completely from lists, replacing them with new and up-and-coming targets of opportunity. • Phishing attacks have occurred frequently in the Payment, Financial, and Webmail sectors. • There has been an increase in phishing attacks using free hosting providers or web site builders. APWG contributor PhishLabs has examined what type of resources phishers choose to use. According to Crane Hassold, Manager of

	Threat Intelligence at PhishLabs, there has been an increase in the number of phishing attacks using free hosting providers or website builders, which is not only easy to use and cheap, but also allows threat representatives to create subdomains spoofing that targeted brand, resulting in a more legitimate-looking phishing site. Free hosts provide an additional level of anonymity, as these services do not make registrant information readily available, including some of the most common hosts used by phishers. 000WEBHOST.COM, MYJINO.COM, and FREEAVAILABLEDOMAINS.COM. The number of Free Hosting attacks was increased to 1,939 in June 2017 compared to 1,323 seen in January 2017. • Of the 7,990 phishing incidents reported, many were spread via Facebook. Half were hosted in the United States, followed by Brazil, as identified by ASN (autonomous system number, or network). • The number of unique phishing websites detected in June 2017 was increased to 50,720 compared to 42,889 in January 2017. • The number of unique phishing email reports (campaigns) in June 2017 was decreased to 92,657, compared to 96,148 seen in January 2017. • PhishLabs found that the number of domain names used fluctuated from month to month as various phishers used different methods to create and mail out phishing URLs. The number of domain names used in attacks was increased to 18,404 in June 2017, compared to 13,977 in January 2017.
(Wombat Security Technologies, 2018).	• 76% of the surveyed infosec professionals reported that their organisation experienced a steady or higher volume of phishing attacks in 2017 compared to 2016 statistics. • 53% of infosec professionals reported that their organisation has experienced spear phishing in 2017. • The report revealed that organisations are using different types of tools to train end users to recognize and avoid phishing attacks. In this regard, the number of organisations using Computer-Based Awareness Training was increased in 2017 to 79% compared to 62% seen in 2016. The number of organisations using Phishing Simulation Exercises was 68%, and 46% used Awareness Campaigns (Videos and Posters), 45% used In-Person Security Awareness Training and 38% used Monthly Notifications or Newsletters. • The report found that UK organisations tend to rely on once-a-year training models and passive security awareness

	training tools like (videos, newsletters, and email notifications) compared to their US counterparts which are mostly rely on interactive training. • With regards to the phishing impacts, the report revealed that the phishing impacts were more broadly felt compared to what is seen in 2016, with more than 80% increase in reports of malware infection, compromise, and loss of data associated with phishing attacks. • Types of phishing emails that are people falling for are including consumer emails, corporate emails, commercial emails and cloud emails. • In regards to the most successful phishing templates, the report found that although the click rates were dropped to an average, the combat against phishing is undoubtedly continuing. The report revealed alarmingly figures of a high failure rates regarding the themes and topics that are most tempting to end users. In this regard, the most successful simulated phishing templates were including Online Shopping Security Updates with a rate of 86%, Corporate Voicemail from Unknown Caller with a rate of 86% and in addition to a rate of 89% Corporate Email Improvements.

6.4 The Need for Raised Awareness of Spotting Phishing Emails

There is no surprise that the main tools currently used as the first line of defence in combating phishing emails, are the filtering algorithms and tools that are used by email applications. However, there are some flaws that require improvement in this first line of defence. For example, some legitimate emails are often classified as spam or phishing emails and some spam or phishing emails may be classified as legitimate emails. It should be mentioned that it is out of the scope of this research to examine the performance or the reliability of the algorithms used in the email filters, but rather it focuses on how to make users fully aware of the phishing email in the case that the email reaches the users' mailbox.

Users receive phishing emails almost every day. However, there is a lack of support to raise the security awareness for the users in the case that the phishing email has

reached their mailbox. The current information provided to users regarding these phishing emails are often inadequate and sometimes misleading which makes it harder for users to be appropriately aware of the threats. This flaw and shortcomings are hindering the efforts to make users aware of the phishing emails threats and therefore users in such situations may not able to take the appropriate security precautions that help to protect them from the associated threats.

Users of the email application are provided with a means to block emails before reaching their mailbox or moving them to a junk email folder, however, they are not appropriately informed, warned and made aware of what the spam or phishing emails actually are.

Email services are among the preferred methods for cybercriminals to target users. To protect users, there are many tools and solutions that have been developed to keep users from being victims of cyber criminals. The majority of these tools and solutions are covering one side of the picture which is the technical side, and have not done enough in terms of increasing security awareness of users by informing them about potential risks associated with blocked phishing emails, and phishing links and attachments before they take actions that unblock the content. Increasing the awareness of users before unblocking any content is a key factor to avoid users becoming victims of this attack, and to avoid any possible security implications.

There is currently no adequate security guidance and feedback available within the email applications that provide support and help to users to make the appropriate security decision to protect themselves from the security risks associated with blocked email messages, which could potentially be scam or phishing emails. The currently available option is only alerting the user in an inadequate manner by informing the users that the email has been blocked. However, what is actually missing in this

situation is to provide appropriate security guidance accompanying this risk. Furthermore, at this point, users need an appropriate security guidance to take the required security countermeasures that would mitigate the security risks which would help to protect them from the potential risks.

Two of the candidate applications that have been evaluated and identified with flaws and shortcomings in making users appropriately aware when a phishing email reaches their mailbox, are the Microsoft Outlook and YAHOO email.

The next section provides an example of the proposed solution and provides illustrative examples of how the current interface design of the Microsoft Outlook application can be improved by applying the identified design principles and guidelines.

6.5 Proposed Solution for Combating Phishing Emails

Phishing is growing and it evolves to avoid detection and bypass defences (Vayansky and Kumar, 2018). Users receive phishing emails on a daily basis. However, there is a lack of support to raise the security awareness for the users in cases where the phishing email reached the user mailbox. The current security guidance and the security information provided to users regarding these phishing emails are inadequate, which makes it harder for users to recognise and be aware of the phishing emails threats. This flaw and shortcomings can be perceived to be an effort obstacle to make users aware of the phishing emails threats in the first place. Therefore, users in such situations may not be able to take the appropriate security precautions to avoid risks associated with the phishing emails.

In order to combat phishing emails and mitigate its implications, Figure 73 illustrates the proposed anti-phishing solution in which phishing emails can be combatted by adopting targeted security awareness-raising approach as the last protection stage

designed to increase security awareness for users if a phishing email arrived in the users' mailbox.

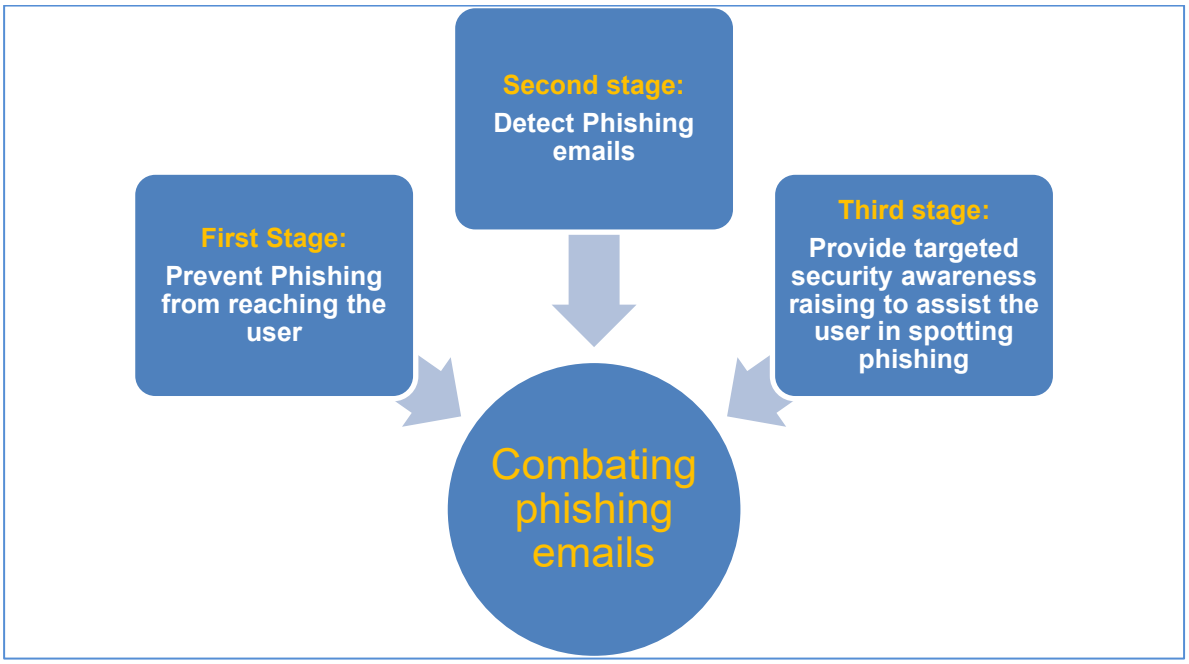

Figure 73: Proposed solution for combating phishing emails

Prevent Phishing from reaching the user

- *Block malicious and phishing websites.*
- *Filter phishing emails.*

Detect Phishing

- *Use indicators in web browsers.*
- *Use anti-phishing tools and solutions.*

Assist users in spotting the Phishing emails when they reach users' mailbox

- *Provide a clear classification of the blocked emails.*
- *Provide a clear notification to spot the phishing email.*

- *Provide adequate security information and advice to users about the blocked email to make them fully aware of the threat.*
- *Provide a feature for the user to learn more information about how to recognise phishing emails.*

The first stage in combating phishing emails is to prevent them from reaching the user at the first instance by filtering out phishing emails. There is no doubt that the main tool currently used as the first line of defence to achieve this, is the email filtering algorithms and tools that are used by email applications. However, there are some flaws that require improvement in this first line of defence. For example, in many cases, email filters failed to detect and accurately identify phishing emails, since attackers use sophisticated methods to bypass the employed defences and reach unprotected and unaware users, there is a possibility that they succeed in their try in case the employed tools and algorithms are unsuccessful to prevent the phishing emails from reaching the users mailbox.

The second stage is to accurately identify the phishing emails. As per current performance of the email filters, there is a lack in accurately identifying and classifying the phishing emails, which results in many cases the phishing success in bypassing the employed defences and reaches the users' mailbox. For example, some legitimate emails are being classified as spam or phishing emails and vice versa.

While the first two stages are proposed here to address the technical aspect of the problem, the third phase proposed to address the lack of security awareness of the end users in spotting phishing emails. Therefore, it should be mentioned that it is out of the scope of this research to examine the performance or the reliability of the algorithms used in the email filters and discuss in detail the prevention and the detection tools and

mechanisms used for preventing and detecting phishing emails. The objective of this research is to focus on adopting targeted security awareness-raising approach to make users fully aware of the phishing email message when it arrives a user's mailbox.

The third stage is based on making improvements in the current user interfaces of the email applications in spotting phishing emails, by applying the identified design principles and guidelines. The first step in this stage is to provide a clear classification of the blocked email, the second step is to provide a clear notification to spot the phishing email, and the third step is to provide adequate security information and advice to the users about the blocked email to make the user fully aware of the risk. The fourth step is to provide a feature for the user to learn more information about how to recognize phishing email messages.

6.6 Evaluation methods

The usability of the current Microsoft Outlook interface design was assessed using an informal cognitive walkthrough method. The current interface design has been inspected, and some aspects have been identified that could be improved based on the proposed design principles and guidelines described in Chapter 5.

The Cognitive Walkthrough has been defined in many ways as presented in Table 13.

Table 13: Different definitions for Cognitive Walkthrough method

Source	Definitions
(Wharton et al., 1994).	The Cognitive Walkthrough is a usability inspection method that focuses on evaluating a design for ease of learning, particularly by exploration.
(usability.gov, 2018).	An inspection method for evaluating the design of a user interface, with special attention to how well the interface supports exploratory learning, i.e., first-time use without formal training. The evaluation is done by having a group of evaluators go step-by-step through commonly used tasks. It can be performed by evaluators in the early stages of design, before performance testing is possible.
(usabilitybok.org, 2018)	The cognitive walkthrough is a usability evaluation method in which one or more evaluators work through a series of tasks and ask a set of questions from the perspective of the user. The focus of the cognitive walkthrough is on understanding the system's learnability for new or infrequent users.

As per Whitten and Tygar (1999), in order to conduct a cognitive walkthrough, the evaluators need to go step-by-step through the software as if they were novice users, trying to mentally simulate what the novices' understanding of the software would be at each point, and looking for potential errors and areas of confusion. As an assessment tool, cognitive walkthrough focuses primarily on the user's ability to learn, and as such, is an appropriate tool for assessing the usability of security.

While the provided analysis in this chapter is primarily described as a cognitive walkthrough, it also combines aspects of another technique, primarily heuristic evaluation. In this technique, the user interface is assessed against a specific list of usability principles. The Heuristic assessment is ideally performed by people who are experts and are very familiar with both the application area and the techniques and requirements of use such as background of people expected to use the program (Whitten and Tygar, 1999).

6.7 Improved Interface Design of Spotting Phishing Emails Using the Proposed Design Principles

The identified design principles and guidelines proposed for targeted security awareness have been introduced and discussed in detail in the previous chapter. The reason for proposing these design principles and guidelines is to assist in the development and the design of interfaces that are associated with the security environment, and particularly treating and overcoming the flaws of the user interface design, by ensuring that the users are provided with the necessary information that makes them aware of the risks they may encounter. These design principles are identified from the prior experimental work. They have been established and introduced to address the essentials in a security environment and in particular to serve the objective of increasing users' security awareness through improving the security features that are included in some applications that users deal with on a daily basis. These principles are perceived as a security domain-specific user interface design that focused on specific design issue in the security environment which should make them easier to comply with and be implemented.

In the next section, some of the design principles are discussed in more detail by illustrating the current interface design of the surveyed applications, and the improved interface design of Microsoft Outlook using the proposed design principles, which should assist the user on how to spot phishing emails and provide a clear indications and enhanced security visuals of the security risks associated the suspected blocked email.

6.7.1 Applying Principles 1 and 2: Severity of the Security Risk and the Security Visuals

The interface should always keep users informed about the current state of the security risk through the use of appropriate visual indications before taking any actions.

Currently, in order to identify and inspect the sender's email, users need to click on the sender's email address and determine whether the email is from a legitimate address. Figure 74 shows the only way that users can inspect and identify the sender's email address using the current version of Outlook. Although it has been detected as a phishing email in this case, it does not provide any security information or guidance for the user before or while making a decision to unblock the email content.

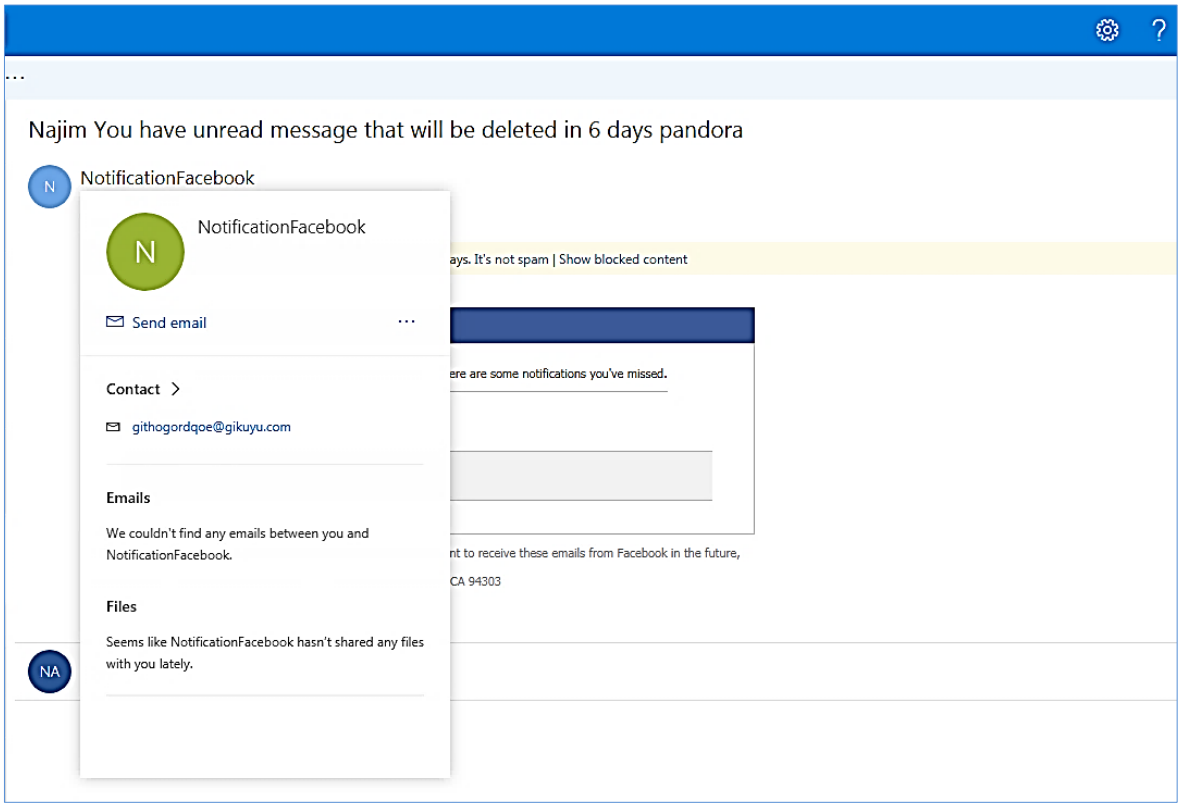

Figure 74: Inspecting the sender's email using MS Outlook taken in 2017

In such situation, it is unlikely that novice users or users with average computer skills would have the experience to take these security precautions. It would be challenging for them to identify and inspect the sender's email address, given the lack of awareness.

The screenshots presented in Figures 75, 76, 77, 78 and 79 are illustrating some examples of the current notifications used by Microsoft Outlook to inform the user about the blocked emails.

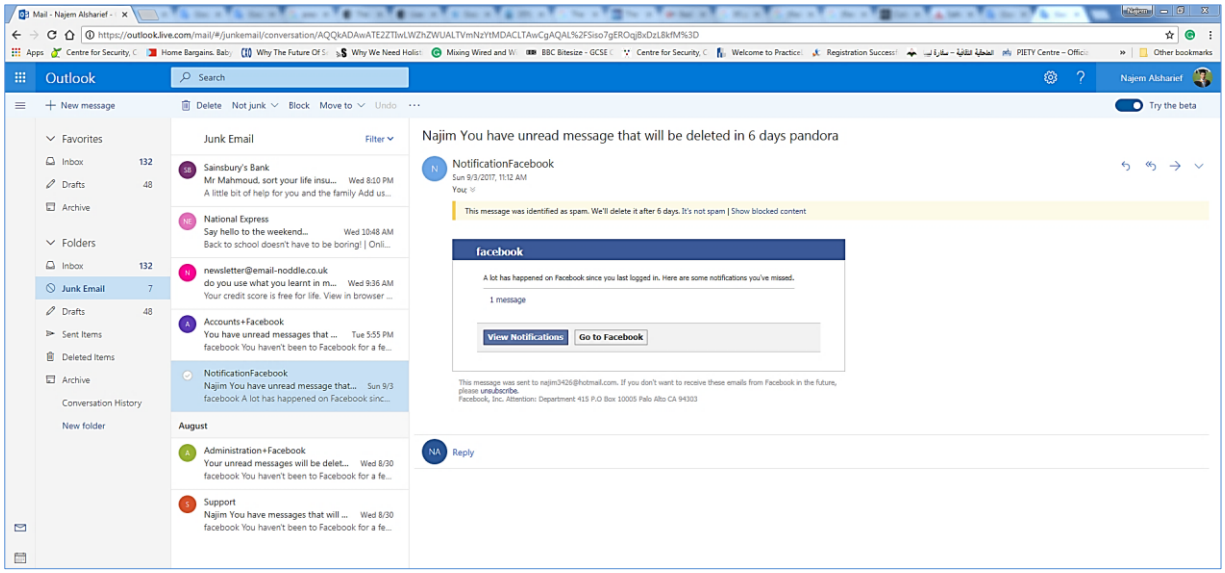

Figure 75: Detecting phishing email in Microsoft Outlook

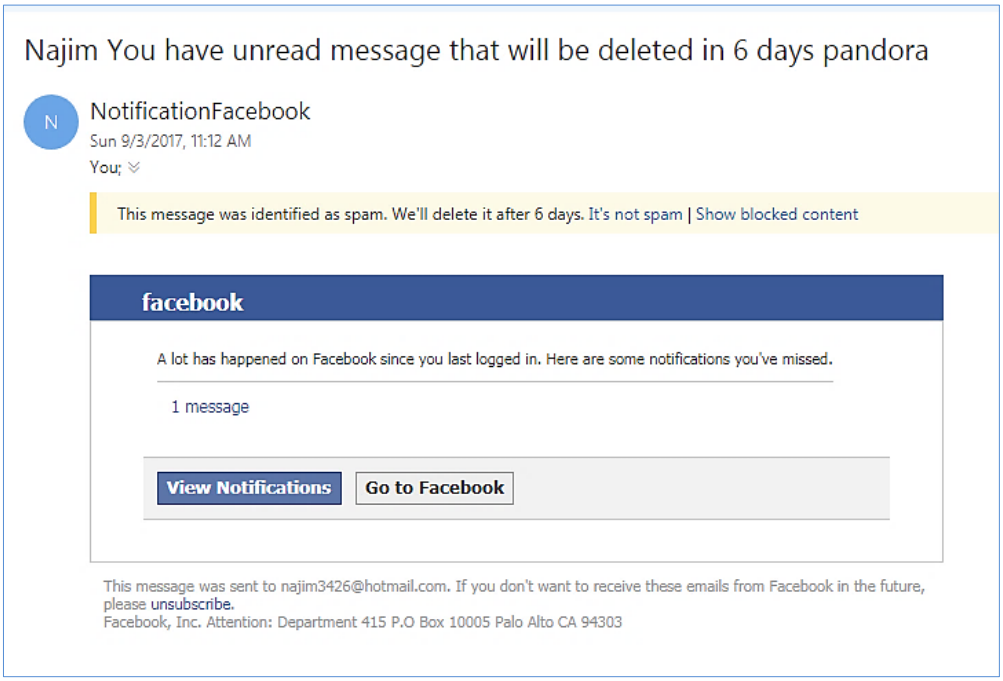

Figure 76: The current Microsoft Outlook warning message for blocked email

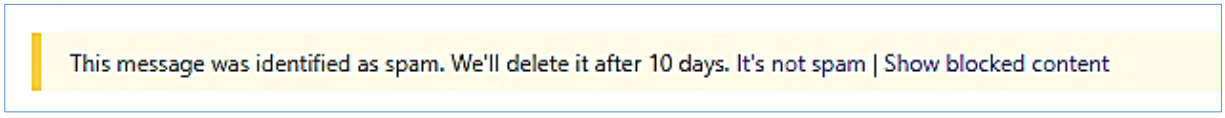

Figure 77: The used warning message for blocked email by Microsoft Outlook

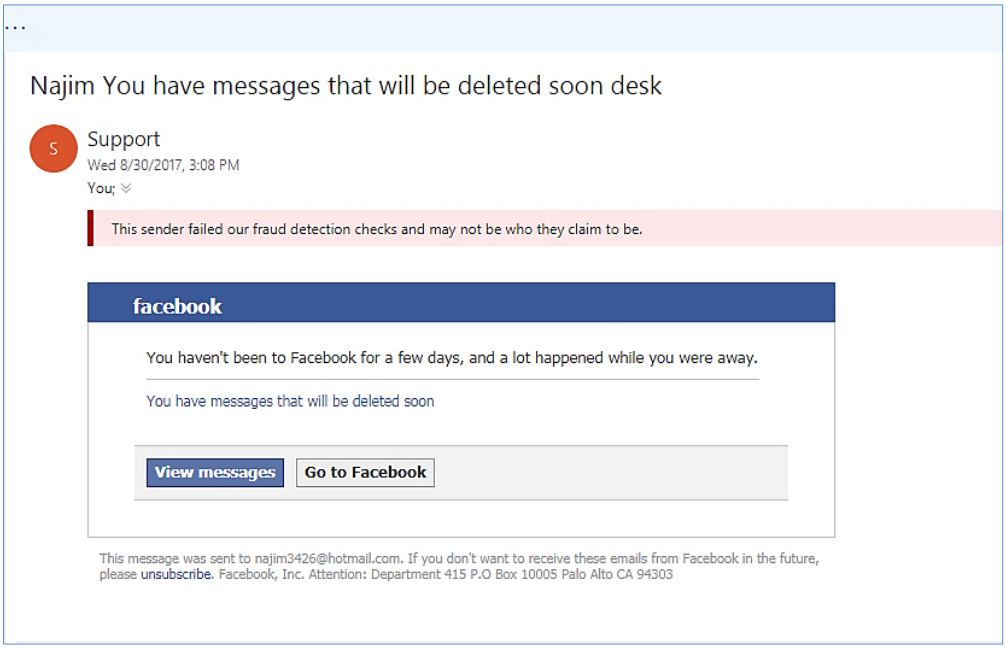

Figure 78: Different warning message for blocked email by Microsoft Outlook

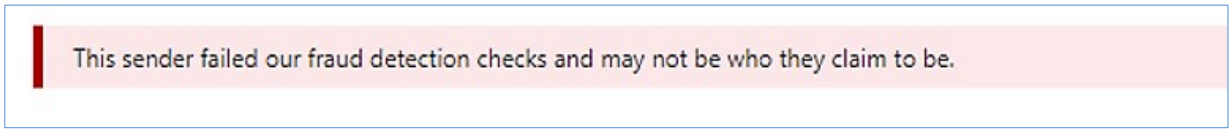

Figure 79: The used warning message for blocked email by Microsoft Outlook

Another application examined is the YAHOO email application. In contrast, YAHOO email has not done better in terms of informing the users about the potential risks associated with the phishing email as per screenshots are shown in Figures 80 and 81. Moreover, YAHOO email's current version is not offering the user any type of clear security notifications when a suspected phishing email reached the user mailbox. On the other hand, in some cases, it warns the user by providing a vague warning message only when the user clicks on an active link in the blocked email as per screenshot is shown in Figure 82. Furthermore, it did not provide any means of security information and security guidance for the user to access if in doubt, to assist the users to understand the risk and the consequences of clicking or reacting to this potential phishing email. Additionally, it failed to provide this opportunity in other cases of

blocked emails which were phishing emails as per screenshots are shown in Figures 83 and 84.

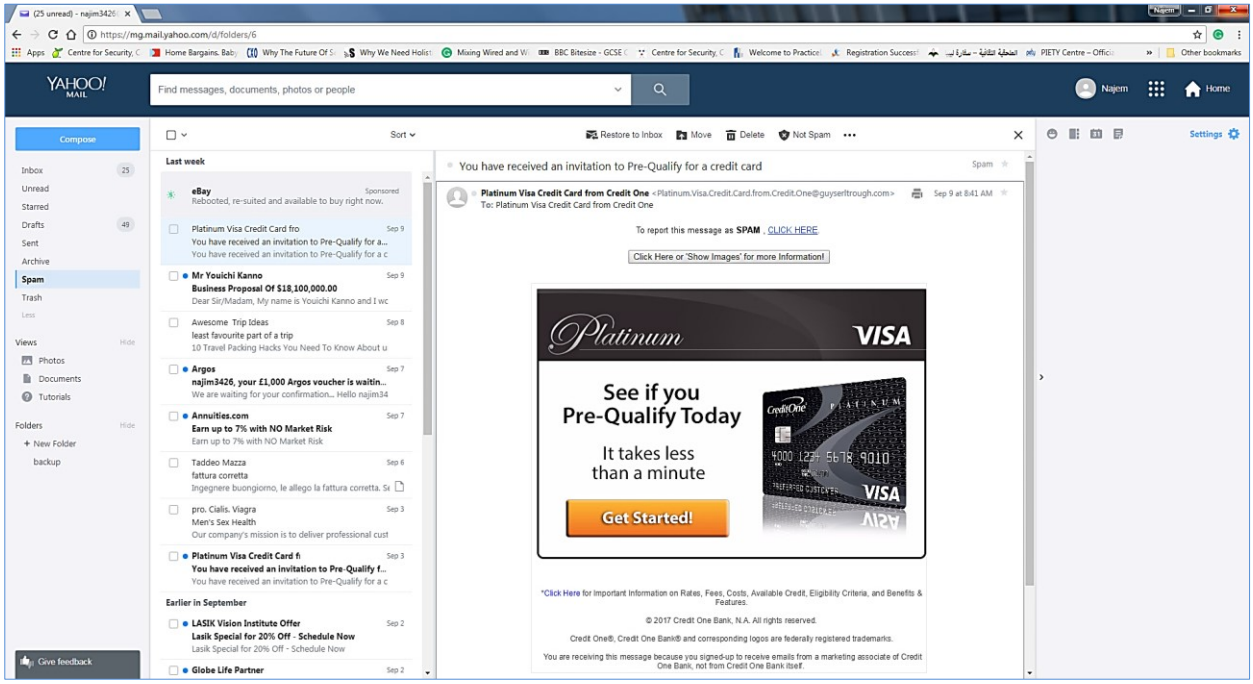

Figure 80: Detecting phishing email in YAHOO email

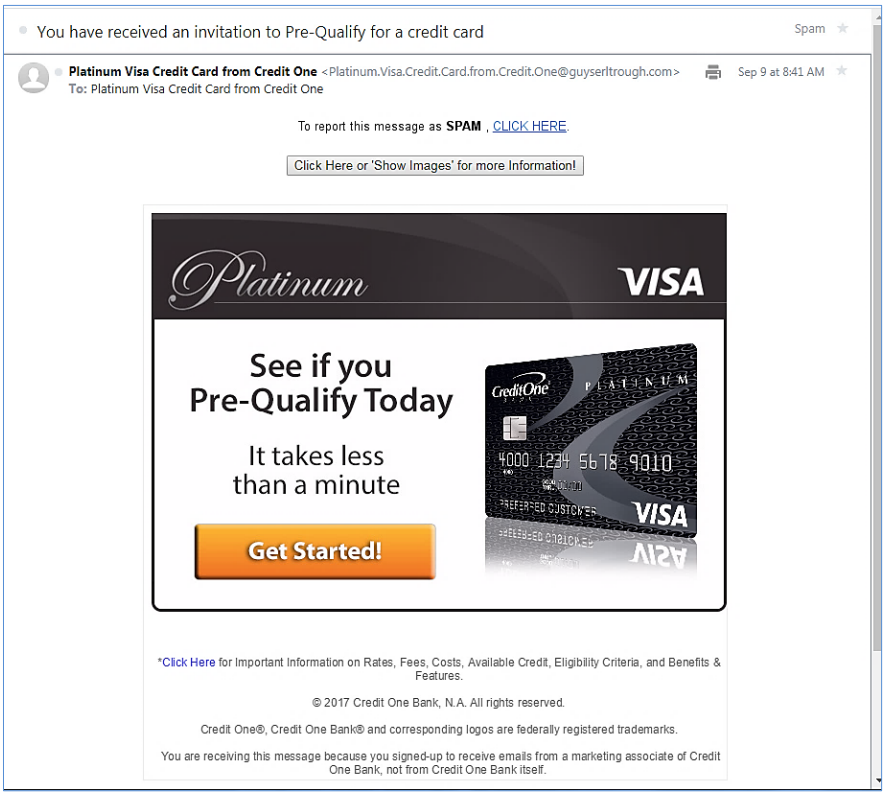

Figure 81: Blocked email content by YAHOO email

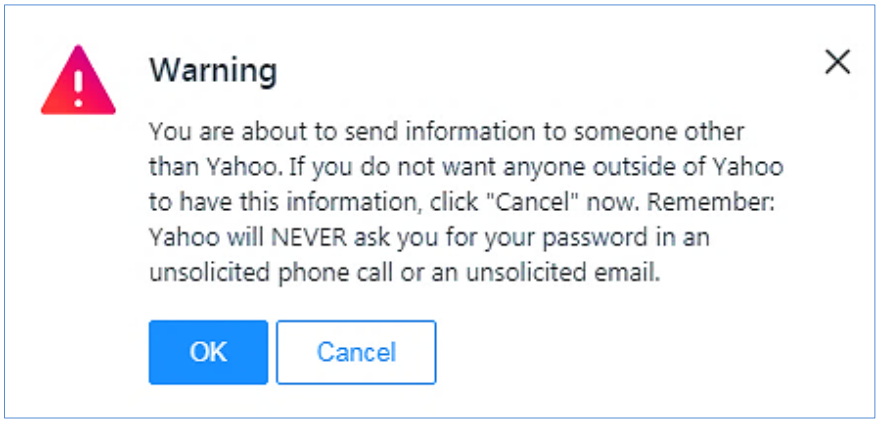

Figure 82: Warning message by YAHOO email when clicking on a link in a blocked email

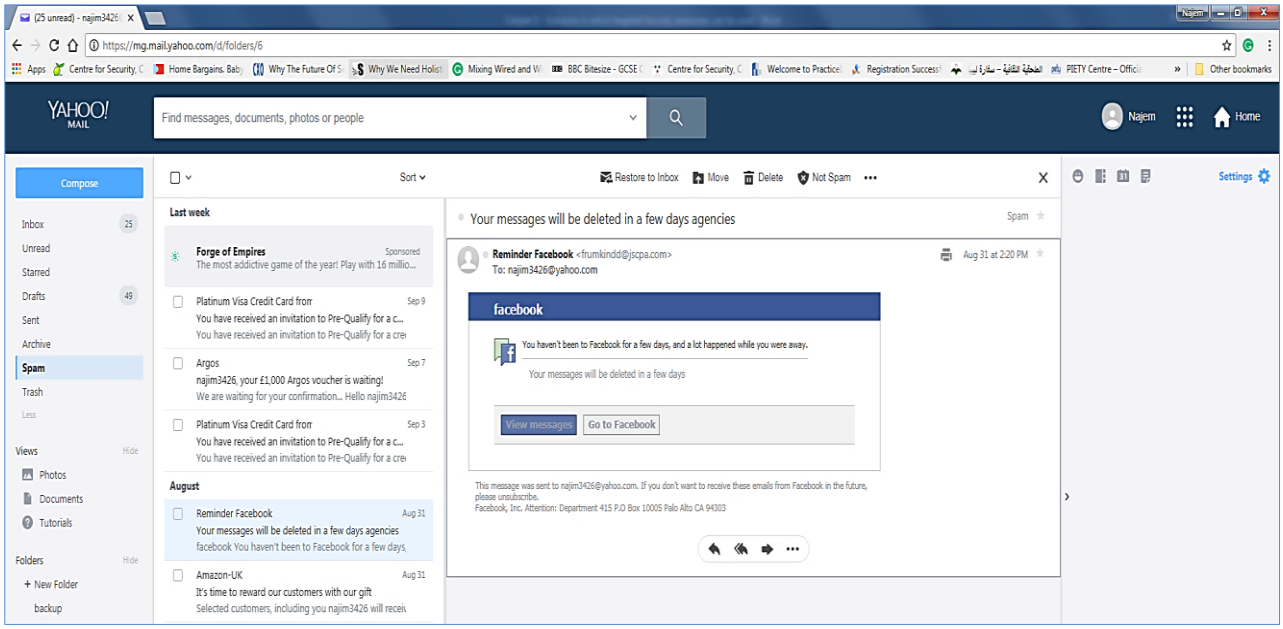

Figure 83: Blocked email content by YAHOO email

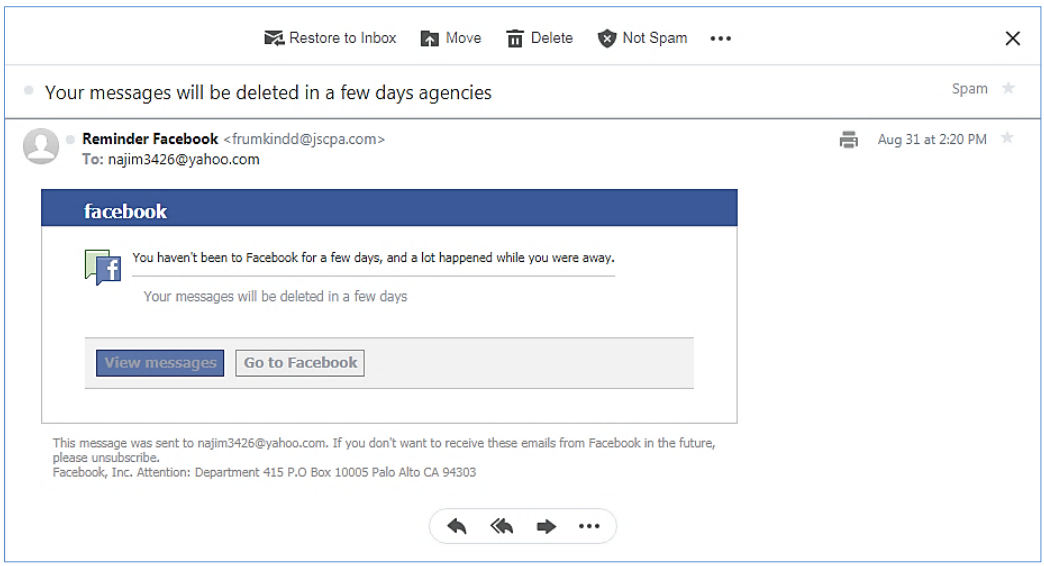

Figure 84: Blocked email content by YAHOO email

Clearly users should be alerted to the severity of the security risk of the blocked email, to avoid confusion to the user. Users should also receive a clear indication of the current security status, including notifications and warnings. This will allow the user to easily observe the security risk of the blocked email. An example of this is the use of varied banners with background colour codes to attract attention and signify the severity of the security risk and/or inform the user whether the email is from a trusted sender. This should be accompanied with suitable warning signs, for example by using coloured warning triangles which all users are familiar with, which is displayed in the left corner of the banners as shown in Figures 85, 86, 87, 88, 89, 90, 91 and 92, to attract attention and signify severity. This should persuade the user to take the required precautions and appropriate actions. This proposed clear visible security warning message should help users to comprehend the security risk quickly and make them aware of the risks in a consistent manner.

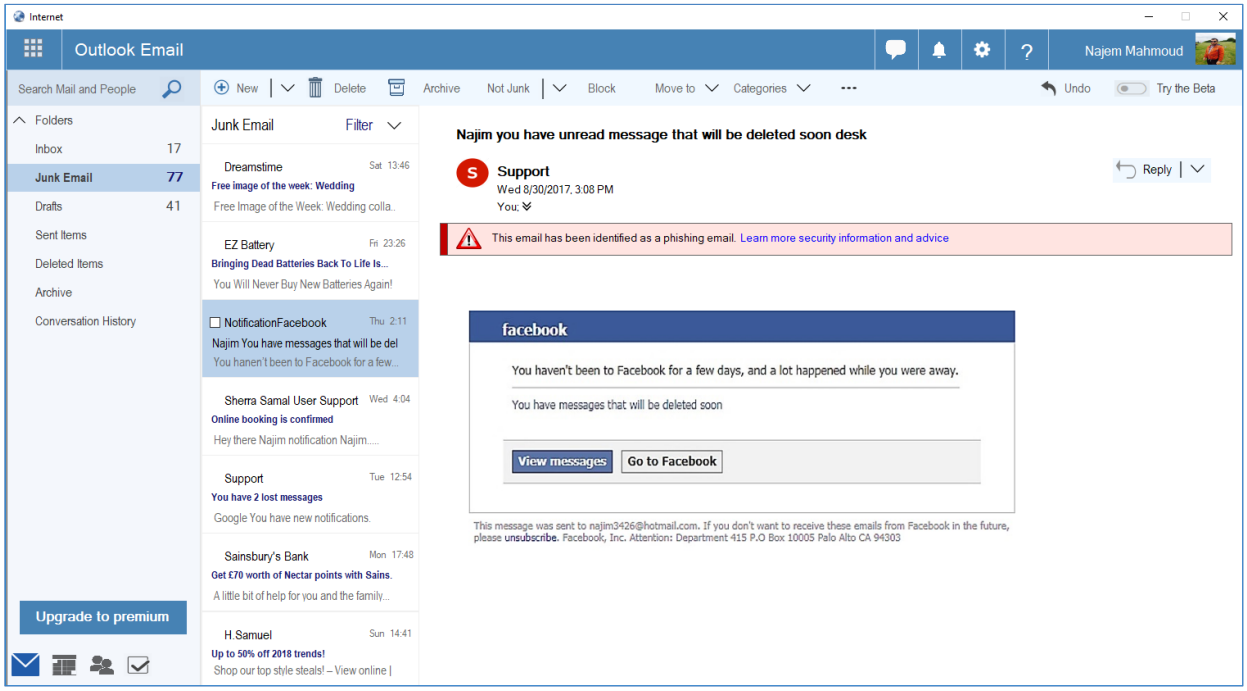

Figure 85: Proposed warning message when a phishing email is identified

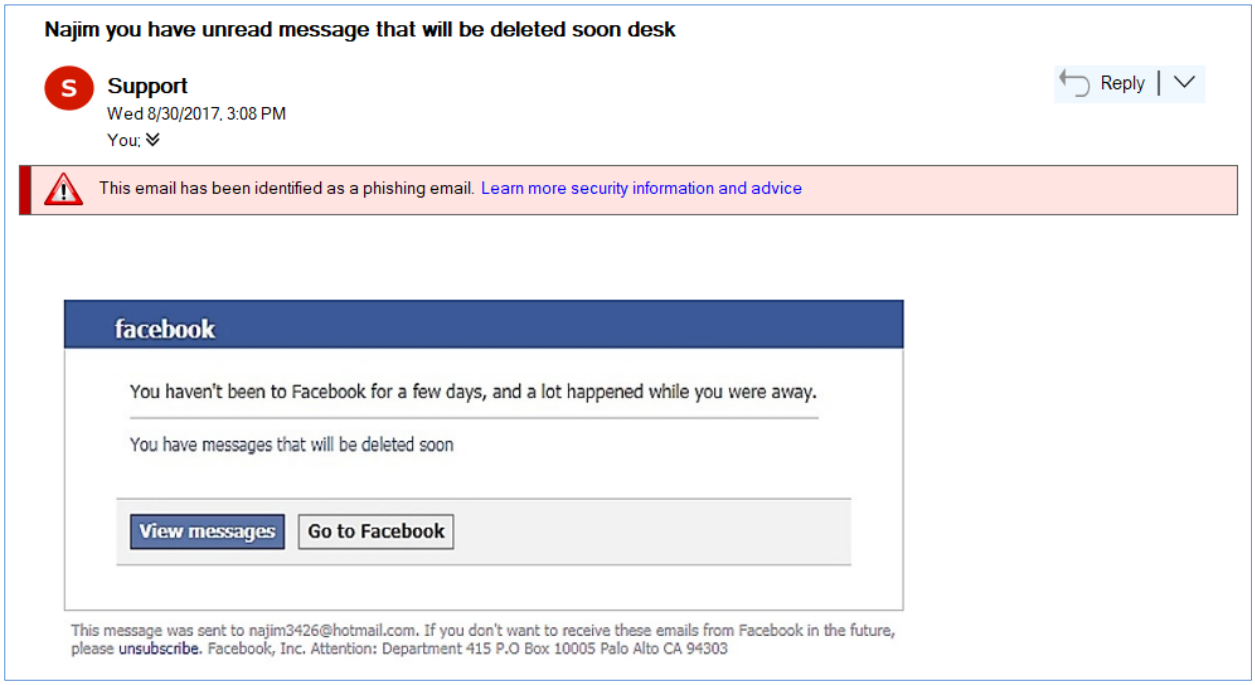

Figure 86: Proposed warning message when a phishing email is identified

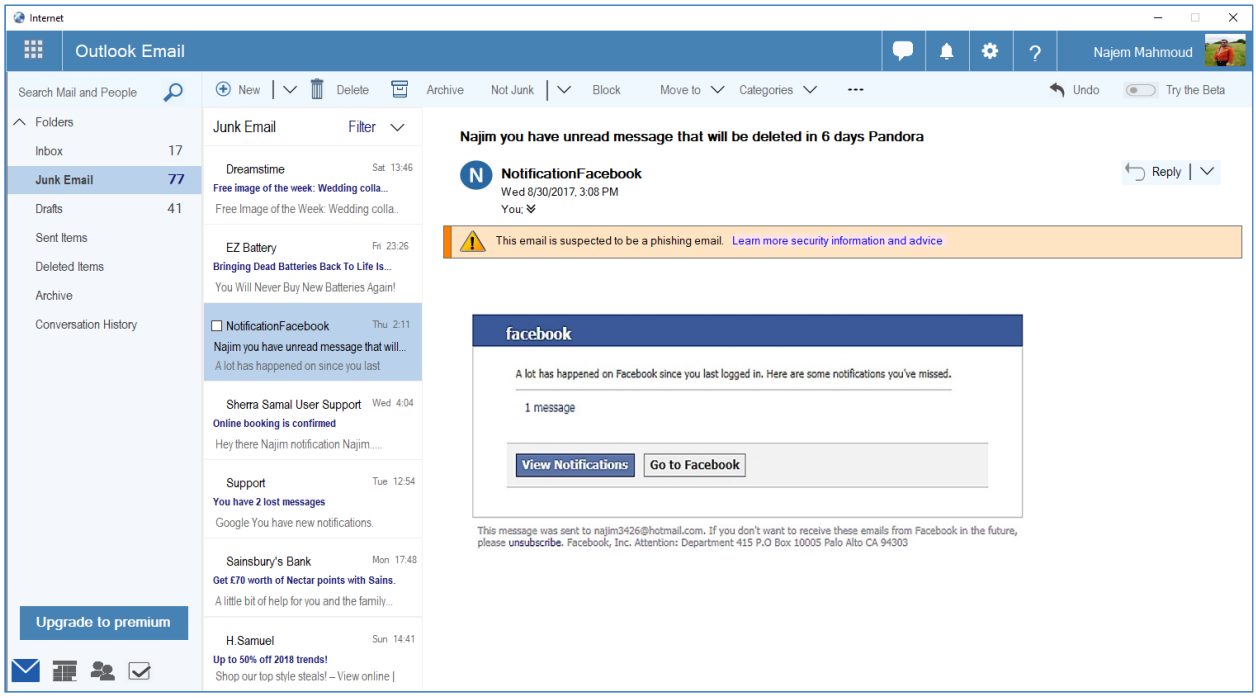

Figure 87: Proposed warning message when a suspected phishing email is detected

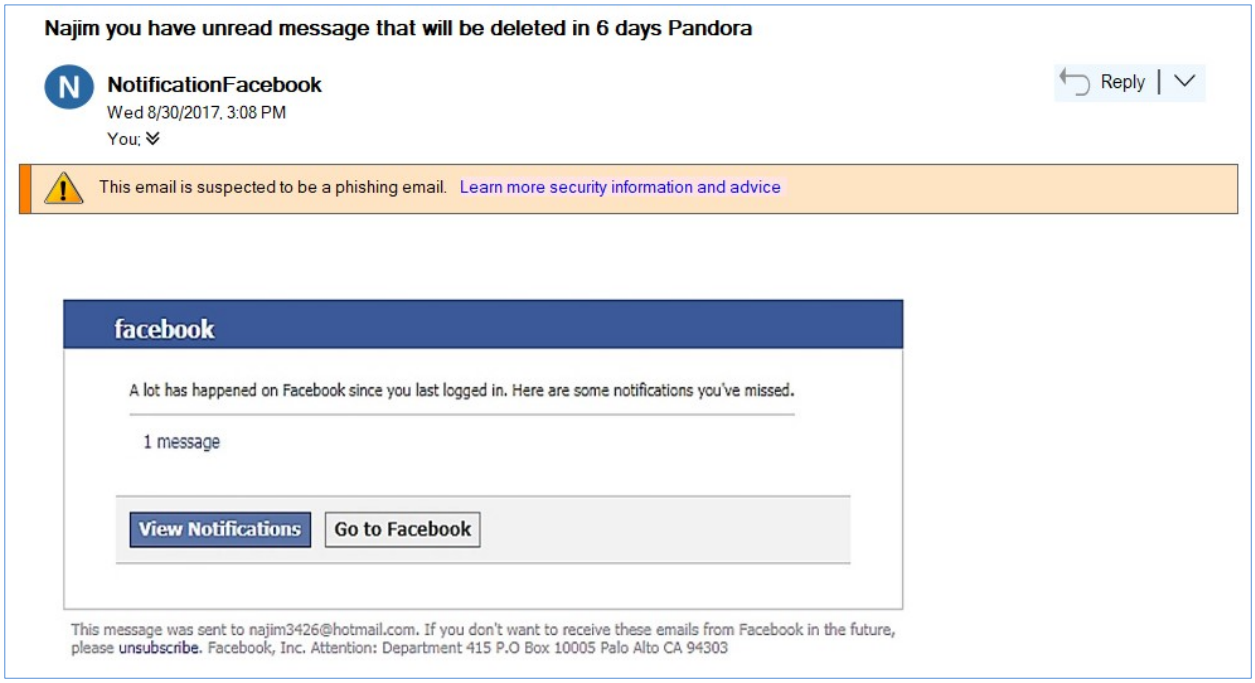

Figure 88: Proposed warning message when a suspected phishing email is detected

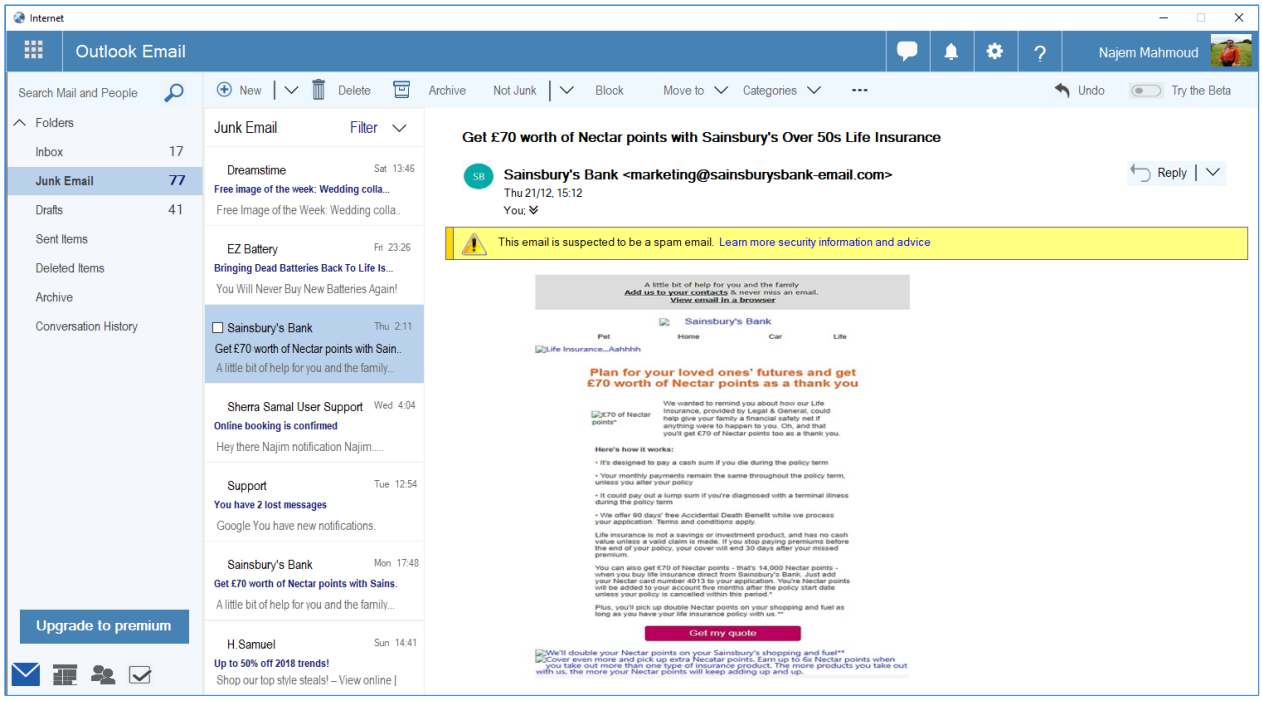

Figure 89: Proposed warning message when a Spam email is detected

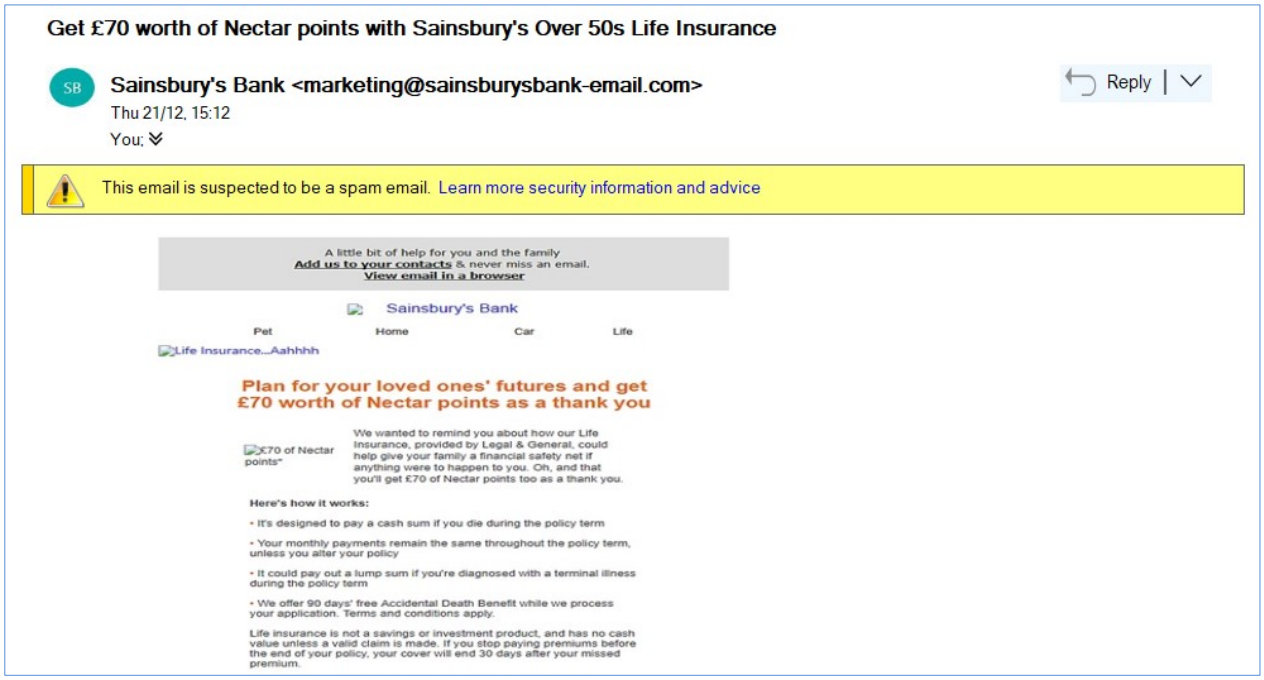

Figure 90: Proposed warning message when a Spam email is detected

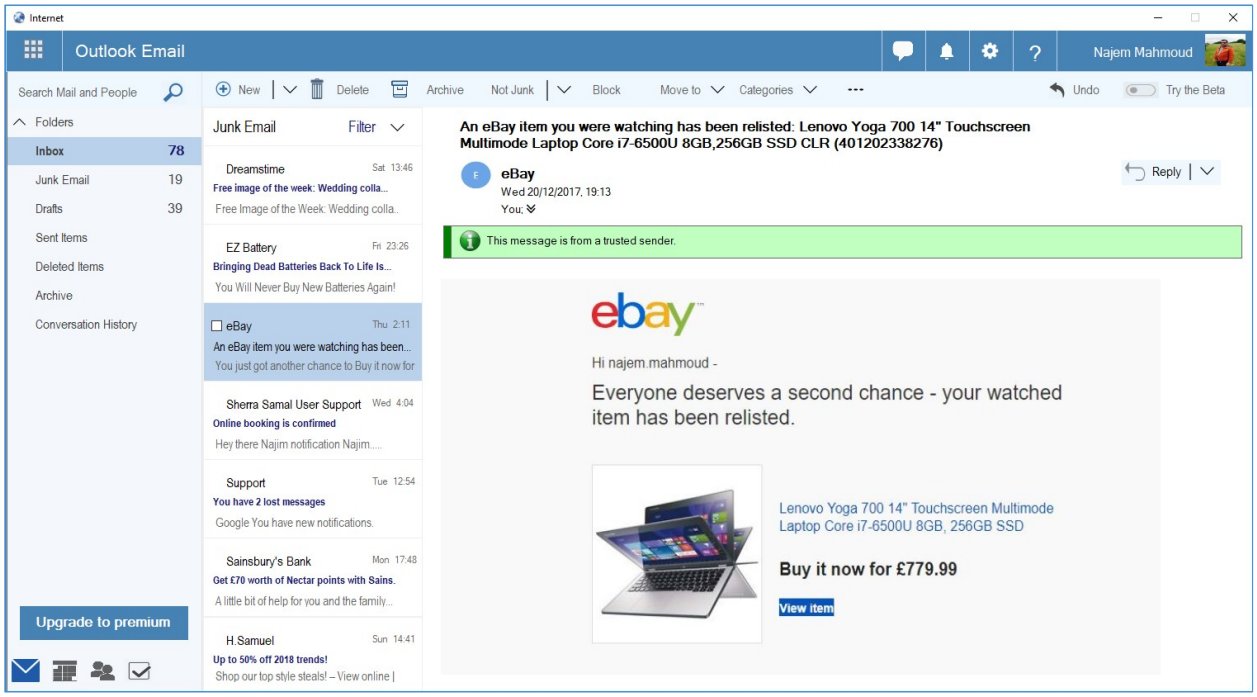

Figure 91: Proposed notification when receiving an email from a trusted sender

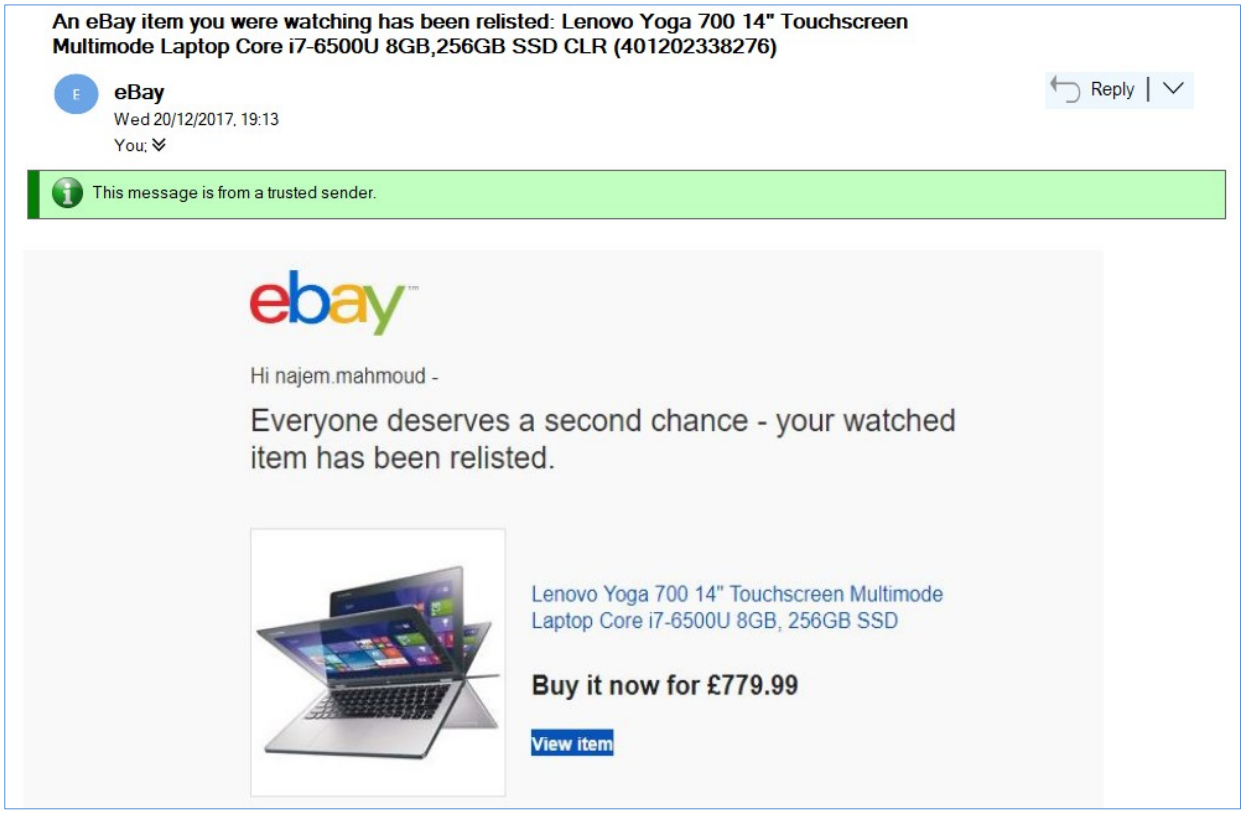

Figure 92: Proposed notification when receiving an email from a trusted sender

6.7.2 Applying Principle 3: Simplified Security Explanation

In addition to the security visuals, and based on the results obtained from the prior experimental work, users with average computer skills are also appreciate the presence of text that explains the specifics of the security threat in a common language, with the least possible use of technological terminology, and avoiding presenting irrelevant information and options. The language used should be suitable for first-time as well as advanced users, in which there should be a balance between the need to provide adequate information for a first time user while not providing surplus information for an experienced user. This will help users to comprehend and correlate the presented security visuals with the security explanation of the security threats they are facing. For example, if the interface is providing vague, irrelevant, confusing, or inadequate information, the user may not comprehend the security risk and as a result, they may act inappropriately which may leads to compromise their system.

In relation to providing simplified security explanation issue, the Microsoft Outlook offers to users to click on a link to decide whether it is not spam or to show the blocked content. Microsoft Outlook also adds more confusion by not specifying the suspicious email clearly. For instance, whether it is a spam or a phishing email, whether is certainly a phishing email that it has been detected or a suspected phishing email. As per the current interface design, it is in some cases categorises both spam and phishing emails as spam emails, whereas there is a difference between them, apart from the fact that both are associated with cybercriminal activities. The same flaw has been identified in the YAHOO email application.

In these apparent examples, in the current version of the surveyed email applications, users face a situation where they need to make security decisions while improper and inadequate guidance or advice is provided to them. As a result, this will not make users appropriately aware of the threat and practically hindrance the ability of the users to make an appropriate and informed decision that leads to protecting their devices and data.

In the screenshots shown earlier in Figures 76 and 77, Microsoft Outlook has blocked an email as a spam and warned the user with a message of yellow background setting stating that "*This message was identified as spam. We'll delete it after 3 days. It's not spam| Show blocked content*" and offers links to the user to click and decide that this is email *is not a spam or to show blocked content.* In other occasions, it blocks similar suspected phishing email from a different illegitimate sender and potentially a scammer and warned the user in a different way with a message as presented per screenshots in Figures 78 and 79 with red background setting stating that "*This sender failed our fraud detection checks and may not be who they claim to be*". This design has the potential to be a misleading security guidance that potentially leads the user to take

inappropriate actions, which potentially lead to compromising the user account and as a result the theft of user's sensitive information.

This flaw can be tackled by providing only the relevant information to the user at this stage. Users at this stage needs a very clear message and notification that explains the threat associated with the blocked email and what actually the type of the email that has been blocked. There should be no options presented to the users in the banner to decide whether it is a spam email or not, instead and as a solution, users should be informed clearly whether the blocked email is a phishing email, spam email, suspected phishing email or a trusted email. Examples are presented on screenshots in Figures 93, 94, 95, and 96. These screenshots are demonstrating the proposed security warning message or notification by improving the banners appearance and the warning message content when a phishing email has been blocked.

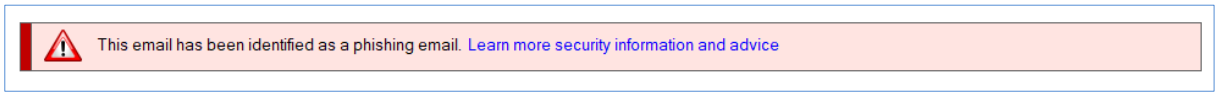

Figure 93: Proposed warning message of an identified phishing email

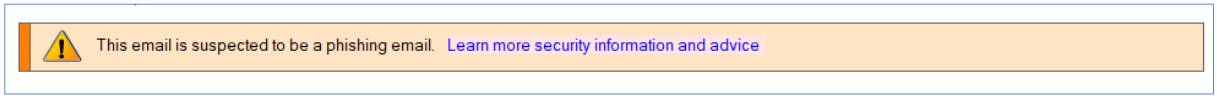

Figure 94: Proposed warning message of a suspected phishing email

Figure 95: Proposed warning message of a suspected spam email

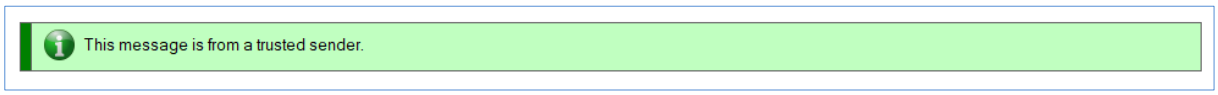

Figure 96: Proposed notification message of a trusted email

6.7.3 Applying Principle 4: Proposed Recommendation

It has been noticed from the previous experimental work conducted during this research that there is significant advantage of providing adequate security information and advice to the users to deal with security risks. This is required to enable the users to take the necessary actions that safeguard their crucial IT systems and data. For example, providing a *Learn more security information and advice* link could be offered to the users in this situation to provide preliminary security guidance and feedback when necessary that can help the user make informed decisions at the right time and when it needed. The security guidance should be brief, specific about the risk and with the necessary information that has the least possible use of technical terminology. An example of what an adequate security information and security advice in this situation might include the following:

Security information:

- *This email has been blocked because our email filters were unable to verify the sender's integrity.*
- *There is a potential that this email might be sent to you by a hacker or scammer to trick you into disclosing personal information and passwords that will result in stealing your sensitive and valuable information.*
- *There is a potential risk that your computer gets malware if you unblock the content of this email.*

Security advice:

- *You are advised to check the sender's or the company's email by checking the sender's address to verify the integrity of the sender by clicking or hovering over the email address of the senders.*

- *Do not block the content if you are unsure about the content or the sender and delete this email immediately.*
- *Never follow links or open attachments in suspicious or unsolicited emails. If in doubt, or if you need further assistance, contact directly the company that claims to have sent it.*
- *Please check that your anti-virus is up to date to avoid acquiring malware as a result of unblocking the content of this email.*

This security information and advice has the potential to help and support users by making them aware of the threat, thus contributing to mitigate the security risks that the users may encounter if a suspicious email has reached their mailbox. However, as with the current settings of the notification message used in Microsoft Outlook, offering a link to the user to unblock the content without providing adequate security guidance and adequate information, may result in the user becoming a victim of a scam. In the case that users are still in doubt, a wider information could be offered to them to learn more about the blocked email for example by offering a webpage that provides further security information and details associated with the encountered threat.

In the proposed security message that contains the security information and advice, users are also offered a link to (*Learn more information about how to recognize phishing email messages*) at the bottom of the security message, to acquire more information if they are still not appropriately aware of what is the risk to learn more security information and advice about phishing emails, as shown in Figures 97, 98 and 99. This will be critical if the users are uncertain about the blocked email. Providing this additional feature will give the users the opportunity to learn more information about how to recognize phishing emails. Microsoft has provided a webpage to educate users on how to protect themselves from phishing. However, at present, Microsoft has not

provided this opportunity when the task in hand within Outlook when a suspicious phishing email identified or blocked. The webpage is provided here: https://support.microsoft.com/en-ph/help/4033787/windows-protect-yourself-from-phishing.

The security information and the recommended advice provided in the new proposed design, should help to raise the security awareness for the users before taking actions to unblock suspected phishing emails. This proposed design approach has the potential to provide support to users at the point of need, in order to take the necessary security precautions and make informed decisions.

Figure 97: Proposed appearance of security message for detected phishing emails

Figure 98: Proposed appearance of security message for suspected phishing emails

Figure 99: Proposed appearance of security message for Spam emails

The previous design of the warning pop-windows has been criticised as not an ideal friendly user interface with potential dense nature and high volume of text on the information, and recommendations provided. Therefore, the warning security pop-windows have been revised and the associated appearance and the content based on user feedback are significantly improved by reducing the amount of information and

making it as focused and concise as possible. These improvements are presented in Figures 100, 101 and 102.

Figure 100: Improved appearance and content of the security message for detected phishing emails

Figure 101: Improved appearance and content of the security message for suspected phishing emails

Figure 102: Improved appearance and content of the security message for Spam emails

6.7.4 Applying Principle 5: Minimal Intrusion

In this regard, within the current interface of the Microsoft Outlook application, the currently used security notifications using banners in the Microsoft Outlook application are not inhibiting the user from completing their everyday tasks and does not intrude on screen space. Moreover, the warning message currently used in the Microsoft Outlook application does not interfere or affect the other components of the interface, i.e., it does not block, modify, overlap or make the interface harder to interact by the user. Therefore, no significant changes or improvements have been made apart from improving the background colour codes and the appearance of the banners. However, regarding the number of actions that require interaction or clicks that are involving users to interact or click on two links in which two options to perform (i.e. to decide It's not spam or to Show blocked content), in the improved design users are only see one link that leads to a security information and advice to understand the risk and if they still unsure or not yet fully aware of the threat, they can access to a broader information by clicking on the provided link in the pop up security panel/window to (*Learn how to spot phishing emails*).

6.7.5 Applying Principle 6: Aiding the Decision Latency

While the current design of Microsoft Outlook does not provide any means or feature for the user to obtain additional information regarding the potential risks, the new design has improved the current situation by providing an option to the user to access broader information if the user is still unaware of the threat, and not been able to comprehend the security risk.

The improved design is simple and streamlined without confusing the user, for example, the proposed designs of the warning messages are consisting a very specific and clear description of the type of the blocked email. For instance, when a phishing email has

been identified which represents the highest security risk, the presented message at this situation is (*This email has been identified as a phishing email. Learn more security information and advice*), the second situation is when suspected phishing email has been detected which represents the second degree in terms of the security risk, the presented message at this condition is (*This email is suspected to be a phishing email. Learn more security information and advice*). The third situation is when a suspected spam email has been blocked, the presented message is (*This email is suspected to be a spam. Learn more security information and advice*), which represents the third degree in terms of the security risk and the last type of the presented message is a notification to inform the user that the received email is from a trusted sender and the message used is (*This message is from a trusted sender*). The reason for this design viewpoint is that providing a different and clear classification of security warnings will be practical to assist the users to comprehend, and differentiate between the severities risks associated with suspicious emails, and to make them appropriately aware of the differences between the blocked emails.

In the proposed design users are appropriately aware of the threat, and the time requires users to spend assessing the information in order to assist them making an informed security decision without the need to search for further information is simplified, and curtailed in which users will not be required to search for further information. The required and the necessary security information is provided by clicking on one link and was made to be easily accessible.

6.7.6 Applying Principle 7: Level of Detail and Clarity

As mentioned earlier in the previous sections, users may need to know the level of the security consideration that they need to take into account, and what is the nature of details that required them to look at, to inspect whether the blocked email is from

legitimate or official sender/organisation. For example, users should have the option to acquire more information that explains how to identify and inspect whether the sender is legitimate or a scammer.

Although Microsoft has improved the earlier interfaces of Outlook application slightly for alerting the user when phishing email is detected and has taken steps towards improving the warning design for the users about the blocked emails, Microsoft has not done enough in terms of making the users appropriately aware of the phishing emails and is still prone to provide the necessary information and assistance that makes the user appropriately aware of the threat to mitigate any risks associated with the phishing emails.

Security awareness of the potential risks associated with the phishing emails should be raised for users and appropriate security information and advice should be provided to users on what they should do if they are not trusting the sender, or the email that reached their mailbox.

It is instead, giving the opportunity for the cybercrimes to be succeed in their quest by allowing the user to unblock the blocked email content as mentioned earlier, without providing a proper security guidance which would be useful to help the user to make the appropriate and informed decision at the right time before unblocking the content of the blocked email.

For more specific assessment, Table 14 presents an assessment of the security features of the current and the proposed improved interfaces based on the design principles and guidelines discussed in chapter 5.

Table 14: An assessment of current and proposed interfaces' security features

The proposed design principles		The current design of the interface of Microsoft Outlook	The proposed design of the interface of Microsoft Outlook after applying proposed design principles
1.	Severity of Security Risk	It is using only two different background colours to demonstrate the severity of security risk. However, the used background colour code not quite visible and no warning signs are used.	Improved by using clear illustrations that are easy to recognize and comprehend by users, which helps to diagnose the threat and make users pay more attention to the security threat that has been detected.
2.	Security Visuals	Lack of use of background colour codes and security signs that help to clearly notify the user about the security status.	Improved attention to the visibility of the security status, by using four colour codes accompanied with suitable warning signs were used (Triangle warning signs), with different background colour codes that demonstrate without confusion the severity of the encountered threat.
3.	Simplified Security Explanation	Lack of providing Help, and proper explanations to users to understand the encountered threat, which may lead users to make uninformed decisions.	This has been ameliorated in the proposed design by providing a link with a Learn more security information about the detected threat that provides a clear explanation to the users with the necessary information about the threat. Additional support is offered by accessing Microsoft webpage that explains how to recognize the threat.
4.	Proposed Recommendation	Absence of providing proposed recommendations to users to deal with the detected threat.	Improved by providing security recommendations and advice to users in order to help them take the appropriate and required actions that need to be taken to avoid compromise.

5.	Minimal Intrusion	Although is not hindering the user from performing tasks, it provides no adequate information and only provides a misleading message to allow the user to click on a link to decide that the blocked email "*It's not a spam*" or to click on "*Show blocked content*".	Has no intrusion. It provides and equips the users with the necessary information, by accessing security information to acquiring more recommendations about the threat that has been detected.
6.	Aiding the Decision Latency	Users have no means of support at the time when the security threat is presented, in terms of any sort of available information to understand the threat that has been detected, hence user is forced to search for more information in order to understand the risk, which may require more time to search around. This may frustrate users if they spend too long looking, which may lead them to give up and thus remain unprotected.	It requires the most minimal time for users to assess information that is necessary to help them understand the security threat that has been detected, and consequently making an informed decision without needing to search for more information, as they are only required to visit the Microsoft webpage that explains how to recognize this threat.
7.	Level of Detail and Clarity	The currently used interfaces do not provide the necessary and required details and clarity about the detected security threat, which makes the user uncertain to understand and deal appropriately with the detected threat.	Enhanced by providing the necessary details and clarity to help users understand the detected security threat and make them aware of the detected threat and deal with it appropriately without being overwhelmed by the superfluous information.

6.8 Conclusions

Security issues are being increasingly recognised by IT users, as more security-related features are being introduced in a range of applications. However, based on the examples discussed in this chapter, it is clear that the effort to highlight aspects related

to security issues is still inadequate in raising sufficient awareness among users about the security risks they encounter in their daily use of IT systems.

Microsoft Outlook has not progressed from its previous version, meaning that it still provides similar warning messages and notifications when a suspicious email is blocked, which is almost representing a phishing email. Although the new interface design of the Microsoft Outlook application is slightly enhanced compared to its previous interface design, the new design does not introduce any fundamental changes that help familiarise users with the phishing email threat, or assist them to make an informed security decision before unblocking the content of the blocked email.

The proposed new design principles are considered to be achievable. To demonstrate this, improvements were made to the warning messages and notifications that are currently used in the interface of the Microsoft Outlook email application, which either do not exist in the current version, or that requires improvements. These improvements are intended to redesign the graphical user interface in a manner that will help make the users aware of the security risk encountered and simultaneously be easier to use. Furthermore, additional attention was paid in the newly proposed interfaces so that the use of security features would be improved. For instance, some security signs (warning triangles signs to make the warning message more visible) were added, more visible background colour codes were used to demonstrate the difference between the severity risk, additional functionality was added using links such as, "*Learn more security information and advice*", to raise the security awareness for the users about the detected phishing email, before taking actions to unblock the suspected or the identified email. Furthermore, in the warning message, users were offered to visit a webpage provided by Microsoft for users to access more information about how to recognise phishing email messages.

Although this research has conveyed an interesting result in terms of opportunities for improvement, it has only achieved an assessment of the appearance level of the surveyed application and how the proposed design principles and guidelines would help to make users aware of the encountered security threat in a more apparent manner.

The new design principles and guidelines have been applied to the interface of the application and compared with the current interface design of the application. The results reflect the need for improvement of the current design, which will raise the awareness of the user to aid them in spotting phishing threats.

Chapter 7

Conclusions and Future Work

This chapter concludes the thesis by outlining the concrete contributions and the achievements of the research. The limitations of the research are then summarised and followed by identifying the potential opportunities for future work. Finally, the future of cybersecurity awareness is highlighted.

7.1 Contributions and Achievements of the Research

The research aims and objectives which were initially planned and set in Chapter 1 have been accomplished, with an experimental study leading to the development of a series of related design principles and guidelines for targeted security awareness-raising approach which has been applied to the appearance of email notifications that aim to assist users in spotting phishing threats. The fundamental contributions and achievements of this research are briefly listed below:

- The research highlighted that although there are security features included in the applications that users deal with on a daily basis, and there is a presence of design principles and guidelines to build applications that contain consistent user interfaces and adequate information, the developers of these applications are prone to releasing a reliable application that provides adequate security information and advice for users to understand the security issue and to make them appropriately aware of the threats that they may encounter during their use of these applications. Moreover, it should help them recognise the threats in an apparent manner to mitigate any security risks associated with these threats.

- The results obtained from the experimental study are very encouraging and are based primarily on the use of targeted security awareness-raising approach by developing the interfaces of some applications that lack adequate information which helps to make the users aware of the potential security risk. It can be argued that this approach is primarily aiming at increasing user security awareness by providing adequate information and recommendations to users regarding the potential risks, and leaving users with the option to make informed decisions based on providing adequate security information and recommendations to mitigate security risks and its related implications.
- From the investigation conducted during this research to examine the opportunities for applying this approach in other security scenarios, it can be said that despite the availability of a good design principles that are recognised in terms of effectiveness and their wide use, does not mean neglecting the development of new principles in line with new requirements that may arise as a result of several factors, including the possibility of shortcomings in the existing user interfaces of some applications, as well as the evolving and changing of the potential security risks faced by users.
- One of the most important contributions of this research is the introduction and discussion of new design principles and guidelines for security features that can be used to improve the security of IT systems, by modifying the interfaces to increase the security awareness of the users. This objective can be accomplished by moving towards making the users aware through focusing on educating users about the security threats they are facing and assisting them by providing appropriate security recommendations so they can make informed decisions.
- Another contribution of this research is that it highlighted the possibility of developing user interfaces for some of the prominent applications currently used to effectively protect systems and data, by improving the design of user interfaces

currently used, to help increase security awareness of the users in order to improve their decisions.

- Besides, an additional contribution of this research is that it has introduced an innovative, promising and an effective approach that can be relied on to increase user security awareness by ensuring that security guidance and feedback is available during the task in hand, providing effective information to help the users to make the right decision at the right time to avoid security risks. The use of the targeted security awareness raising approach to increase the security awareness of users has become more imperative than ever before. It is an emerging area that has the potential to be considered as a valuable method for raising the security awareness of end-users. This can be achieved without the need for any additional costs, such as, training users, or make substantial changes to the systems currently in use. The only requirement is to develop the user interfaces by appropriately optimizing the existing security tools and features used in a variety of applications, to increase users' security awareness of the potential threats.
- Despite the existence of some examples where some prominent software developers have adopted and implemented targeted security awareness-raising approach in their software (as discussed in chapter 3), along with evidence of related studies, this research observed that there is a lack of direct and extensive research and studies that explores and investigates targeted security awareness-raising approach profoundly. This emphasizes that there is an imperative need for further research to study this approach. This work paves the way for further research and studies in this field and outlines the possible application areas to evaluate the effectiveness of this approach in other security scenarios.

7.2 Limitations of the Research

Despite the tangible achievements of this research and the fact that objectives have been met, some issues have identified, which may have limited the work progress and findings. The key limitations of the research are briefed below:

- There were insufficient resources and a lack in the literature that precisely explores, discusses and evaluates the implementation of the targeted security awareness-raising approach and its effectiveness. Therefore, all the discussions are built on the diligence and self-effort of exploring the potential opportunities for implementing this approach in some security scenarios.
- Although the effectiveness of the targeted security awareness-raising approach has been assessed through a wide pilot study that involved 100 participants by using a prototype software that simulates the process of viewing available Wi-Fi networks and allowing the user to connect to the most appropriate network in different given scenarios. The results were encouraging and promising in adopting this approach in raising users' awareness of the potential threats. It should be noted that was not a full implementation of a new software that detects Wi-Fi networks and reads a real Wi-Fi networks data and provides a feedback and recommendations based on an actual data. It should be also noted that this was to establish, provide evidence and evaluate the effectiveness of the targeted security awareness-raising approach in increasing users' awareness by conducting an experimental study. Considering the research nature, a full implementation of the software in a real environment was not required to prove and evaluate the effectiveness of this approach. Therefore, it should mentioned that to appraise the practical usefulness of the proposed approach, a full implementation of the software will be very useful to evaluate this approach in the real environment and can give better understanding of the

effectiveness of it, bearing in mind that high programming skills and enough time are required for a full implementation such software.

- Moreover, although the new design principles have been devised to adopt the targeted security awareness-raising approach and apply these design principles to improve user interfaces for Microsoft Outlook, no empirical study has been conducted to assess the effectiveness of the improved interfaces in increasing users' awareness of spotting phishing emails. It would, therefore, be very useful to conduct a pilot study to evaluate the effectiveness of the improved interfaces of email applications on this aspect.
- Due to issues and difficulties which were experienced during the course of this research, only two scenarios where investigated in which the targeted security awareness raising approach can be useful, and this was achieved by either a pilot study or applying the design principles in existing interfaces of applications. However, it would better to investigate further opportunities by conducting further empirical studies to broadly explore this approach and to deeply investigate the effectiveness of it.

7.3 Opportunities for Future Work

This research programme has in general perspective introduced a new approach in the field of raising the security awareness of the users with design principles and guidelines for targeted security awareness in particular. However, there are a number of opportunities for empirical work and further investigations which can be carried out in order to better evaluate and understand the areas precisely related to this research. These opportunities are listed below:

- One of the most important possible future work for this research is to evaluate the effectiveness of the targeted security awareness approach in other security

scenarios, where there are weaknesses and lack of user interfaces that make users aware of the potential security risks they may face, and also inadequate recommendations provided to users to make better security decisions that contribute to protection of their devices and data and/or reduce the security implications of any security breach.

- In addition, this research can also be further developed to include the evaluation of interfaces of some applications currently in use, find the shortcomings in them and study the possibility of developing these interfaces by adhering to the new design principles, which aims to improve the user interfaces currently used in some applications in order to increase the security awareness by adopting the targeted security awareness-raising approach for users. In general, it can be argued that there is a broad scope to study and evaluate the effectiveness of the targeted security awareness-raising approach for users by conducting further empirical studies on other security scenarios.

7.4 The Future of Cybersecurity Awareness

Users are often referred to as the weakest link in the information security chain. This is mainly due to a number of factors, the primary factor is the lack of security awareness among users regarding the emerging and evolving security threats. Moreover, unaware users can pose more risks to their organisations' IT security and potentially can be the root cause of security breaches, for example by responding to phishing emails, visiting malware infected websites, writing their passwords down or sharing them with others, or even providing sensitive information over the phone when exposed to social engineering. In order to transform the weakest link into a primary defence line against cybersecurity threats and to strengthen them in an information security perspective, there are different and diverse methods employed to support them. These methods are

ranging from simple, such as the use of posters, scheduled security awareness campaigns, to the most ratified method which is conducting security awareness programs designed to cover specific security topics. The number of security threats is increasing and becoming more complex as cybercriminals create new ways to breach IT systems. This makes it difficult to rely solely on the material provided in these security programs. Furthermore, users may forget what they have been trained over time and are likely to get confused by the similarity of security-related topics.

In addition, security awareness programs are often criticised for their lack of appropriate materials, the methodology which they are implemented, and the ability of staff to comprehend and practice the acquired material. Despite the notable criticism, security awareness programs like all related efforts, are to mitigate security risks rather than fully preventing security threats from taking a place, consequently they need to be implemented appropriately.

Furthermore, organisations may tend to rely on “One-size-fits-all” or may be tempted by a “set it and forget it” security awareness programs. These organisations should exercise caution when adopting these approaches, as they may lose the ability to respond to the emerging threats or mitigate their implications. Increasing the security awareness of end users is an ongoing issue because of several crucial factors. Firstly, the workforce changes over time, staff come, go and roles often also change over time. Secondly, threats change and evolve in an accelerated manner, taking ransomware as an example, which has been a very different security concern in the last few years compared to how it is perceived now. Thirdly, awareness is not the same as knowledge, because knowing a threat is not necessarily knowing how to recognise it and respond to it. Fourthly, knowledge is not a constant especially in the cybersecurity domain,

users tend to forget what they have trained for or what they have gathered from the security awareness programs.

This emphasises the imperative need for innovative techniques and methods to increase users' awareness other than using the traditional methods, to provide support and assistance and increase the security awareness of the user while dealing with the IT systems. Providing adequate security information and guidance in a timely manner during the task in hand is a method that has the potential to help the user to deal with potential security threats and thus make informed decisions that help protect the user and device data.

From aforementioned, it is clear that there is an imperative need to devise innovative methods to increase the security awareness of users while dealing with IT systems during their day-to-day operations, when they need support to understand a specific security problem. Novice users or users with limited computer skills are representing the largest population of computer users, therefore there is a need to ensure that only related information is provided to them regarding the potential threats, while in the same time ensuring not superfluous information are provided to avoid confusion for them. Undoubtedly, there is a need to maintain a balance between security and usability. Security should not intrude or hinder the interaction between the user and the device. Users are more likely to disable such features if they interfere with the task the user is trying to achieve. Furthermore, users should be able to find information when needed and not spending too much time to find such information, otherwise they may give up on looking up for the information and remain unprotected. No unrealistic assumptions about the user should be made by the technology. Users should be able to determine the level of protection from the technology. Appropriate warnings and status indicators are useful to remind users when such safeguards are not enabled.

Security awareness tends to be unreliable at times it is needed. One of the most promising and innovative methods to effectively increase security awareness for users is to use targeted security awareness-raising approach. This approach provides guidance and nudges during the task in hand. The experimental study conducted during this research exposed the effectiveness of adopting this approach to increase the security awareness of users. The study was conducted to demonstrate the effectiveness of providing adequate security information and recommendations before users connecting to unknown and potentially insecure Wi-Fi networks. The results obtained showed that providing adequate security information and the necessary guidance and recommendations improved user's decisions and helped them in making better security decisions by choosing secure Wi-Fi networks.

The Targeted Security Awareness Raising field is a promising and rich area for conducting further research and studies and is an innovative method that relies merely on providing support, adequate security information, guidance, and recommendations to help users make better and informed decisions that protect their data and devices. This approach does not require additional costs or make substantial changes to the existing IT systems. All that is required to implement this promising new approach is to improve existing user interfaces of some applications, which are providing inadequate security information and recommendation, and have shortcomings and flaws in their interfaces, to provide adequate security information and guidance that are necessary for the users to help them to make better security decisions.

References

1. Albrechtsen, E. & Hovden, J. 2010. Improving information security awareness and behaviour through dialogue, participation and collective reflection. An intervention study. Computers & Security, 29, 432-445.
2. Anti-Phishing Working Group (APWG). 2017. Phishing Activity Trends Report - 1st Half 2017. Retrieved from: http://docs.apwg.org/reports/apwg_trends_report_h1_2017.pdf (Accessed 10 January 2018).
3. Banerjee, C. & Pandey, S.K., 2010. Research on software security awareness: problems and prospects. ACM SIGSOFT Software Engineering Notes, 35(5), pp.1-5.
4. BSI. 2013. Information technology - Security techniques- Code of Practice for information security controls. BSI Standards Limited.
5. Bulgurcu, B., Cavusoglu, H. & Benbasat, I., 2010. Information security policy compliance: an empirical study of rationality-based beliefs and information security awareness. MIS quarterly, 34, 523-548.
6. Caldwell, T., 2016. Making security awareness training work. Computer Fraud & Security, (6), pp.8-14.
7. Canadian Bankers Association CBA. 2014. Staying Safe Online - October is Cyber Security Awareness Month. Retrieved from: https://cba.ca/staying-safe-online (Accessed 20 November 2015).
8. Clearswift. 2018. #1 Cyber security threat. Protecting your organisation against email based attacks. Retrieved from: https://www.clearswift.com/blog/2018/03/20/1-cyber-security-threat-protecting-your-organisation-against-email-based-attacks (Accessed 23 March 2018).

9. Crossler, R.E., Johnston, A.C., Lowry, P.B., Hu, Q., Warkentin, M. and Baskerville, R., 2013. Future directions for behavioral information security research. Computers & security, 32, pp.90-101.
10. Crowd Research Partners. 2018. Insider Threat Report. Retrieved from: https://www.ca.com/content/dam/ca/us/files/ebook/insider-threat-report.pdf (Accessed 15 July 2018).
11. Crowe, J, 2016. Phishing by the Numbers: Must-Know Phishing Statistics 2016. Retrieved from: https://blog.barkly.com/phishing-statistics-2016 (Accessed 1 September 2017).
12. Drevin, L., Kruger, H.A. & Steyn, T., 2006. Value-focused assessment of ICT security awareness in an academic environment, In: IFIP International Federation for Information Processing, Volume 201, Security and Privacy in Dynamic Environments, eds. Fischer-Hubner, S., Ranneberg, K.,Yngstrom, L., Lindskog, S. Boston: Springer, 448-453.
13. Drevin, L., Kruger, H.A. and Steyn, T., 2007. Value-focused assessment of ICT security awareness in an academic environment. Computers & Security, 26(1), pp.36-43.
14. ENISA. 2007. Information security awareness initiatives: Current practice and the measurement of success. European Network and Information Security Agency.
15. ENISA. 2010. The new users' guide: How to raise information security awareness.
16. ENISA. 2017. Threat Landscape Report 2017. 15 Top Cyber-Threats and Trends. Retrieved from: https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017 (Accessed 6 July 2018).
17. Ernst & Young. 2012. Fighting to close the gap. Global Information Security Survey. EYG no. AU1889. Retrieved from:

http://www.ey.com/Publication/vwLUAssets/GISS2012/$FILE/EY_GISS_2012.pdf (Accessed 20 September 2013).

18. Ernst & Young. 2016. Path to cyber resilience: Sense, resist, react. The 19th Global Information Security Survey. EYG no. 04260-163GBL. Retrieved from: https://www.ey.com/Publication/vwLUAssets/Global_Information_Security_Survey_2016/$FILE/REPORT%20-%20EY's%2019th%20Global%20Information%20Security%20Survey.pdf (Accessed 25 May 2018).
19. Ernst & Young. 2017. Cybersecurity regained: preparing to face cyber-attacks. 20th Global Information Security Survey. EYG no. 06574-173Gbl. Retrieved from: https://www.ey.com/Publication/vwLUAssets/ey-cybersecurity-regained-preparing-to-face-cyber-attacks/$FILE/ey-cybersecurity-regained-preparing-to-face-cyber-attacks.pdf (Accessed 25 May 2018).
20. Ernst & Young. 2018. Is cybersecurity about more than protection?.Global Information Security Survey 2018. EYG no. 011483-18Gbl. Retrieved from: https://www.ey.com/Publication/vwLUAssets/ey-global-information-security-survey-2018-19/$FILE/ey-global-information-security-survey-2018-19.pdf (Accessed 20 February 2019).
21. Florencio, D. & Herley, C., 2007. A large-scale study of web password habits. Proceedings of the 16th international conference on World Wide Web. ACM, 657-666.
22. Forbes. 2017. Phishing Scams Cost American Businesses Half A Billion Dollars A Year. Retrieved from: www.forbes.com/sites/leemathews/2017/05/05/phishing-scams-cost-american-businesses-half-a-billion-dollars-a-year/#3c420cc73fa1 (Accessed 20 January 2018).

23. F-Secure. 2014. Tainted Love: How Wi-Fi Betrays Us. F-Secure Corporation. Retrieved from: https://fsecureconsumer.files.wordpress.com/2014/09/wi-fi-experiment_uk_2014.pdf. (Accessed 28 November 2014).
24. Furnell, S. & Bär, N., 2013. Essential Lessons Still Not Learned? Examining the Password Practices of End-Users and Service Providers. In: MARINOS, L. & ASKOXYLAKIS, I. (eds.) Human Aspects of Information Security, Privacy, and Trust. Springer Berlin Heidelberg.
25. Furnell, S. & Clarke, N., 2012. Power to the people? The evolving recognition of human aspects of security. Computers & Security.
26. Furnell, S., 2005. Authenticating ourselves: will we ever escape the password? Network Security, 2005, 8-13.
27. Furnell, S., 2016. The usability of security-revisited. Computer Fraud & Security, (9), pp.5-11.
28. Furnell, S., Alotaibi, F. and Esmael, R., 2019. Aligning Security Practice with Policy: Guiding and Nudging towards Better Behavior. In Proceedings of the 52nd Hawaii International Conference on System Sciences.
29. Furnell, S., Esmael, R., Yang, W. and Li, N., 2018. Enhancing security behaviour by supporting the user. Computers & Security, 75, pp.1-9.
30. Get Safe Online. 2017. Spam and Scam email. Retrieved from: https://www.getsafeonline.org/protecting-yourself/spam-and-scam-email/ (Accessed 5 September 2017).
31. GetCyberSafe. 2014a. Email. Public Safety Canada. Retrieved from: http://www.getcybersafe.gc.ca/cnt/rsks/nln-ctvts/ml-eng.aspx (Accessed 5 October 2014).

32. GetCyberSafe. 2014b. Email Scams. Public Safety Canada. Retrieved from: http://www.getcybersafe.gc.ca/cnt/rsks/scms-frd/ml-eng.aspx (Accessed 1 October 2014).
33. GetCyberSafe. 2014c. File Downloading and Sharing. Public Safety Canada. Retrieved from: http://www.getcybersafe.gc.ca/cnt/prtct-dvcs/cmptrs-tblts/dwnldng-shrng-eng.aspx (Accessed 15 October 2014).
34. Heartfield, R. and Loukas, G., 2018. Detecting semantic social engineering attacks with the weakest link: Implementation and empirical evaluation of a human-as-a-security-sensor framework. Computers & Security, 76, pp.101-127.
35. Herath, T. & Rao, H. R., 2009. Encouraging information security behaviors in organisations: Role of penalties, pressures and perceived effectiveness. Decision Support Systems, 47, 154-165.
36. Herley, C. & Van Oorschot, P., 2012. A research agenda acknowledging the persistence of passwords. Security & Privacy, IEEE, 10, 28-36.
37. Hewett, T.T., Baecker, R., Card, S., Carey, T., Gasen, J., Mantei, M., Perlman, G., Strong, G. and Verplank, W., 1992. ACM SIGCHI curricula for human-computer interaction. ACM.
38. Hinson, G., First published in 2003, updated most recently in February 2014. The true value of information security awareness. Addressing the rhetorical question: why do we need security awareness?. White paper. Retrieved from: http://www.noticebored.com/html/value_of_awareness.html (Accessed 26 April 2018).
39. Ifinedo, P., 2009. Information technology security management concerns in global financial services institutions: Is national culture a differentiator? Information Management & Computer Security, 17, 372-387.

40. Ifinedo, P., 2012. Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. Computers & Security, 31, 83-95.
41. Ifinedo, P., 2014. Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. Information & Management, 51(1), pp.69-79.
42. iPass. 2016a. iPass Mobile Professional Report 2016. Retrieved from: https://www.ipass.com/wp-content/uploads/2016/11/iPass-Mobile-Professional-Report-2016.pdf (Accessed 24 March 2017).
43. iPass. 2016b. 2016 Mobile Security Report. Retrieved from: https://www.ipass.com/wp-content/uploads/2016/05/iPass-2016-Mobile-Security-Report.pdf (Accessed 24 March 2017).
44. IronScales. 2017. Trend Report: How Modern Email Phishing Attacks Have Organisations on The Hook. Retrieved from: https://ironscales.com/wp-content/uploads/2017/05/Trend_Report_Rev7.pdf (Accessed 2 July 2018).
45. ISF. 2011. The 2011 Standard of Good Practice for Information Security. Information Security Forum Limited.
46. IT Governance. 2018. The biggest cyber security threat is inside your organisation. Retrieved from: https://www.itgovernance.co.uk/blog/the-biggest-cyber-security-threat-is-inside-your-organisation/ (Accessed 5 March 2018).
47. Johnston, J., Eloff, J.H. and Labuschagne, L., 2003. Security and human computer interfaces. Computers & Security, 22(8), pp.675-684.
48. Kaspersky Lab. 2012. Digital Consumer's Online Trends and Risks. Kaspersky Lab.
49. Kaspersky Lab. 2014. Main sources of threats penetration. Retrieved from: http://support.kaspersky.co.uk/viruses/general/789#block1 (Accessed 15 December 2014).

50. Kaspersky Lab. 2016. Consumer Security Risks Survey, Connected But Not Protected. Kaspersky Lab. Retrieved from: https://dl.acronis.com/u/pdf/Kaspersky_B2C_survey_2016_report.pdf (Accessed 30 March 2017).
51. Katsabas, D., Furnell, S.M. & Dowland, P.S., 2005. Using human computer interaction principles to promote usable security. In Proceedings of the Fifth International Network Conference (INC 2005), Samos, Greece (pp. 235-242).
52. Katsikas, S. K., 2000. Health care management and information systems security: awareness, training or education? International Journal of Medical Informatics, 60, 129-135.
53. Kegel, R.H., 2015. The Personal Information Security Assistant. In Requirements Engineering Conference (RE), IEEE 23rd International (pp. 393-397). IEEE.
54. Kessel, P. V., 2012. Fighting to Close the Gap: Ernst & Young's 2012 Global Information Security Survey. Ernst & Young's, 5, 23-31.
55. Korovessis, P., Furnell, S., Papadaki, M. and Haskell-Dowland, P., 2017. A toolkit approach to information security awareness and education. Journal of Cybersecurity Education, Research and Practice, (2), p.5.
56. Kruger, H., Drevin, L. and Steyn, T., 2007. Email Security Awareness – a Practical Assessment of Employee Behaviour. In Fifth World Conference on Information Security Education (pp. 33-40). Springer Boston.
57. Macdonald, N., 2010. The Future of Information Security Is Context Aware and Adaptive. 14 May 2010 ed.: Gartner RAS Core Researc.
58. Microsoft. 2015. Download files from the web. Retrieved from: https://support.microsoft.com/en-us/help/17436/windows-internet-explorer-download-files-from-web (Accessed 1 December 2014).

59. Muñoz-Arteaga, J., González, R.M., Martin, M.V., Vanderdonckt, J. & Álvarez-Rodríguez, F., 2009. A methodology for designing information security feedback based on User Interface Patterns. Advances in Engineering Software, 40(12), pp.1231-1241.

60. NETMARKETSHARE. 2017. Desktop Operating System Market Share. April 2017. Retrieved from: http://www.netmarketshare.com/operating-system-market-share.aspx?qprid=10&qpcustomd=0)&qpsp=2016&qpnp=1&qptimeframe=Y(Accessed 30 March 2017).

61. Nielsen, J., 1994, April. Enhancing the explanatory power of usability heuristics. In Proceedings of the SIGCHI conference on Human Factors in Computing Systems (pp. 152-158). ACM.

62. Nielsen, J., 1995. Ten Usability heuristics. Retrieved from: https://www.nngroup.com/articles/ten-usability-heuristics/ (Accessed 10 December 2017).

63. Nurse, J.R., Creese, S., Goldsmith, M. & Lamberts, K., 2011. Guidelines for usable cybersecurity: Past and present. In Cyberspace Safety and Security (CSS), 2011. Third International Workshop on (pp. 21-26). IEEE.

64. Pahnila, S., Siponen, M. & Mahmood, A. Employees' behavior towards IS security policy compliance. System Sciences, 2007. HICSS 2007. 40th Annual Hawaii International Conference on, 2007. IEEE, 156b-156b.

65. Patrick, A.S., Long, A.C. & Flinn, S., 2003. HCI and security systems. In CHI'03 Extended Abstracts on Human Factors in Computing Systems (pp. 1056-1057). ACM.

66. PCI. 2014. Security Standards Council. Security Awareness Program Special Interest Group. Best Practices for Implementing a Security Awareness Program. October 2014. Version: 1.0. September 25 2015. Retrieved from:

https://www.pcisecuritystandards.org/documents/PCI_DSS_V1.0_Best_Practices_for_Implementing_Security_Awareness_Program.pdf (Accessed 10 December 2014).

67. Peltier, T. R., 2005. Implementing an Information Security Awareness Program. Information Systems Security, 14, 37-49.
68. Phishing.org. 2018. What Is Phishing?. Retrieved from: http://www.phishing.org/what-is-phishing (Accessed 10 January 2018).
69. Ponemon Institute LLC. 2017. Cyber Security Breaches Survey. Cost of Data Breach Study: United Kingdom. Benchmark research sponsored by IBM Security, independently conducted by Ponemon Institute LLC. Retrieved from: https://public.dhe.ibm.com/common/ssi/ecm/se/en/sel03130gben/SEL03130GBEN.PDF (Accessed 20 May 2018).
70. PricewaterhouseCoopers LLP, PwC. 2012. Information Security Breaches Survey 2012. Retrieved from: https://www.pwc.co.uk/assets/pdf/olpapp/uk-information-security-breaches-survey-technical-report.pdf (Accessed 17 September 2013).
71. PricewaterhouseCoopers LLP. PwC. 2013. INFORMATION Security Breaches Survey 2013. Retrieved from: https://www.pwc.co.uk/assets/pdf/cyber-security-2013-technical-report.pdf (Accessed 10 August 2014).
72. PricewaterhouseCoopers LLP. PwC. 2014. Information Security Breaches Survey 2014. Retrieved from: https://www.pwc.co.uk/assets/pdf/cyber-security-2014-technical-report.pdf (Accessed 30 July 2015).
73. PricewaterhouseCoopers LLP. PwC. 2015. Information Security Breaches Survey 2015. Retrieved from: https://www.pwc.co.uk/assets/pdf/2015-isbs-technical-report-blue-03.pdf (Accessed 25 June 2016).
74. PricewaterhouseCoopers LLP. PwC. 2018. Strengthening digital society against cyber shocks. Key findings from The Global State of Information Security Survey.

Retrieved from: https://www.pwc.com/us/en/cybersecurity/assets/pwc-2018-gsiss-strengthening-digital-society-against-cyber-shocks.pdf (Accessed 5 March 2018).

75. Randell, C., 2013. Why security awareness campaigns fail. MWR InfoSecurity. Retrieved from: https://www.mwrinfosecurity.com/our-thinking/why-security-awareness-campaigns-fail/ (Accessed 20 November 2014).
76. RBC. 2014. Steps for Safe Computing and Online Privacy. Royal Bank of Canada Website. Retrieved from: http://www.rbc.com/privacysecurity/ca/steps-for-safe-computing.html (Accessed 1 October 2014).
77. Ryan, J. J. C., 2004. Information security tools and practices: what works? Computers, IEEE Transactions on, 53, 1060-1063.
78. Sasse, M. A., Brostoff, S. & Weirich, D., 2001. Transforming the 'weakest link'- a human/computer interaction approach to usable and effective security. BT technology journal, 19, 122-131.
79. Shaw, R. S., Chen, C. C., Harris, A. L. & HUANG, H.-J., 2009. The impact of information richness on information security awareness training effectiveness. Computers & Education, 52, 92-100.
80. Shepherd, L. A., Archibald, J. & Ferguson, R., 2013. Perception of Risky Security Behaviour by Users: Survey of Current Approaches. Human Aspects of Information Security, Privacy, and Trust. Springer.
81. Silic, M. & Back, A., 2017. Deterrent Effects of Warnings on User's Behavior in Preventing Malicious Software Use. In Proceedings of the 50th Hawaii International Conference on System Sciences.
82. Siponen, M. T., 2000. A conceptual foundation for organisational information security awareness. Information Management & Computer Security, 8, 31-41.
83. SplashData. 2014. "Password" unseated by "123456" on SplashData's annual "Worst Passwords" list. Retrieved from:

http://splashdata.com/press/worstpasswords2013.htm (Accessed 7 November 2014).

84. SplashData. 2015. "123456" Maintains the Top Spot on SplashData's Annual "Worst Passwords" List. Retrieved from: http://splashdata.com/press/worst-passwords-of-2014.htm (Accessed 26 January 2015).
85. SplashData. 2017. Worst Passwords of 2017 Top 100. Retrieved from: https://www.teamsid.com/worst-passwords-2017-full-list/ (Accessed 7 February 2018).
86. Stanton, J. M., Stam, K. R., Mastrangelo, P. & Jolton, J., 2005. Analysis of end user security behaviors. Computers & Security, 24, 124-133.
87. Statista. 2018. Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions). Retrieved from: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/ (Accessed 15 July 2018).
88. Švehla, Z.L., Sedinić, I. & Pauk, L., 2016. Going white hat: Security check by hacking employees using social engineering techniques. In Information and Communication Technology, Electronics and Microelectronics (MIPRO), 39th International Convention on (pp. 1419-1422). IEEE.
89. The Department for Culture, Media and Sport (DCMS), UK. 2017. Cyber security breaches survey. Retrieved from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/609186/Cyber_Security_Breaches_Survey_2017_main_report_PUBLIC.pdf (Accessed 20 May 2018).
90. The Department for Culture, Media and Sport (DCMS), UK. 2018. Cyber security breaches survey. Retrieved from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/atta

chment_data/file/702074/Cyber_Security_Breaches_Survey_2018_-_Main_Report.pdf (Accessed 3 July 2018).

91. Tioh, J.N., Mina, M. & Jacobson, D.W., 2017. Cyber security training a survey of serious games in cyber security. In IEEE Frontiers in Education Conference (FIE) (pp. 1-5). IEEE.
92. Torrubia, A., Mora, F. J. & Marti, L., 2001. Cryptography Regulations for E-commerce and Digital Rights Management. Computers & Security, 20, 724-738.
93. Tsohou, A., Kokolakis, S., Karyda, M. & Kiountouzis, E., 2008. Investigating information security awareness: research and practice gaps. Information Security Journal: A Global Perspective, 17, 207-227.
94. Turland, J., Coventry, L., Jeske, D., Briggs, P., & van Moorsel, A., 2015. Nudging towards security: Developing an application for wireless network selection for android phones. In Proceedings of the 2015 British HCI conference (pp. 193-201). ACM.
95. Ur, B., Kelley, P. G., Komanduri, S., Lee, J., Maass, M., Mazurek, M. L., Passaro, T., Shay, R., Vidas, T. & Bauer, L., 2012. How Does Your Password Measure Up? The Effect of Strength Meters on Password Creation. USENIX Security Symposium, 2012. 65-80.
96. usability.gov. 2018. Cognitive walkthrough. Retrieved from: https://www.usability.gov/what-and-why/glossary/cognitive-walkthrough.html (Accessed 25 March 2018).
97. usabilitybok.org. 2018. Cognitive Walkthrough. Retrieved from: http://www.usabilitybok.org/cognitive-walkthrough (Accessed 25 March 2018).
98. Vayansky, I. and Kumar, S., 2018. Phishing – challenges and solutions. Computer Fraud & Security, (1), pp.15-20.

99. Verizon. 2016. Data Breach Investigations Report. Retrieved from: https://conferences.law.stanford.edu/cyberday/wp-content/uploads/sites/10/2016/10/2b_Verizon_Data-Breach-Investigations-Report_2016_Report_en_xg.pdf (Accessed 3 September 2017).
100. Volkamer, M., Bartsch, S. & Kauer, M., 2013. Contextualized Security Interventions in Password Transmission Scenarios. EISMC, 2013. 12-22.
101. Voss, B. D., 2001. The Ultimate Defense of Depth: Security Awareness in Your Company. As part of the Information Security Reading Room. ed. SANS Institute InfoSec Reading Room: SANS Institute 2001.
102. Vroom, C. & Von Solms, R., 2004. Towards information security behavioural compliance. Computers & Security, 23, 191-198.
103. Wharton, C., Rieman, J., Lewis, C., & Polson, P., 1994. The cognitive walkthrough method: a practitioner's guide. Retrieved from: https://www.colorado.edu/ics/sites/default/files/attached-files/93-07.pdf (Accessed 10 March 2018).
104. Whitten, A. & Tygar, J.D., 1999, August. Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. In USENIX Security Symposium (Vol. 348).
105. Williams, N. & Li, S., 2017. Simulating Human Detection of Phishing Websites: An Investigation into the Applicability of the ACT-R Cognitive Behaviour Architecture Model. In Cybernetics (CYBCONF), 3rd IEEE International Conference on (pp. 1-8). IEEE.
106. Wilson, M. & Hash, J., 2003. Building an information technology security awareness and training program. NIST Special publication, 800, 50.
107. WinZip. 2014. Potentially Unsafe File Types. WinZip Computing. Retrieved from: http://kb.winzip.com/help/ZipSecurity.htm#tips (Accessed 5 December 2014).

108. Wombat Security Technologies. 2017. State of the Phish. Retrieved from: http://info.wombatsecurity.com/hubfs/State%20of%20the%20Phish%202017/Wombat%20State%20of%20the%20Phish%202017.pdf?submissionGuid=2d05e32f-eff7-48c9-9978-fbdad3d59490 (Accessed 10 September 2017).

109. Wombat Security Technologies. 2018. State of the Phish. Retrieved from: https://www.wombatsecurity.com/hubfs/2018%20State%20of%20the%20Phish/Wombat-StateofPhish2018.pdf?submissionGuid=1bfe9271-60af-4391-a854-98a7e47f5bf6 (Accessed 30 January 2018).

110. Workman, M., Bommer, W. H. & Straub, D., 2008. Security lapses and the omission of information security measures: A threat control model and empirical test. Computers in Human Behavior, 24, 2799-2816.

111. World Economic Forum. 2017. The Global Risks Report, 12th Edition. ISBN: 978-1-944835-07-1. REF: 050117. Retrieved from: http://www3.weforum.org/docs/GRR17_Report_web.pdf (Accessed 15 June 2018).

112. Wulgaert, T., 2005. Security Awareness: Best Practices to Secure Your Enterprise, ISACA.

113. Zaaba, Z. F., Furnell, S. M., & Dowland, P. S., 2014. A study on improving security warnings. In Information and Communication Technology for The Muslim World (ICT4M), 2014 The 5th International Conference on (pp. 1-5). IEEE.

Bibliography

1. Bryant, P., Furnell, S.M. and Phippen, A.D., 2008. Improving protection and security awareness amongst home users. Advances in Networks, Computing and Communications, 4, p.182.
2. Cavusoglu, H., Cavusoglu, H. & Raghunathan, S., 2004. Economics of IT Security Management: Four Improvements to Current Security Practices. Communications of the Association for Information Systems, 14(1), pp. 65-75.
3. Cohen, F., 1999. Managing network security: The limits of awareness. Network Security, 1999(6), pp.8-10.
4. Daryanani, M., 2012. Overload Information. ITNOW, 54 (3), 26-27.
5. Ernst & Young. 2008. Identity and Access Management, beyond compliance. Insights on governance, risk and compliance. EYG no. AU1638. Retrieved from: https://www.ey.com/publication/vwluassets/identity_and_access_management_beyond_compliance/$file/identity_and_access_management_beyond_compliance_au1638.pdf (Accessed 20 September 2013).
6. Furnell, S., Warren, A. and Dowland, P.S., 2004. Improving security awareness and training through computer-based training. In Proceedings of the 3rd World Conference on Information Security Education (WISE 2004). California: Monterey.
7. Furnell, S.M, Gennatou M, Dowland P.S., 2000. Promoting security awareness training within small organisations. Proceedings of the First Australian Information Security Management (AISM) Workshop, Geelong, Australia, 2000.
8. Furnell, S.M., Gennatou, M. & Dowland, P.S., 2002. A prototype tool for information security awareness and training. Logistics Information Management, 15(5/6), pp.352-357.

9. Hansche, S., 2001a. Designing a Security Awareness Program: Part 1. Information Systems Security, 9, 1-9.
10. Hansche, S., 2001b. Making Security Awareness Happen, part 1. Auerbach Publications. 2001 CRC Press LLC. Retrieved from: http://ittoday.info/AIMS/DSM/82-01-02.pdf (Accessed 25 February 2013).
11. Hansche, S., 2001c. Information system security training: Making it happen, Part 2. Information systems security, 10 (3), pp.51-70.
12. Kruger, H. A. & Kearney, W. D., 2006. A prototype for assessing information security awareness. Computers & Security, 25, 289-296.
13. Kruger, H.A., Drevin, L. and Steyn, T., 2006. A Framework for Evaluating ICT Security Awareness. In ISSA (pp. 1-11). Retrieved from: http://icsa.cs.up.ac.za/issa/2006/Proceedings/Full/17_Paper.pdf (Accessed 15 March 2013).
14. Leach, J., 2003. Improving user security behaviour. Computers & Security, 22(8), pp.685-692.
15. Neidich, J. 2004. IT Security Awareness Best Practices. Global Information Assurance Certification Paper. Version 1.4b. SANS Cyber Defense Whitepapers. SANS Institute. Retrieved from: https://www.giac.org/paper/gsec/4087/security-awareness-practices/106602 (Accessed 10 September 2016).
16. Ransbotham, S. & Mitra, S., 2009. Choice and chance: A conceptual model of paths to information security compromise. Information Systems Research, 20 (1), pp.121-139.
17. Rezgui, Y. and Marks, A., 2008. Information security awareness in higher education: An exploratory study. Computers & Security, 27(7-8), pp.241-253.
18. Schultz, E.E., 2004. Security training and awareness - fitting a square peg in a round hole. Computers & Security, 23, 1-2.

19. Spurling, P., 1995. Promoting security awareness and commitment. Information management & computer security, 3(2), pp.20-26.
20. Talib, S., Clarke, N.L. and Furnell, S.M., 2010, February. An analysis of information security awareness within home and work environments. In Availability, Reliability, and Security, 2010. ARES'10 International Conference on (pp. 196-203). IEEE.
21. Thomson, M.E. and von Solms, R., 1998. Information security awareness: educating your users effectively. Information management & computer security, 6(4), pp.167-173.
22. Tsaganidi, V-G., & Furnell,S.M., 2008. Assessing Protection and Security Awareness amongst Home Users, Advances in Communications, Computing, Networks and Security: Volume 5. ISBN: 978-1-84102-257-4, pp303-312.
23. Valentine, J.A., 2006. Enhancing the employee security awareness model. Computer Fraud & Security, 2006 (6), pp.17-19.

Appendices

Appendix A – Ethical Approval (Experimental and Post-Experiment surveys)

From: Paula Simson on behalf of Science and Engineering Human Ethics
Sent: 15 January 2016 15:19
To: Najem Mahmoud
Cc: Steven Furnell; Paul Dowland
Subject: RE: Application for Ethical Approval (Najem Mahmoud)

Dear Najem

I am pleased to confirm your application has been approved and I have attached your approval letter.

Best wishes
Paula

From: Paula Simson on behalf of Science and Engineering Human Ethics**Sent:** 22 December 2015 14:41
To: Najem Mahmoud
Cc: Steven Furnell; Paul Dowland
Subject: RE: Application for Ethical Approval (Najem Mahmoud)

Dear Najem

Thank you for submitting your ethical approval application, I will forward this to the Ethics Committee to consider today, and will let you know their decision as soon as possible in the New Year.

Best wishes
Paula

Paula Simson I Administrative assistant I Dean's Office I Faculty of Science and Engineering I 009 Smeaton I Ext 84503 I email paula.simson@plymouth.ac.uk
Working hours: Monday – Thursday 09.30 – 17.00 Friday 09.30 – 16.30

From: Najem Mahmoud
Sent: 22 December 2015 13:56
To: Paula Simson
Cc: Steven Furnell; Paul Dowland; Science and Engineering Human Ethics
Subject: Application for Ethical Approval (Najem Mahmoud)
Importance: High

Dear Paula,

Please find attached a completed application for Ethical approval that is needed for my research study.

Should you need any further information, please do not hesitate to contact me.

Best Regards,

Najem Mahmoud

Centre for Security, Communications and Network Research (CSCAN)
School of Computing and Mathematics
Faculty of Science and Engineering
University of Plymouth
Office#: A304, Portland Square Building
University of Plymouth, Drake Circus,
Plymouth, PL4 8AA, UK
Office Tel: +44 (0) 1752586287

Appendix B- Post-Experiment Participant Feedback (surveys)

Wi-Fi Interface Testing (Group A)

INFOSECURITY WITH PLYMOUTH UNIVERSITY

Centre for Security, Communications and Network Research (CSCAN)

This survey is being conducted for PhD research on testing different alternatives for user interface design in the context of Wi-Fi networking at Plymouth University, United Kingdom. The survey aims to investigate and find out whether users would connect or continue to connect if they have been given extra informative information before they make their decision to access unknown Wi-Fi hotspots within public environments. There are 5 main sections in this survey.

Researcher details:

Najem Mahmoud

Centre for Security, Communications and Network Research (CSCAN)

School of Computing, Electronics and Mathematics

Plymouth University

Plymouth, PL4 8AA

United Kingdom

E-mail: najem.mahmoud@plymouth.ac.uk

Project Supervisors: Prof. Steven Furnell and Dr. Paul Dowland.

A note on privacy

This survey is anonymous.

The record kept of your survey responses does not contain any identifying information about you.

If you click 'Next', you confirm that you have read and understood the information given, understand that you are free to withdraw up until the point of submission of your responses, you are 18 years or above, and agree to take part in the study.

Section (A)

- What is your gender?

Male	□
Female	□

- What is your age group (in years)?

18-29	□
30-39	□
40-49	□
50-59	□
60+	□

- What is your current employment status:

Employed	☐
Self-employed	☐
Student	☐
Other	☐

- What is your highest educational level?

Postgraduate (e.g. Masters, PhD)	☐
Higher education (e.g. Bachelor Degree, HND, Diploma)	☐
Further education (e.g. Certificates, A-Levels, GNVQ)	☐
Other	☐

Section (B)

- The instructions provided were suitably clear.

Strongly agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree
☐	☐	☐	☐	☐

- To what extent do you feel that you followed the instructions?

Fully	Moderately	Partially	Did not follow any
☐	☐	☐	☐

Section (C)

- How frequently do you use the following types of Wi-Fi connections? (Please select the most appropriate choice for each row).

	Hourly	Daily	Weekly	Monthly	Rarely	N/A
Wi-Fi (Home)	☐	☐	☐	☐	☐	☐
Wi-Fi (Public)	☐	☐	☐	☐	☐	☐
Wi-Fi (Work)	☐	☐	☐	☐	☐	☐

- Considering your use of Wi-Fi (Home), please select how frequently do you perform the following tasks?

	Frequently	Sometimes	Not used at all
Checking email	☐	☐	☐
Online banking	☐	☐	☐
Social networking	☐	☐	☐
Do bookings	☐	☐	☐
Buying/ Selling goods	☐	☐	☐
Other	☐	☐	☐

- Considering your use of Wi-Fi (Public), please select how frequently do you perform the following tasks?

	Frequently	Sometimes	Not used at all
Checking email	☐	☐	☐
Online banking	☐	☐	☐
Social networking	☐	☐	☐
Do bookings	☐	☐	☐
Buying/ Selling goods	☐	☐	☐
Other	☐	☐	☐

- Considering your use of Wi-Fi (Work), please select how frequently do you perform the following tasks?

	Frequently	Sometimes	Not used at all
Checking email	☐	☐	☐
Online banking	☐	☐	☐
Social networking	☐	☐	☐
Do bookings	☐	☐	☐
Buying/ Selling goods	☐	☐	☐
Other	☐	☐	☐

- Do you know the difference between secure and unsecure Wi-Fi?

Yes	No	Somewhat	Not sure
☐	☐	☐	☐

*Note: If the answer is "No" or "Somewhat", please provide more details in the opposite comments box.

Section (D)

- Was the information provided by the software easy to understand?

Yes	No	Somewhat	Not sure
☐	☐	☐	☐

*Note: If the answer is "No" or "Somewhat", please provide more details in the opposite comments box.

- Do you think the usability aspect can be improved?

Yes	No	Somewhat	Not sure
☐	☐	☐	☐

*Note: If the answer is "Yes" or "Somewhat", please provide more details in the opposite comments box.

- How satisfied were you about the supported information about the presented networks?

Completely satisfied	Very satisfied	Somewhat satisfied	Very dissatisfied	Completely dissatisfied
☐	☐	☐	☐	☐

- Did you feel confident that you connected to an appropriate network?

Yes	No	Somewhat	Not sure
☐	☐	☐	☐

*Note: If the answer is "No" or "Somewhat", please provide more details in the opposite comments box.

- Did you consider the security aspects of the Wi-Fi network when you made your decision?

Yes	No	Somewhat	Not sure
☐	☐	☐	☐

*Note: If the answer is "No" or "Somewhat", please provide more details in the opposite comments box.

- (If yes), did you feel that you had enough information to make a decision about whether the network was safe/trustworthy or not?

Yes	No	Somewhat	Not sure
☐	☐	☐	☐

*Note: If the answer is "No" or "Somewhat", please provide more details in the opposite comments box.

- What are the security features did you look at when you made your decision?

The network uses security protocols	☐
The network uses encryption protocols	☐
Network Name	☐
None of the above	☐

- Do you know whether the Wi-Fi connection you selected was secure or not?

Yes	No	Somewhat	Not sure
☐	☐	☐	☐

*Note: If the answer is "No" or "Somewhat", please provide more details in the opposite comments box.

- Are you aware of the security risks associated with the use of insecure Wi-Fi hotspots?

Yes	No	Somewhat	Not sure
☐	☐	☐	☐

- Please indicate how concerned are you when connecting to unsecured Wi-Fi hotspots?

Not at all concerned	Slightly concerned	Moderately concerned	Very concerned	Extremely concerned
☐	☐	☐	☐	☐

*Note: If the answer is " Not at all concerned " or " Slightly concerned ", please provide more details in the opposite comments box.

- From your point of view, please rank the security features that the user must take into account before using Wi-Fi hotspots.

	Very important	Important	Neither important nor unimportant	Unimportant	Very unimportant
Security protocols	☐	☐	☐	☐	☐
Encryption protocols	☐	☐	☐	☐	☐
Network Name	☐	☐	☐	☐	☐

- After your experience today, please rank how likely your behaviour online would be changed depending on whether your Wi-Fi connection is secure or not?

Not at all likely	Slightly likely	Moderately likely	Very likely	Completely Changed
☐	☐	☐	☐	☐

*Note: If the answer is “Not at all likely " or " Slightly likely ", please provide more details in the opposite comments box.

Section (E)

- This system has the functions and capabilities I expect it to have.

Yes	No	Somewhat	Not sure
☐	☐	☐	☐

*Note: If the answer is "No" or "Somewhat", please provide more details in the opposite comments box.

- Overall, I am satisfied with the software system.

Yes	No	Somewhat	Not sure
☐	☐	☐	☐

*Note: If the answer is "No" or "Somewhat", please provide more details in the opposite comments box.

Wi-Fi Interface Testing (Group B)

Centre for Security, Communications and Network Research (CSCAN)

This survey is being conducted for PhD research on testing different alternatives for user interface design in the context of Wi-Fi networking at Plymouth University, United Kingdom. The survey aims to investigate and find out whether users would connect or continue to connect if they have been given extra informative information before they make their decision to access unknown Wi-Fi hotspots within public environments.

There are 5 main sections in this survey.

Researcher details:

Najem Mahmoud

Centre for Security, Communications and Network Research (CSCAN)

School of Computing, Electronics and Mathematics

Plymouth University

Plymouth, PL4 8AA

United Kingdom

E-mail: najem.mahmoud@plymouth.ac.uk

Project Supervisors: Prof. Steven Furnell and Dr. Paul Dowland.

A note on privacy

This survey is anonymous.

The record kept of your survey responses does not contain any identifying information about you.

If you click 'Next', you confirm that you have read and understood the information given, understand that you are free to withdraw up until the point of submission of your responses, you are 18 years or above, and agree to take part in the study.

Section (A)

- What is your gender?

Male	□
Female	□

- What is your age group (in years)?

18-29	□
30-39	□
40-49	□
50-59	□
60+	□

- What is your current employment status:

Employed	☐
Self-employed	☐
Student	☐
Other	☐

- What is your highest educational level?

Postgraduate (e.g. Masters, PhD)	☐
Higher education (e.g. Bachelor Degree, HND, Diploma)	☐
Further education (e.g. Certificates, A-Levels, GNVQ)	☐
Other	☐

Section (B)

- The instructions provided were suitably clear.

Strongly agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree
☐	☐	☐	☐	☐

- To what extent do you feel that you followed the instructions?

Fully	Moderately	Partially	Did not follow any
☐	☐	☐	☐

Section (C)

- How frequently do you use the following types of Wi-Fi connections? (Please select the most appropriate choice for each row).

	Hourly	Daily	Weekly	Monthly	Rarely	N/A
Wi-Fi (Home)	☐	☐	☐	☐	☐	☐
Wi-Fi (Public)	☐	☐	☐	☐	☐	☐
Wi-Fi (Work)	☐	☐	☐	☐	☐	☐

- Considering your use of Wi-Fi (Home), please select how frequently do you perform the following tasks?

	Frequently	Sometimes	Not used at all
Checking email	☐	☐	☐
Online banking	☐	☐	☐
Social networking	☐	☐	☐
Do bookings	☐	☐	☐
Buying/ Selling goods	☐	☐	☐
Other	☐	☐	☐

- Considering your use of Wi-Fi (Public), please select how frequently do you perform the following tasks?

	Frequently	Sometimes	Not used at all
Checking email	☐	☐	☐
Online banking	☐	☐	☐
Social networking	☐	☐	☐
Do bookings	☐	☐	☐
Buying/ Selling goods	☐	☐	☐
Other	☐	☐	☐

- Considering your use of Wi-Fi (Work), please select how frequently do you perform the following tasks?

	Frequently	Sometimes	Not used at all
Checking email	☐	☐	☐
Online banking	☐	☐	☐
Social networking	☐	☐	☐
Do bookings	☐	☐	☐
Buying/ Selling goods	☐	☐	☐
Other	☐	☐	☐

- Do you know the difference between secure and unsecure Wi-Fi?

Yes	No	Somewhat	Not sure
☐	☐	☐	☐

*Note: If the answer is "No" or "Somewhat", please provide more details in the opposite comments box.

Section (D)

- Was the information provided by the software easy to understand?

Yes	No	Somewhat	Not sure
☐	☐	☐	☐

*Note: If the answer is "No" or "Somewhat", please provide more details in the opposite comments box.

- Do you think the usability aspect can be improved?

Yes	No	Somewhat	Not sure
☐	☐	☐	☐

*Note: If the answer is "Yes" or "Somewhat", please provide more details in the opposite comments box.

- How satisfied were you about the supported information about the presented networks?

Completely satisfied	Very satisfied	Somewhat satisfied	Very dissatisfied	Completely dissatisfied
☐	☐	☐	☐	☐

- Did you feel confident that you connected to an appropriate network?

Yes	No	Somewhat	Not sure
☐	☐	☐	☐

*Note: If the answer is "No" or "Somewhat", please provide more details in the opposite comments box.

- Did you consider the security aspects of the Wi-Fi network when you made your decision?

Yes	No	Somewhat	Not sure
☐	☐	☐	☐

*Note: If the answer is "No" or "Somewhat", please provide more details in the opposite comments box.

- (If yes), did you feel that you had enough information to make a decision about whether the network was safe/trustworthy or not?

Yes	No	Somewhat	Not sure
☐	☐	☐	☐
*Note: If the answer is "No" or "Somewhat", please provide more details in the opposite comments box.			

- What are the security features did you look at when you made your decision?

The network uses security protocols	☐
The network uses encryption protocols	☐
Network Name	☐
None of the above	☐

- Do you know whether the Wi-Fi connection you selected was secure or not?

Yes	No	Somewhat	Not sure
☐	☐	☐	☐

*Note: If the answer is "No" or "Somewhat", please provide more details in the opposite comments box.

- Are you aware of the security risks associated with the use of insecure Wi-Fi hotspots?

Yes	No	Somewhat	Not sure
☐	☐	☐	☐

- Please indicate how concerned are you when connecting to unsecured Wi-Fi hotspots?

Not at all concerned	Slightly concerned	Moderately concerned	Very concerned	Extremely concerned
☐	☐	☐	☐	☐

*Note: If the answer is " Not at all concerned " or " Slightly concerned ", please provide more details in the opposite comments box.

- From your point of view, please rank the security features that the user must take into account before using Wi-Fi hotspots.

	Very important	Important	Neither important nor unimportant	Unimportant	Very unimportant
Security protocols	☐	☐	☐	☐	☐
Encryption protocols	☐	☐	☐	☐	☐
Network Name	☐	☐	☐	☐	☐

- After your experience today, please rank how likely your behaviour online would be changed depending on whether your Wi-Fi connection is secure or not?

Not at all likely	Slightly likely	Moderately likely	Very likely	Completely Changed
☐	☐	☐	☐	☐

*Note: If the answer is “Not at all likely " or " Slightly likely ", please provide more details in the opposite comments box.

Section (E)

- Does the new design make the information more presentable than the current dashboard that displays the wireless networks in the Windows platform?

Yes	No	Somewhat	Not sure
☐	☐	☐	☐

*Note: If the answer is "No" or "Somewhat", please provide more details in the opposite comments box.

- This system has the functions and capabilities I expect it to have.

Yes	No	Somewhat	Not sure
☐	☐	☐	☐

*Note: If the answer is "No" or "Somewhat", please provide more details in the opposite comments box.

- Using the software system was convenient.

Yes	No	Somewhat	Not sure
☐	☐	☐	☐

*Note: If the answer is "No" or "Somewhat", please provide more details in the opposite comments box.

- I think the full implementation of the software can be used to facilitate users in choosing the appropriately secure Wi-Fi network.

Yes	No	Somewhat	Not sure
☐	☐	☐	☐

*Note: If the answer is "No" or "Somewhat", please provide more details in the opposite comments box.

- Overall, I am satisfied with the software system.

Yes	No	Somewhat	Not sure
☐	☐	☐	☐

Wi-Fi Interface Testing (Group C)

Centre for Security, Communications and Network Research (CSCAN)

This survey is being conducted for PhD research on testing different alternatives for user interface design in the context of Wi-Fi networking at Plymouth University, United Kingdom. The survey aims to investigate the information that users would find useful in determining whether or not to connect to unknown Wi-Fi hotspots within different public environments.

There are 5 main sections in this survey.

Researcher details:

Najem Mahmoud

Centre for Security, Communications and Network Research (CSCAN)

School of Computing, Electronics and Mathematics

Plymouth University

Plymouth, PL4 8AA

United Kingdom

E-mail: najem.mahmoud@plymouth.ac.uk

Project Supervisors: Prof. Steven Furnell and Dr. Paul Dowland.

A note on privacy

This survey is anonymous.

The record kept of your survey responses does not contain any identifying information about you.

If you click 'Next', you confirm that you have read and understood the information given, understand that you are free to withdraw up until the point of submission of your responses, you are 18 years or above, and agree to take part in the study

Section (A)

- What is your gender?

Male	□
Female	□

- What is your age group (in years)?

18-29	□
30-39	□
40-49	□
50-59	□
60+	□

- What is your current employment status:

Employed	☐
Self-employed	☐
Student	☐
Other	☐

- What is your highest educational level?

Postgraduate (e.g. Masters, PhD)	☐
Higher education (e.g. Bachelor Degree, HND, Diploma)	☐
Further education (e.g. Certificates, A-Levels, GNVQ)	☐
Other	☐

Section (B)

The instructions provided were suitably clear.

Strongly agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree
☐	☐	☐	☐	☐

- To what extent do you feel that you followed the instructions?

Fully	Moderately	Partially	Did not follow any
☐	☐	☐	☐

Section (C)

- How frequently do you use the following types of Wi-Fi connections? (Select the most appropriate choice for each row).

	Hourly	Daily	Weekly	Monthly	Rarely	N/A
Wi-Fi (Home)	☐	☐	☐	☐	☐	☐
Wi-Fi (Public)	☐	☐	☐	☐	☐	☐
Wi-Fi (Work)	☐	☐	☐	☐	☐	☐

- Considering your use of Wi-Fi (Home), please select how frequently do you perform the following tasks?

	Frequently	Sometimes	Not used at all
Checking email	☐	☐	☐
Online banking	☐	☐	☐
Social networking	☐	☐	☐
Do bookings	☐	☐	☐
Buying/ Selling goods	☐	☐	☐
Other	☐	☐	☐

- Considering your use of Wi-Fi (Public), please select how frequently do you perform the following tasks?

	Frequently	Sometimes	Not used at all
Checking email	☐	☐	☐
Online banking	☐	☐	☐
Social networking	☐	☐	☐
Do bookings	☐	☐	☐
Buying/ Selling goods	☐	☐	☐
Other	☐	☐	☐

- Considering your use of Wi-Fi (Work), please select how frequently do you perform the following tasks?

	Frequently	Sometimes	Not used at all
Checking email	☐	☐	☐
Online banking	☐	☐	☐
Social networking	☐	☐	☐
Do bookings	☐	☐	☐
Buying/ Selling goods	☐	☐	☐
Other	☐	☐	☐

- Do you know the difference between secure and unsecure Wi-Fi?

Yes	No	Somewhat	Not sure
☐	☐	☐	☐

*Note: If the answer is "No" or "Somewhat", please provide more details in the opposite comments box.

Section (D)

- Was the information provided by the software easy to understand?

Yes	No	Somewhat	Not sure
☐	☐	☐	☐

*Note: If the answer is "No" or "Somewhat", please provide more details in the opposite comments box.

- Do you think the usability aspect can be improved?

Yes	No	Somewhat	Not sure
☐	☐	☐	☐

*Note: If the answer is "Yes" or "Somewhat", please provide more details in the opposite comments box.

- Was the security level indicator helpful?

Yes	No	Somewhat	Not sure
☐	☐	☐	☐

*Note: If the answer is "No" or "Somewhat", please provide more details in the opposite comments box.

- How satisfied were you about the supported information about the presented networks?

Completely satisfied	Very satisfied	Somewhat satisfied	Very dissatisfied	Completely dissatisfied
☐	☐	☐	☐	☐

- Did you feel confident that you connected to an appropriate network?

Yes	No	Somewhat	Not sure
☐	☐	☐	☐

*Note: If the answer is "No" or "Somewhat", please provide more details in the opposite comments box.

- Did you consider the security aspects of the Wi-Fi network when you made your decision?

Yes	No	Somewhat	Not sure
☐	☐	☐	☐

*Note: If the answer is "No" or "Somewhat", please provide more details in the opposite comments box.

- (If yes), did you feel that you had enough information to make a decision about whether the network was safe/trustworthy or not

Yes	No	Somewhat	Not sure
☐	☐	☐	☐

*Note: If the answer is "No" or "Somewhat", please provide more details in the opposite comments box.

- What are the security features did you look at when you made your decision?

The network uses security protocols	☐
The network uses encryption protocols	☐
Start Time	☐
Previously connected	☐
Network Name	☐
None of the above	☐

- Did you find the security information panel useful to help you to make your decision?

Yes	No	Somewhat	Not sure
☐	☐	☐	☐

*Note: If the answer is "No" or "Somewhat", please provide more details in the opposite comments box.

- Do you know whether the Wi-Fi connection you selected was secure or not?

Yes	No	Somewhat	Not sure
☐	☐	☐	☐

*Note: If the answer is "No" or "Somewhat", please provide more details in the opposite comments box.

- Are you aware of the security risks associated with the use of insecure Wi-Fi hotspots?

Yes	No	Somewhat	Not sure
☐	☐	☐	☐

- Please indicate how concerned are you when connecting to unsecured Wi-Fi hotspots?

Not at all concerned	Slightly concerned	Moderately concerned	Very concerned	Extremely concerned
☐	☐	☐	☐	☐

*Note: If the answer is " Not at all concerned " or " Slightly concerned ", please provide more details in the opposite comments box.

- From your point of view, please rank the security features that the user must take into account before using Wi-Fi hotspots.

	Very important	Important	Neither important nor unimportant	Unimportant	Very unimportant
Security protocols	☐	☐	☐	☐	☐
Encryption protocols	☐	☐	☐	☐	☐
Start Time	☐	☐	☐	☐	☐
Previously connected	☐	☐	☐	☐	☐
Network Name	☐	☐	☐	☐	☐
Security level indicator	☐	☐	☐	☐	☐

- After your experience today, please rank how likely your behaviour online would be changed depending on whether your Wi-Fi connection is secure or not?

Not at all likely	Slightly likely	Moderately likely	Very likely	Completely Changed
☐	☐	☐	☐	☐

*Note: If the answer is “Not at all likely " or " Slightly likely ", please provide more details in the opposite comments box.

Section (E)

- Does the new design make the information more presentable than the current dashboard that displays the wireless networks in the Windows platform?

Yes	No	Somewhat	Not sure
☐	☐	☐	☐

*Note: If the answer is "No" or "Somewhat", please provide more details in the opposite comments box.

- This system has the functions and capabilities I expect it to have.

Yes	No	Somewhat	Not sure
☐	☐	☐	☐

*Note: If the answer is "No" or "Somewhat", please provide more details in the opposite comments box.

- Using the software system was convenient.

Yes	No	Somewhat	Not sure
☐	☐	☐	☐

*Note: If the answer is "No" or "Somewhat", please provide more details in the opposite comments box.

- I am more confident in using Wi-Fi software that provides security related information because it helps me to decide whether it is safe to connect to an available Wi-Fi network.

Strongly agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree
☐	☐	☐	☐	☐

*Note: If the answer is " Disagree or Strongly disagree “or “Strongly disagree ", please provide more details in the opposite comments box.

- I think the full implementation of the software can be used to facilitate users in choosing the appropriately secure Wi-Fi network.

Yes	No	Somewhat	Not sure
☐	☐	☐	☐

*Note: If the answer is "No" or "Somewhat", please provide more details in the opposite comments box.

- Overall, I am satisfied with the software system.

Yes	No	Somewhat	Not sure
☐	☐	☐	☐

*Note: If the answer is "No" or "Somewhat", please provide more details in the opposite comments box.

Wi-Fi Interface Testing (Group D)

Centre for Security, Communications and Network Research (CSCAN)

This survey is being conducted for PhD research on testing different alternatives for user interface design in the context of Wi-Fi networking at Plymouth University, United Kingdom. The survey aims to investigate the information that users would find useful in determining whether or not to connect to unknown Wi-Fi hotspots within different public environments.

There are 5 main sections in this survey.

Researcher details:

Najem Mahmoud

Centre for Security, Communications and Network Research (CSCAN)

School of Computing, Electronics and Mathematics

Plymouth University

Plymouth, PL4 8AA

United Kingdom

E-mail: najem.mahmoud@plymouth.ac.uk

Project Supervisors: Prof. Steven Furnell and Dr. Paul Dowland.

A note on privacy

This survey is anonymous.

The record kept of your survey responses does not contain any identifying information about you.

If you click 'Next', you confirm that you have read and understood the information given, understand that you are free to withdraw up until the point of submission of your responses, you are 18 years or above, and agree to take part in the study

Section (A)

- What is your gender?

Male	□
Female	□

- What is your age group (in years)?

18-29	□
30-39	□
40-49	□
50-59	□
60+	□

- What is your current employment status:

Employed	☐
Self-employed	☐
Student	☐
Other	☐

- What is your highest educational level?

Postgraduate (e.g. Masters, PhD)	☐
Higher education (e.g. Bachelor Degree, HND, Diploma)	☐
Further education (e.g. Certificates, A-Levels, GNVQ)	☐
Other	☐

Section (B)

The instructions provided were suitably clear.

Strongly agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree
☐	☐	☐	☐	☐

- To what extent do you feel that you followed the instructions?

Fully	Moderately	Partially	Did not follow any
☐	☐	☐	☐

Section (C)

- How frequently do you use the following types of Wi-Fi connections? (Select the most appropriate choice for each row).

	Hourly	Daily	Weekly	Monthly	Rarely	N/A
Wi-Fi (Home)	☐	☐	☐	☐	☐	☐
Wi-Fi (Public)	☐	☐	☐	☐	☐	☐
Wi-Fi (Work)	☐	☐	☐	☐	☐	☐

- Considering your use of Wi-Fi (Home), please select how frequently do you perform the following tasks?

	Frequently	Sometimes	Not used at all
Checking email	☐	☐	☐
Online banking	☐	☐	☐
Social networking	☐	☐	☐
Do bookings	☐	☐	☐
Buying/ Selling goods	☐	☐	☐
Other	☐	☐	☐

- Considering your use of Wi-Fi (Public), please select how frequently do you perform the following tasks?

	Frequently	Sometimes	Not used at all
Checking email	☐	☐	☐
Online banking	☐	☐	☐
Social networking	☐	☐	☐
Do bookings	☐	☐	☐
Buying/ Selling goods	☐	☐	☐
Other	☐	☐	☐

- Considering your use of Wi-Fi (Work), please select how frequently do you perform the following tasks?

	Frequently	Sometimes	Not used at all
Checking email	☐	☐	☐
Online banking	☐	☐	☐
Social networking	☐	☐	☐
Do bookings	☐	☐	☐
Buying/ Selling goods	☐	☐	☐
Other	☐	☐	☐

- Do you know the difference between secure and unsecure Wi-Fi?

Yes	No	Somewhat	Not sure
☐	☐	☐	☐

*Note: If the answer is "No" or "Somewhat", please provide more details in the opposite comments box.

Section (D)

- Was the information provided by the software easy to understand?

Yes	No	Somewhat	Not sure
☐	☐	☐	☐

*Note: If the answer is "No" or "Somewhat", please provide more details in the opposite comments box.

- Do you think the usability aspect can be improved?

Yes	No	Somewhat	Not sure
☐	☐	☐	☐

*Note: If the answer is "Yes" or "Somewhat", please provide more details in the opposite comments box.

- Was the security level indicator helpful?

Yes	No	Somewhat	Not sure
☐	☐	☐	☐

*Note: If the answer is "No" or "Somewhat", please provide more details in the opposite comments box.

- How satisfied were you about the supported information about the presented networks?

Completely satisfied	Very satisfied	Somewhat satisfied	Very dissatisfied	Completely dissatisfied
☐	☐	☐	☐	☐

- Did you feel confident that you connected to an appropriate network?

Yes	No	Somewhat	Not sure
☐	☐	☐	☐

*Note: If the answer is "No" or "Somewhat", please provide more details in the opposite comments box.

- Did you consider the security aspects of the Wi-Fi network when you made your decision?

Yes	No	Somewhat	Not sure
☐	☐	☐	☐

*Note: If the answer is "No" or "Somewhat", please provide more details in the opposite comments box.

- (If yes), did you feel that you had enough information to make a decision about whether the network was safe/trustworthy or not?

Yes	No	Somewhat	Not sure
☐	☐	☐	☐

*Note: If the answer is "No" or "Somewhat", please provide more details in the opposite comments box.

- What are the security features did you look at when you made your decision?

The network uses security protocols	☐
The network uses encryption protocols	☐
Start Time	☐
Previously connected	☐
Network Name	☐
None of the above	☐

- Did you find the security information panel useful to help you to make your decision?

Yes	No	Somewhat	Not sure
☐	☐	☐	☐

*Note: If the answer is "No" or "Somewhat", please provide more details in the opposite comments box.

- Do you know whether the Wi-Fi connection you selected was secure or not?

Yes	No	Somewhat	Not sure
☐	☐	☐	☐

*Note: If the answer is "No" or "Somewhat", please provide more details in the opposite comments box.

- Are you aware of the security risks associated with the use of insecure Wi-Fi hotspots?

Yes	No	Somewhat	Not sure
☐	☐	☐	☐

- Please indicate how concerned are you when connecting to unsecured Wi-Fi hotspots?

Not at all concerned	Slightly concerned	Moderately concerned	Very concerned	Extremely concerned
☐	☐	☐	☐	☐

*Note: If the answer is " Not at all concerned " or " Slightly concerned ", please provide more details in the opposite comments box.

- From your point of view, please rank the security features that the user must take into account before using Wi-Fi hotspots.

	Very important	Important	Neither important nor unimportant	Unimportant	Very unimportant
Security protocols	☐	☐	☐	☐	☐
Encryption protocols	☐	☐	☐	☐	☐
Start Time	☐	☐	☐	☐	☐
Previously connected	☐	☐	☐	☐	☐
Network Name	☐	☐	☐	☐	☐
Security level indicator	☐	☐	☐	☐	☐

- After your experience today, please rank how likely your behaviour online would be changed depending on whether your Wi-Fi connection is secure or not?

Not at all likely	Slightly likely	Moderately likely	Very likely	Completely Changed
☐	☐	☐	☐	☐

*Note: If the answer is “Not at all likely " or " Slightly likely ", please provide more details in the opposite comments box.

Section (E)

- Does the new design make the information more presentable than the current dashboard that displays the wireless networks in the Windows platform?

Yes	No	Somewhat	Not sure
☐	☐	☐	☐

*Note: If the answer is "No" or "Somewhat", please provide more details in the opposite comments box.

- This system has the functions and capabilities I expect it to have.

Yes	No	Somewhat	Not sure
☐	☐	☐	☐

*Note: If the answer is "No" or "Somewhat", please provide more details in the opposite comments box.

- Using the software system was convenient.

Yes	No	Somewhat	Not sure
☐	☐	☐	☐

*Note: If the answer is "No" or "Somewhat", please provide more details in the opposite comments box.

- I am more confident in using Wi-Fi software that provides security related information because it helps me to decide whether it is safe to connect to an available Wi-Fi network.

Strongly agree	Agree	Neither agree nor disagree	Disagree	Strongly disagree
☐	☐	☐	☐	☐

*Note: If the answer is " Disagree or Strongly disagree “or “Strongly disagree ", please provide more details in the opposite comments box.

- I think the full implementation of the software can be used to facilitate users in choosing the appropriately secure Wi-Fi network.

Yes	No	Somewhat	Not sure
☐	☐	☐	☐

*Note: If the answer is "No" or "Somewhat", please provide more details in the opposite comments box.

- Overall, I am satisfied with the software system.

Yes	No	Somewhat	Not sure
☐	☐	☐	☐

*Note: If the answer is "No" or "Somewhat", please provide more details in the opposite comments box.

Appendix C – Ethical Approval Letter, Research Information Sheet, Consent Form and the Experiment Scenario

RESEARCH WITH PLYMOUTH UNIVERSITY

15 January 2016

CONFIDENTIAL
Najem Mahmoud
School of Computing, Electronics and Mathematics

Dear Najem

Ethical Approval Application

Thank you for submitting the ethical approval form and details concerning your project:

Targeted security awareness for end users

I am pleased to inform you that this has been approved.

Kind regards

Paula Simson
Secretary to Faculty Research Ethics Committee

Cc. Prof Steve Furnell
Dr Paul Dowland

Faculty of Science and Engineering
Plymouth University
Drake Circus
PL4 8AA

T +44 (0) 1752 584 584
F +44 (0) 1752 584 540
W www.plymouth.ac.uk

Mrs Christine Mushens BA
Faculty Business Manager

PLYMOUTH UNIVERSITY

School of Computing, Electronics and Mathematics

Faculty of Science and Engineering

RESEARCH INFORMATION SHEET

Name of researcher

Najem Mahmoud.

Title of Research

Targeted Security Awareness for End Users.

Aim of research

The purpose of the user trials is to investigate the usability and clarity of different user interfaces, and to determine whether they have an effect upon user decisions. Participants will be required to use prototype software that simulates the process of viewing available Wi-Fi networks and allowing the user to connect to the most appropriate network in different given scenarios.

Description of procedure

Users will be involved in the study for one session, which will include trying the proposed system for approximately 15 minutes.

After completing the practical activity, participants will be asked to complete an online survey to capture their views about the usability issues. This task also takes approximately 15 minutes.

Benefits of proposed research

The findings of the research will assist in determining the level of guidance that it is appropriate to provide to users when performing routine online tasks, without unduly interrupting or overloading the user within information.

Right to withdraw

Participants have the right to withdraw at any time and without giving a reason.

Contact for Further Information

If you require further information about this study, please do not hesitate to contact the researcher:
Najem Mahmoud, A304, Portland Square Building, Plymouth University.
Email: najem.mahmoud@plymouth.ac.uk. Telephone: 01752 586287, Mobile: 07447494349.

PLYMOUTH UNIVERSITY

School of Computing, Electronics and Mathematics

Faculty of Science and Engineering

CONSENT TO PARTICIPATE IN PRACTICAL RESEARCH STUDY

Name of researcher

Najem Mahmoud

Title of Research

Targeted Security Awareness for End Users.

1. I confirm that I have read and understood the research information sheet for the above named study and have had the opportunity to ask questions.
2. I understand that I am free to withdraw at any time and without giving any reason.
3. I understand that all information collected in this study will be anonymous and strictly confidential.
4. I confirm that I am 18 years old or above.
5. I agree to participate in the research.

Name: ……..……..

Signature: .....…….. Date: .....…….

Experiment Scenario

Consider yourself at the university campus, and you are connecting to Wi-Fi hotspot to browse the Internet in order to use applications such as emails, online banking, and social networking services.

You are requested to use the wireless network selection interface to choose an appropriate network from which to conduct these activities.

Please note that you only need to select and connect to an appropriate network; you will not actually be required to send emails, or perform any of the other tasks mentioned above.

You will be asked to repeat the process several times, using different interface designs.

You will then be asked to comment upon the usefulness or suitability of the interfaces that were used.

Appendix D – Wi-Fi prototypes Software Code

Requirement: To run the code and for the best experience, use Microsoft Visual Studio 2015 or later version.

- **First Wi-Fi interface software code.**

(Simulating of *Existing interface used in MS Windows platforms*).

```
Public Class Form1

    Public network1 As Integer = 0
    Public network2 As Integer = 0
    Public network3 As Integer = 0
    Public network4 As Integer = 0

    Public startTime As DateTime
    Dim MyPanel1Clicked As Boolean = False
    Dim MyPanel2Clicked As Boolean = False
    Dim MyPanel3Clicked As Boolean = False
    Dim MyPanel4Clicked As Boolean = False

    Public eduroamPasswordEntered As Integer = 0
    Public eduroamLoginSuccessful As Integer = 0
    Public eduroamLoginFailed As Integer = 0
    Public eduroamCanceled As Integer = 0
    Public eduroamKilled As Integer = 0

Public Sub Button1_Click(sender As Object, e As EventArgs) Handles Button1.Click
        Dim win As Form2 = New Form2
        If Button1.Text = "Connect" Then
            win.ShowDialog(Me)
            If win.isSuccessful Then
                Button1.Text = "Disconnect"
                network1 = network1 + 1
                eduroamLoginSuccessful = eduroamLoginSuccessful + 1
                Button2.Text = "Connect"
                Button3.Text = "Connect"
                Button4.Text = "Connect"
            ElseIf win.isFailed Then
                eduroamLoginFailed = eduroamLoginFailed + 1
                Button1.Text = "Connect"
            ElseIf win.isCanceled Then
                eduroamCanceled = eduroamCanceled + 1
                Button1.Text = "Connect"
            Else
                eduroamKilled = eduroamKilled + 1
                Button1.Text = "Connect"
            End If
        ElseIf Button1.Text = "Disconnect" Then
            Button1.Text = "Connect"
        End If

        If win.isPasswordEnetered Then
            eduroamPasswordEntered = eduroamPasswordEntered + 1
        End If
```

```
    End Sub

    Private Sub Button2_Click(sender As Object, e As EventArgs) Handles
Button2.Click
        If Button2.Text = "Connect" Then
            Button2.Text = "Disconnect"
            network2 = network2 + 1
            Button1.Text = "Connect"
            Button3.Text = "Connect"
            Button4.Text = "Connect"
        Else
            Button2.Text = "Connect"
        End If
    End Sub
Private Sub Button3_Click(sender As Object, e As EventArgs) Handles Button3.Click
        If Button3.Text = "Connect" Then
            Button3.Text = "Disconnect"
            network3 = network3 + 1
            Button1.Text = "Connect"
            Button2.Text = "Connect"
            Button4.Text = "Connect"
        Else
            Button3.Text = "Connect"
        End If
    End Sub

    Private Sub Button4_Click(sender As Object, e As EventArgs) Handles
Button4.Click
        If Button4.Text = "Connect" Then
            Button4.Text = "Disconnect"
            network4 = network4 + 1
            Button1.Text = "Connect"
            Button2.Text = "Connect"
            Button3.Text = "Connect"
        Else
            Button4.Text = "Connect"
        End If
    End Sub

    Private Sub MyPanel1_MouseHover(sender As Object, e As EventArgs) Handles
MyPanel1.MouseHover
        MyPanel1.BorderColor = Color.SkyBlue
        MyPanel1.BorderWidth = 2
        MyPanel1.BackColor = Color.AliceBlue
    End Sub

    Private Sub MyPanel1_MouseLeave(sender As Object, e As EventArgs) Handles
MyPanel1.MouseLeave
        MyPanel1.BorderColor = Color.White
        MyPanel1.BorderWidth = 0
        MyPanel1.BackColor = Color.White
    End Sub

    Private Sub MyPanel2_MouseHover(sender As Object, e As EventArgs) Handles
MyPanel2.MouseHover
        MyPanel2.BorderColor = Color.SkyBlue
        MyPanel2.BorderWidth = 2
        MyPanel2.BackColor = Color.AliceBlue
    End Sub
```

```
    Private Sub MyPanel2_MouseLeave(sender As Object, e As EventArgs) Handles
MyPanel2.MouseLeave
        MyPanel2.BorderColor = Color.White
        MyPanel2.BorderWidth = 0
        MyPanel2.BackColor = Color.White
    End Sub

    Private Sub MyPanel3_MouseHover(sender As Object, e As EventArgs) Handles
MyPanel3.MouseHover
        MyPanel3.BorderColor = Color.SkyBlue
        MyPanel3.BorderWidth = 2
        MyPanel3.BackColor = Color.AliceBlue
    End Sub
Private Sub MyPanel3_MouseLeave(sender As Object, e As EventArgs) Handles
MyPanel3.MouseLeave
        MyPanel3.BorderColor = Color.White
        MyPanel3.BorderWidth = 0
        MyPanel3.BackColor = Color.White
    End Sub

    Private Sub MyPanel4_MouseHover(sender As Object, e As EventArgs) Handles
MyPanel4.MouseHover
        MyPanel4.BorderColor = Color.SkyBlue
        MyPanel4.BorderWidth = 2
        MyPanel4.BackColor = Color.AliceBlue
    End Sub

    Private Sub MyPanel4_MouseLeave(sender As Object, e As EventArgs) Handles
MyPanel4.MouseLeave
        MyPanel4.BorderColor = Color.White
        MyPanel4.BorderWidth = 0
        MyPanel4.BackColor = Color.White
    End Sub

    Private Sub MyPanel1_MouseClick(sender As Object, e As MouseEventArgs) Handles
MyPanel1.MouseClick
        CheckBox1.Visible = True
        Button1.Visible = True
        CheckBox2.Visible = False
        Button2.Visible = False
        CheckBox3.Visible = False
        Button3.Visible = False
        CheckBox4.Visible = False
        Button4.Visible = False
        PictureBox6.Visible = False
        Label5.Visible = False
        Label7.Visible = False
        PictureBox9.Visible = False
        Label6.Visible = False
        PictureBox10.Visible = False

    End Sub
Private Sub MyPanel2_MouseClick(sender As Object, e As MouseEventArgs) Handles
MyPanel2.MouseClick

        CheckBox1.Visible = False
        Button1.Visible = False
        CheckBox2.Visible = True
        Button2.Visible = True
        Label7.Visible = False
```

```
        PictureBox9.Visible = False
        CheckBox3.Visible = False
        Button3.Visible = False
        CheckBox4.Visible = False
        Button4.Visible = False
        PictureBox6.Visible = True
        Label5.Visible = True
        Label6.Visible = False
        PictureBox10.Visible = False
    End Sub

    Private Sub MyPanel3_MouseClick(sender As Object, e As MouseEventArgs) Handles
MyPanel3.MouseClick
        CheckBox1.Visible = False
        Button1.Visible = False
        CheckBox2.Visible = False
        Button2.Visible = False
        CheckBox3.Visible = True
        Button3.Visible = True
        PictureBox9.Visible = True
        Label6.Visible = True
        PictureBox10.Visible = False
        CheckBox4.Visible = False
        Button4.Visible = False
        PictureBox6.Visible = False
        Label5.Visible = False
        Label7.Visible = False
    End Sub

    Private Sub MyPanel4_MouseClick(sender As Object, e As MouseEventArgs) Handles
MyPanel4.MouseClick
        CheckBox1.Visible = False
        Button1.Visible = False
        CheckBox2.Visible = False
        Button2.Visible = False
        CheckBox3.Visible = False
        Button3.Visible = False
        CheckBox4.Visible = True
        Button4.Visible = True
        PictureBox6.Visible = False
        Label5.Visible = False
        Label7.Visible = True
        PictureBox9.Visible = False
        Label6.Visible = False
        PictureBox10.Visible = True
    End Sub
Private Sub MyPanel5_MouseClick(sender As Object, e As MouseEventArgs) Handles
MyPanel5.MouseClick
        CheckBox1.Visible = False
        Button1.Visible = False
        CheckBox2.Visible = False
        Button2.Visible = False
        CheckBox3.Visible = False
        Button3.Visible = False
        CheckBox4.Visible = False
        Button4.Visible = False
        PictureBox6.Visible = False
        Label5.Visible = False
        Label7.Visible = False
        PictureBox9.Visible = False
```

```
        Label6.Visible = False
        PictureBox10.Visible = False
    End Sub

    Private Sub Form1_FormClosing(sender As Object, e As FormClosingEventArgs)
Handles MyBase.FormClosing

        Dim path As String =
Environment.GetFolderPath(Environment.SpecialFolder.Desktop) +
"\MyControlGroup.csv"
        Dim currTime As DateTime = DateTime.Now
        Dim startMilliseconds As Long = CLng(startTime.Subtract(New DateTime(1970,
1, 1)).TotalMilliseconds)
        Dim milliseconds = CLng(currTime.Subtract(New DateTime(1970, 1,
1)).TotalMilliseconds)
        Dim ellapsedTime As Long = milliseconds - startMilliseconds
        Dim startDateString As String = startTime.ToString("dd MM yyyy")
        Dim startTimeString As String = startTime.ToString("hh:mm:ss")
        Dim endDateString As String = currTime.ToString("dd MM yyyy")
        Dim endTimeString As String = currTime.ToString("hh:mm:ss")
        Dim frirst As Integer = 1

        If System.IO.File.Exists(path) = True Then
            Dim text As String = network1 & "," _
                     & network2 & "," _
                     & network3 & "," _
                     & network4 & "," _
                     & startMilliseconds & "," _
                     & convertMsToMinSec(ellapsedTime) & "," _
                     & startDateString & "," _
                     & startTimeString & "," _
                     & endDateString & "," _
                     & endTimeString & "," _
                     & eduroamPasswordEntered & "," _
                     & eduroamLoginSuccessful & "," _
                     & eduroamLoginFailed & "," _
                     & eduroamCanceled & "," _
                     & eduroamKilled & vbNewLine

            System.IO.File.AppendAllText(path, Text)
        Else

            Dim header As String =
                       "eduroam" _
                     & ",BellacostaCafe" _
                     & ",withPlymouth" _
                     & ",eduroam highspeed" _
                     & ",StartMilliseconds" _
                     & ",Elapsed Time" _
                     & ",Start Date" _
                     & ",Start Time" _
                     & ",End Date" _
                     & ",End Time" _
                     & ",eduroamPasswordEntered" _
                     & ",eduroamLoginSuccessful  " _
                     & ",eduroamLoginFailed " _
                     & ",eduroamCanceled  " _
                     & ",eduroamKilled  " & vbNewLine

            Dim FirstRec As String = network1 & "," _
```

```
                    & network2 & "," _
                    & network3 & "," _
                    & network4 & "," _
                    & startMilliseconds & "," _
                    & convertMsToMinSec(ellapsedTime) & "," _
                    & startDateString & "," _
                    & startTimeString & "," _
                    & endDateString & "," _
                    & endTimeString & "," _
                    & eduroamPasswordEntered & "," _
                    & eduroamLoginSuccessful & "," _
                    & eduroamLoginFailed & "," _
                    & eduroamCanceled & "," _
                    & eduroamKilled & vbNewLine

            System.IO.File.AppendAllText(path, header)
            System.IO.File.AppendAllText(path, FirstRec)

        End If

    End Sub
    Private Sub Form1_Load(sender As Object, e As EventArgs) Handles MyBase.Load
        startTime = DateTime.Now
    End Sub

    Private Function convertMsToMinSec(millsec As Long) As String
        Dim result As String
        result = ""
        Dim time As Double
        time = millsec
        time = time / 1000
        time = time / 60
        Dim min As Integer
        Dim sec As Double
        min = Math.Truncate(time)
        time = time - min
        time = time * 60
        sec = time
        result = min.ToString() + ":" + sec.ToString()
        convertMsToMinSec = result
    End Function

End Class


Public Class Form2
    Public Username1 As String = "Alsharief"
    Public Password1 As String = "Alsharief77"
    Private Canceled As Boolean = False
    Private Successful As Boolean = False
    Private Failed As Boolean = False
    Private PasswordEntered As Boolean = False

    Public ReadOnly Property isCanceled As Boolean
        Get
            Return Canceled
        End Get
    End Property

    Public ReadOnly Property isPasswordEnetered As Boolean
```

```
        Get
            Return PasswordEntered
        End Get
    End Property
    Public ReadOnly Property isSuccessful As Boolean
        Get
            Return Successful
        End Get
    End Property

    Public ReadOnly Property isFailed As Boolean
        Get
            Return Failed
        End Get
    End Property
    Private Sub closeWin()
        Canceled = True
        Me.Close()
    End Sub

    Private Sub Cancel_Click(sender As Object, e As EventArgs) Handles
Cancel.Click
        Canceled = True
        Me.Close()
    End Sub

    Private Sub btnLogin_Click(sender As Object, e As EventArgs) Handles
Login.Click
        If (Username1 = TextBox1.Text And Password1 = TextBox2.Text) Then
            Successful = True
            Me.Close()
        Else
            Failed = True
            MsgBox("Password or username is invalid", MsgBoxStyle.Critical)
        End If
    End Sub
    Private Sub TextBox2_keypress(ByVal sender As Object, ByVal e As
System.Windows.Forms.KeyPressEventArgs) Handles TextBox2.KeyPress

        If TextBox2.Text <> " " Then
            PasswordEntered = True
        End If

    End Sub

End Class
```

- **Second Wi-Fi interface software code.**

(Improved user interface with a warning message).

```
Public Class Form1

    Public network1 As Integer = 0
    Public network2 As Integer = 0
    Public network3 As Integer = 0
    Public network4 As Integer = 0
    Public startTime As DateTime
    Dim MyPanel1Clicked As Boolean = False
    Dim MyPanel2Clicked As Boolean = False
    Dim MyPanel3Clicked As Boolean = False
    Dim MyPanel4Clicked As Boolean = False

    Public clickedAccept As Integer = 0
    Public clickedReject As Integer = 0
    Public Killedthewindow As Integer = 0

    Public eduroamPasswordEntered As Integer = 0
    Public eduroamLoginSuccessful As Integer = 0
    Public eduroamLoginFailed As Integer = 0
    Public eduroamCanceled As Integer = 0
    Public eduroamKilled As Integer = 0

    Public BellacostaCafeAccepted As Integer = 0
    Public BellacostaCafeRejected As Integer = 0
    Public BellacostaCafeKilled As Integer = 0

    Public withPlymouthAccepted As Integer = 0
    Public withPlymouthRejected As Integer = 0
    Public withPlymouthKilled As Integer = 0

    Public eduroamhighspeedAccepted As Integer = 0
    Public eduroamhighspeedRejected As Integer = 0
    Public eduroamhighspeedKilled As Integer = 0

Public Sub Button1_Click(sender As Object, e As EventArgs) Handles Button1.Click
        Dim win As Form2 = New Form2
        If Button1.Text = "Connect" Then
            win.ShowDialog(Me)
            If win.isSuccessful Then
                Button1.Text = "Disconnect"
                network1 = network1 + 1
                eduroamLoginSuccessful = eduroamLoginSuccessful + 1
                Button2.Text = "Connect"
                Button3.Text = "Connect"
                Button4.Text = "Connect"
            ElseIf win.isFailed Then
                eduroamLoginFailed = eduroamLoginFailed + 1
                Button1.Text = "Connect"
            ElseIf win.isCanceled Then
                eduroamCanceled = eduroamCanceled + 1
                Button1.Text = "Connect"
            Else
                eduroamKilled = eduroamKilled + 1
                Button1.Text = "Connect"
            End If
        ElseIf Button1.Text = "Disconnect" Then
            Button1.Text = "Connect"
```

```
        End If

        If win.isPasswordEnetered Then
            eduroamPasswordEntered = eduroamPasswordEntered + 1
        End If
    End Sub

    Private Sub Button2_Click(sender As Object, e As EventArgs) Handles
Button2.Click

        Dim win As WiFiSecurityWarning = New WiFiSecurityWarning()

        If Button2.Text = "Connect" Then
            win.ShowDialog(Me)
            If win.isAccepted Then
                Button2.Text = "Disconnect"
                network2 = network2 + 1
                BellacostaCafeAccepted = BellacostaCafeAccepted + 1
                Button1.Text = "Connect"
                Button3.Text = "Connect"
                Button4.Text = "Connect"
            ElseIf win.isRejected Then
                BellacostaCafeRejected = BellacostaCafeRejected + 1
                Button2.Text = "Connect"
            Else
                BellacostaCafeKilled = BellacostaCafeKilled + 1
                Button2.Text = "Connect"
            End If
        ElseIf Button2.Text = "Disconnect" Then
            Button2.Text = "Connect"
        End If
    End Sub

    Private Sub Button3_Click(sender As Object, e As EventArgs) Handles
Button3.Click

        Dim win As WiFiSecurityWarning = New WiFiSecurityWarning()

        If Button3.Text = "Connect" Then
            win.ShowDialog(Me)
        If win.isAccepted Then
            Button3.Text = "Disconnect"
            network3 = network3 + 1
            withPlymouthAccepted = withPlymouthAccepted + 1
            Button1.Text = "Connect"
            Button2.Text = "Connect"
            Button4.Text = "Connect"
        ElseIf win.isRejected Then
            withPlymouthRejected = withPlymouthRejected + 1
            Button3.Text = "Connect"
        Else
            withPlymouthKilled = withPlymouthKilled + 1
            Button3.Text = "Connect"
            End If
        ElseIf Button3.Text = "Disconnect" Then
            Button3.Text = "Connect"
        End If
    End Sub

Private Sub Button4_Click(sender As Object, e As EventArgs) Handles Button4.Click
```

```
        Dim win As WiFiSecurityWarning = New WiFiSecurityWarning()

        If Button4.Text = "Connect" Then
            win.ShowDialog(Me)
            If win.isAccepted Then
                Button4.Text = "Disconnect"
                network4 = network4 + 1
                eduroamhighspeedAccepted = eduroamhighspeedAccepted + 1
                Button1.Text = "Connect"
                Button2.Text = "Connect"
                Button3.Text = "Connect"
            ElseIf win.isRejected Then
                eduroamhighspeedRejected = eduroamhighspeedRejected + 1
                Button4.Text = "Connect"
            Else
                eduroamhighspeedKilled = eduroamhighspeedKilled + 1
                Button4.Text = "Connect"
            End If
        ElseIf Button4.Text = "Disconnect" Then
            Button4.Text = "Connect"
        End If
    End Sub

    Private Sub MyPanel1_MouseHover(sender As Object, e As EventArgs) Handles
MyPanel1.MouseHover
        MyPanel1.BorderColor = Color.SkyBlue
        MyPanel1.BorderWidth = 2
        MyPanel1.BackColor = Color.AliceBlue
    End Sub

    Private Sub MyPanel1_MouseLeave(sender As Object, e As EventArgs) Handles
MyPanel1.MouseLeave
        MyPanel1.BorderColor = Color.White
        MyPanel1.BorderWidth = 0
        MyPanel1.BackColor = Color.White
    End Sub

    Private Sub MyPanel2_MouseHover(sender As Object, e As EventArgs) Handles
MyPanel2.MouseHover
        MyPanel2.BorderColor = Color.SkyBlue
        MyPanel2.BorderWidth = 2
        MyPanel2.BackColor = Color.AliceBlue
    End Sub

    Private Sub MyPanel2_MouseLeave(sender As Object, e As EventArgs) Handles
MyPanel2.MouseLeave
        MyPanel2.BorderColor = Color.White
        MyPanel2.BorderWidth = 0
        MyPanel2.BackColor = Color.White
    End Sub

    Private Sub MyPanel3_MouseHover(sender As Object, e As EventArgs) Handles
MyPanel3.MouseHover
        MyPanel3.BorderColor = Color.SkyBlue
        MyPanel3.BorderWidth = 2
        MyPanel3.BackColor = Color.AliceBlue
    End Sub

    Private Sub MyPanel3_Paint(sender As Object, e As EventArgs) Handles
MyPanel3.MouseLeave
```

```
        MyPanel3.BorderColor = Color.White
        MyPanel3.BorderWidth = 0
        MyPanel3.BackColor = Color.White
    End Sub

    Private Sub MyPanel4_MouseHover(sender As Object, e As EventArgs) Handles
MyPanel4.MouseHover
        MyPanel4.BorderColor = Color.SkyBlue
        MyPanel4.BorderWidth = 2
        MyPanel4.BackColor = Color.AliceBlue
    End Sub

    Private Sub MyPanel4_MouseLeave(sender As Object, e As EventArgs) Handles
MyPanel4.MouseLeave
        MyPanel4.BorderColor = Color.White
        MyPanel4.BorderWidth = 0
        MyPanel4.BackColor = Color.White
    End Sub

    Private Sub MyPanel1_MouseClick(sender As Object, e As MouseEventArgs) Handles
MyPanel1.MouseClick
        CheckBox1.Visible = True
        Button1.Visible = True
        CheckBox2.Visible = False
        Button2.Visible = False
        CheckBox3.Visible = False
        Button3.Visible = False
        CheckBox4.Visible = False
        Button4.Visible = False
    End Sub

    Private Sub MyPanel2_MouseClick(sender As Object, e As MouseEventArgs) Handles
MyPanel2.MouseClick
        CheckBox1.Visible = False
        Button1.Visible = False
        CheckBox2.Visible = True
        Button2.Visible = True
        CheckBox3.Visible = False
        Button3.Visible = False
        CheckBox4.Visible = False
        Button4.Visible = False
    End Sub

    Private Sub MyPanel3_MouseClick(sender As Object, e As MouseEventArgs) Handles
MyPanel3.MouseClick
        CheckBox1.Visible = False
        Button1.Visible = False
        CheckBox2.Visible = False
        Button2.Visible = False
        CheckBox3.Visible = True
        Button3.Visible = True
        CheckBox4.Visible = False
        Button4.Visible = False
    End Sub

    Private Sub MyPanel4_MouseClick(sender As Object, e As MouseEventArgs) Handles
MyPanel4.MouseClick
        CheckBox1.Visible = False
        Button1.Visible = False
        CheckBox2.Visible = False
```

```
        Button2.Visible = False
        CheckBox3.Visible = False
        Button3.Visible = False
        CheckBox4.Visible = True
        Button4.Visible = True
    End Sub

    Private Sub MyPanel5_MouseClick(sender As Object, e As MouseEventArgs) Handles
MyPanel5.MouseClick
        CheckBox1.Visible = False
        Button1.Visible = False
        CheckBox2.Visible = False
        Button2.Visible = False
        CheckBox3.Visible = False
        Button3.Visible = False
        CheckBox4.Visible = False
        Button4.Visible = False

    End Sub

    Private Sub Form1_FormClosing(sender As Object, e As FormClosingEventArgs)
Handles MyBase.FormClosing

        Dim path As String =
Environment.GetFolderPath(Environment.SpecialFolder.Desktop) + "\MyTest1Group.csv"
        Dim currTime As DateTime = DateTime.Now
        Dim startMilliseconds As Long = CLng(startTime.Subtract(New DateTime(1970,
1, 1)).TotalMilliseconds)
        Dim milliseconds = CLng(currTime.Subtract(New DateTime(1970, 1,
1)).TotalMilliseconds)
        Dim ellapsedTime As Long = milliseconds - startMilliseconds
        Dim startDateString As String = startTime.ToString("dd MM yyyy")
        Dim startTimeString As String = startTime.ToString("hh:mm:ss")
        Dim endDateString As String = currTime.ToString("dd MM yyyy")
        Dim endTimeString As String = currTime.ToString("hh:mm:ss")
        Dim frirst As Integer = 1

        If System.IO.File.Exists(path) = True Then

            Dim text As String = network1 & "," _
                     & network2 & "," _
                     & network3 & "," _
                     & network4 & "," _
                     & startMilliseconds & "," _
                     & convertMsToMinSec(ellapsedTime) & "," _
                     & startDateString & "," _
                     & startTimeString & "," _
                     & endDateString & "," _
                     & endTimeString & "," _
                     & eduroamPasswordEntered & "," _
                     & eduroamLoginSuccessful & "," _
                     & eduroamLoginFailed & "," _
                     & eduroamCanceled & "," _
                     & eduroamKilled & "," _
                     & BellacostaCafeAccepted & "," _
                     & BellacostaCafeRejected & "," _
                     & BellacostaCafeKilled & "," _
                     & withPlymouthAccepted & "," _
                     & withPlymouthRejected & "," _
                     & withPlymouthKilled & "," _
```

```
                & eduroamhighspeedAccepted & "," _
                & eduroamhighspeedRejected & "," _
                & eduroamhighspeedKilled & vbNewLine

        System.IO.File.AppendAllText(path, text)
    Else

        Dim header As String =
                  "eduroam" _
                & ",BellacostaCafe" _
                & ",withPlymouth" _
                & ",eduroam highspeed" _
                & ",StartMilliseconds" _
                & ",Elapsed Time" _
                & ",Start Date" _
                & ",Start Time" _
                & ",End Date" _
                & ",End Time" _
                & ",eduroamPasswordEntered" _
                & ",eduroamLoginSuccessful  " _
                & ",eduroamLoginFailed " _
                & ",eduroamCanceled  " _
                & ",eduroamKilled  " _
                & ",BellacostaCafeAccepted " _
                & ",BellacostaCafeRejected " _
                & ",BellacostaCafeKilled " _
                & ",withPlymouthAccepted " _
                & ",withPlymouthRejected " _
                & ",withPlymouthKilled " _
                & ",eduroamhighspeedAccepted " _
                & ",eduroamhighspeedRejected " _
                & ",eduroamhighspeedKilled " & vbNewLine

        Dim FirstRec As String = network1 & "," _
                & network2 & "," _
                & network3 & "," _
                & network4 & "," _
                & startMilliseconds & "," _
                & convertMsToMinSec(ellapsedTime) & "," _
                & startDateString & "," _
                & startTimeString & "," _
                & endDateString & "," _
                & endTimeString & "," _
                & eduroamPasswordEntered & "," _
                & eduroamLoginSuccessful & "," _
                & eduroamLoginFailed & "," _
                & eduroamCanceled & "," _
                & eduroamKilled & "," _
                & BellacostaCafeAccepted & "," _
                & BellacostaCafeRejected & "," _
                & BellacostaCafeKilled & "," _
                & withPlymouthAccepted & "," _
                & withPlymouthRejected & "," _
                & withPlymouthKilled & "," _
                & eduroamhighspeedAccepted & "," _
                & eduroamhighspeedRejected & "," _
                & eduroamhighspeedKilled & vbNewLine

        System.IO.File.AppendAllText(path, header)
        System.IO.File.AppendAllText(path, FirstRec)
```

```
        End If
    End Sub

    Private Sub Form1_Load(sender As Object, e As EventArgs) Handles MyBase.Load
        startTime = DateTime.Now
    End Sub

    Private Function convertMsToMinSec(millsec As Long) As String
        Dim result As String
        result = ""
        Dim time As Double
        time = millsec
        time = time / 1000
        time = time / 60
        Dim min As Integer
        Dim sec As Double
        min = Math.Truncate(time)
        time = time - min
        time = time * 60
        sec = time
        result = min.ToString() + ":" + sec.ToString()
        convertMsToMinSec = result
    End Function


End Class


Public Class Form2

    Public Username1 As String = "Alsharief"
    Public Password1 As String = "Alsharief77"
    Private Canceled As Boolean = False
    Private Successful As Boolean = False
    Private Failed As Boolean = False
    Private PasswordEntered As Boolean = False

    Public ReadOnly Property isCanceled As Boolean
        Get
            Return Canceled
        End Get
    End Property

    Public ReadOnly Property isPasswordEnetered As Boolean
        Get
            Return PasswordEntered
        End Get
    End Property

    Public ReadOnly Property isSuccessful As Boolean
        Get
            Return Successful
        End Get
    End Property

    Public ReadOnly Property isFailed As Boolean
        Get
            Return Failed
        End Get
    End Property
    Private Sub closeWin()
```

```
        Me.Close()
    End Sub

    Private Sub Cancel_Click(sender As Object, e As EventArgs) Handles
Cancel.Click
        Canceled = True
        Me.Close()
    End Sub

    Private Sub btnLogin_Click(sender As Object, e As EventArgs) Handles
Login.Click
        If (Username1 = TextBox1.Text And Password1 = TextBox2.Text) Then
            Successful = True
            Me.Close()
        Else
            Failed = True
            MsgBox("Password or username is invalid", MsgBoxStyle.Critical)
        End If
    End Sub

    Private Sub TextBox2_keypress(ByVal sender As Object, ByVal e As
System.Windows.Forms.KeyPressEventArgs) Handles TextBox2.KeyPress

        If TextBox2.Text <> " " Then
            PasswordEntered = True
        End If

    End Sub
End Class


Public Class WiFiSecurityWarning

    Private accepted As Boolean = False
    Private rejected As Boolean = False
    Public ReadOnly Property isAccepted As Boolean
        Get
            Return accepted
        End Get
    End Property

    Public ReadOnly Property isRejected As Boolean
        Get
            Return rejected
        End Get
    End Property

    Private Sub closeWin()
        Me.Close()
    End Sub

    Private Sub btnAccept_Click(sender As Object, e As EventArgs) Handles
btnAccept.Click
        accepted = True
        closeWin()
    End Sub

    Private Sub btnReject_Click(sender As Object, e As EventArgs) Handles
btnReject.Click
        rejected = True
```

```
        closeWin()
    End Sub


End Class


Public Class FormClickRecord

    Private openTime As DateTime
    Private closeTime As DateTime
    Private network As String

    Public Sub New()
        openTime = Now
        network = ""
    End Sub

    Public Sub New(name As String)
        openTime = Now
        network = name
    End Sub

    Public Sub closeRecord()
        closeTime = Now
    End Sub

    Public Function getNetwork() As String
        getNetwork = network
    End Function

    Public Function ellapsedTime() As Double
        Dim time As Double
        time = -1
        If (Not (IsDBNull(closeTime))) Then
            time = closeTime.Ticks - openTime.Ticks
            time = time / 10000000
        End If
        ellapsedTime = time
    End Function

    Public Sub setNetwork(name As String)
        network = name
    End Sub

End Class
```

- **Third Wi-Fi interface software code.**

(*Advanced interface with security meter (Design 1)*

```
Public Class Form1

    Public network1 As Integer = 0
    Public network2 As Integer = 0
    Public network3 As Integer = 0
    Public network4 As Integer = 0

    Public startTime As DateTime
    Public Records As FormClickRecord

    Dim MyPanel1Clicked As Boolean = False
    Dim MyPanel2Clicked As Boolean = False
    Dim MyPanel3Clicked As Boolean = False
    Dim MyPanel4Clicked As Boolean = False

    Dim eduroam As Integer = 0
    Dim BellacostaCafe As Integer = 0
    Dim withPlymouth As Integer = 0
    Dim eduroamhighspeed As Integer = 0

    Public eduroamElapsedTime As Double = 0
    Public BellacostaCafeElapsedTime As Double = 0
    Public withPlymouthElapsedTime As Double = 0
    Public eduroamhighspeedElapsedTime As Double = 0


 Dim clickRecords As List(Of FormClickRecord) = New List(Of FormClickRecord)

    Private Sub Button1_Click(sender As Object, e As EventArgs) Handles
Button1.Click
        If Button1.Text = "Connect" Then
            Button1.Text = "Disconnect"
            network1 = network1 + 1
            Button2.Text = "Connect"
            Button3.Text = "Connect"
            Button4.Text = "Connect"
        Else
            Button1.Text = "Connect"
        End If
    End Sub

    Private Sub Button2_Click(sender As Object, e As EventArgs) Handles
Button2.Click
        If Button2.Text = "Connect" Then
            Button2.Text = "Disconnect"
            network2 = network2 + 1
            Button1.Text = "Connect"
            Button3.Text = "Connect"
            Button4.Text = "Connect"
        Else
            Button2.Text = "Connect"
        End If
    End Sub

    Private Sub Button3_Click(sender As Object, e As EventArgs) Handles
Button3.Click
```

```
        If Button3.Text = "Connect" Then
            Button3.Text = "Disconnect"
            network3 = network3 + 1
            Button1.Text = "Connect"
            Button2.Text = "Connect"
            Button4.Text = "Connect"
        Else
            Button3.Text = "Connect"
        End If
    End Sub

    Private Sub Button4_Click(sender As Object, e As EventArgs) Handles
Button4.Click
        If Button4.Text = "Connect" Then
            Button4.Text = "Disconnect"
            network4 = network4 + 1
            Button1.Text = "Connect"
            Button2.Text = "Connect"
            Button3.Text = "Connect"
        Else
            Button4.Text = "Connect"
        End If
    End Sub


    Public Sub LinkLabel2_LinkClicked(sender As Object, e As
LinkLabelLinkClickedEventArgs) Handles LinkLabel2.LinkClicked
        eduroam = eduroam + 1
        Dim form As Form2
        form = New Form2(Me, "eduroam")
        form.Show()
    End Sub


Private Sub LinkLabel4_LinkClicked(sender As Object, e As
LinkLabelLinkClickedEventArgs) Handles LinkLabel4.LinkClicked
        BellacostaCafe = BellacostaCafe + 1
        Dim form As Form3
        form = New Form3(Me, "BellacostaCafe")
        form.Show()
    End Sub

    Private Sub LinkLabel6_LinkClicked(sender As Object, e As
LinkLabelLinkClickedEventArgs) Handles LinkLabel6.LinkClicked
        withPlymouth = withPlymouth + 1
        Dim form As Form4
        form = New Form4(Me, "withPlymouth")
        form.Show()
    End Sub

    Private Sub LinkLabel8_LinkClicked(sender As Object, e As
LinkLabelLinkClickedEventArgs) Handles LinkLabel8.LinkClicked
        eduroamhighspeed = eduroamhighspeed + 1
        Dim form As Form5
        form = New Form5(Me, "eduroamhighspeed")
        form.Show()
    End Sub

    Private Sub MyPanel1_MouseHover(sender As Object, e As EventArgs) Handles
MyPanel1.MouseHover
        MyPanel1.BorderColor = Color.SkyBlue
```

```
        MyPanel1.BorderWidth = 2
        MyPanel1.BackColor = Color.AliceBlue
    End Sub

    Private Sub MyPanel1_MouseLeave(sender As Object, e As EventArgs) Handles
MyPanel1.MouseLeave
        MyPanel1.BorderColor = Color.White
        MyPanel1.BorderWidth = 0
        MyPanel1.BackColor = Color.White
    End Sub

    Private Sub MyPanel2_MouseHover(sender As Object, e As EventArgs) Handles
MyPanel2.MouseHover
        MyPanel2.BorderColor = Color.SkyBlue
        MyPanel2.BorderWidth = 2
        MyPanel2.BackColor = Color.AliceBlue
    End Sub

    Private Sub MyPanel2_MouseLeave(sender As Object, e As EventArgs) Handles
MyPanel2.MouseLeave
        MyPanel2.BorderColor = Color.White
        MyPanel2.BorderWidth = 0
        MyPanel2.BackColor = Color.White
    End Sub

    Private Sub MyPanel3_MouseHover(sender As Object, e As EventArgs) Handles
MyPanel3.MouseHover
        MyPanel3.BorderColor = Color.SkyBlue
        MyPanel3.BorderWidth = 2
        MyPanel3.BackColor = Color.AliceBlue
    End Sub

    Private Sub MyPanel3_MouseLeave(sender As Object, e As EventArgs) Handles
MyPanel3.MouseLeave
        MyPanel3.BorderColor = Color.White
        MyPanel3.BorderWidth = 0
        MyPanel3.BackColor = Color.White
    End Sub

    Private Sub MyPanel4_MouseHover(sender As Object, e As EventArgs) Handles
MyPanel4.MouseHover
        MyPanel4.BorderColor = Color.SkyBlue
        MyPanel4.BorderWidth = 2
        MyPanel4.BackColor = Color.AliceBlue
    End Sub

    Private Sub MyPanel4_MouseLeave(sender As Object, e As EventArgs) Handles
MyPanel4.MouseLeave
        MyPanel4.BorderColor = Color.White
        MyPanel4.BorderWidth = 0
        MyPanel4.BackColor = Color.White
    End Sub


Private Sub MyPanel1_MouseClick(sender As Object, e As MouseEventArgs) Handles
MyPanel1.MouseClick
        CheckBox1.Visible = True
        Button1.Visible = True
        CheckBox2.Visible = False
        Button2.Visible = False
        CheckBox3.Visible = False
```

```
        Button3.Visible = False
        CheckBox4.Visible = False
        Button4.Visible = False
    End Sub

    Private Sub MyPanel2_MouseClick(sender As Object, e As MouseEventArgs) Handles
MyPanel2.MouseClick
        CheckBox1.Visible = False
        Button1.Visible = False
        CheckBox2.Visible = True
        Button2.Visible = True
        CheckBox3.Visible = False
        Button3.Visible = False
        CheckBox4.Visible = False
        Button4.Visible = False
    End Sub

    Private Sub MyPanel3_MouseClick(sender As Object, e As MouseEventArgs) Handles
MyPanel3.MouseClick
        CheckBox1.Visible = False
        Button1.Visible = False
        CheckBox2.Visible = False
        Button2.Visible = False
        CheckBox3.Visible = True
        Button3.Visible = True
        CheckBox4.Visible = False
        Button4.Visible = False
    End Sub

    Private Sub MyPanel4_MouseClick(sender As Object, e As MouseEventArgs) Handles
MyPanel4.MouseClick
        CheckBox1.Visible = False
        Button1.Visible = False
        CheckBox2.Visible = False
        Button2.Visible = False
        CheckBox3.Visible = False
        Button3.Visible = False
        CheckBox4.Visible = True
        Button4.Visible = True
    End Sub

    Private Sub MyPanel5_MouseClick(sender As Object, e As MouseEventArgs) Handles
MyPanel5.MouseClick
        CheckBox1.Visible = False
        Button1.Visible = False
        CheckBox2.Visible = False
        Button2.Visible = False
        CheckBox3.Visible = False
        Button3.Visible = False
        CheckBox4.Visible = False
        Button4.Visible = False
    End Sub


Private Sub Form1_FormClosing(sender As Object, e As FormClosingEventArgs) Handles
MyBase.FormClosing
        saveData()
    End Sub

    Private Sub Form1_Load(sender As Object, e As EventArgs) Handles MyBase.Load
        startTime = DateTime.Now
```

```
        Dim colourSetter As New Framework.Controls.FiveWayColourScheme()
        SecurityLevelExcellent.ColorAlgorithm = colourSetter
        SecurityLevelFair.ColorAlgorithm = colourSetter
        SecurityLevelGood.ColorAlgorithm = colourSetter
        SecurityLevelPoor.ColorAlgorithm = colourSetter
    End Sub

    Private Function convertMsToMinSec(millsec As Long) As String
        Dim result As String
        result = ""
        Dim time As Double
        time = millsec
        time = time / 1000
        time = time / 60
        Dim min As Integer
        Dim sec As Double
        min = Math.Truncate(time)
        time = time - min
        time = time * 60
        sec = time
        result = min.ToString() + ":" + sec.ToString()
        convertMsToMinSec = result
    End Function

    Public Sub storeClickRecord_2(aRecord As FormClickRecord)
        clickRecords.Add(aRecord)
    End Sub

    Public Sub storeClickRecord_3(aRecord As FormClickRecord)
        clickRecords.Add(aRecord)
    End Sub
    Public Sub storeClickRecord_4(aRecord As FormClickRecord)
        clickRecords.Add(aRecord)
    End Sub
    Public Sub storeClickRecord_5(aRecord As FormClickRecord)
        clickRecords.Add(aRecord)
    End Sub

    Private Sub saveData()
        Dim path As String =
Environment.GetFolderPath(Environment.SpecialFolder.Desktop) + "\MyTest2Group.csv"
        Dim currTime As DateTime = DateTime.Now
        Dim startMilliseconds As Long = CLng(startTime.Subtract(New DateTime(1970,
1, 1)).TotalMilliseconds)
        Dim milliseconds = CLng(currTime.Subtract(New DateTime(1970, 1,
1)).TotalMilliseconds)
        Dim ellapsedTime As Long = milliseconds - startMilliseconds
        Dim startDateString As String = startTime.ToString("dd MM yyyy")
        Dim startTimeString As String = startTime.ToString("hh:mm:ss")
        Dim endDateString As String = currTime.ToString("dd MM yyyy")
        Dim endTimeString As String = currTime.ToString("hh:mm:ss")
        Dim frirst As Integer = 1

        If System.IO.File.Exists(path) = False Then
            Dim header As String =
                      "eduroam" _
                    & ",BellacostaCafe" _
                    & ",withPlymouth" _
                    & ",eduroam highspeed" _
                    & ",StartMilliseconds" _
```

```
                & ",Elapsed Time" _
                & ",Start Date" _
                & ",Start Time" _
                & ",End Date" _
                & ",End Time" _
                & ",eduroam Clicked" _
                & ",eduroam Elapsed Time" _
                & ",BellacostaCafe Clicked" _
                & ",BellacostaCafe Elapsed Time" _
                & ",withPlymouth Clicked" _
                & ",withPlymouth Elapsed Time" _
                & ",eduroamhighspeed Clicked" _
                & ",eduroamhighspeed Elapsed Time" & vbNewLine
        System.IO.File.AppendAllText(path, header)
    Else
        Dim header As String = "NEW SESSION STARTED" & vbNewLine
        System.IO.File.AppendAllText(path, header)
    End If
    For Each record As FormClickRecord In clickRecords

        eduroam = 0
        BellacostaCafe = 0
        withPlymouth = 0
        eduroamhighspeed = 0

        eduroamElapsedTime = 0
        BellacostaCafeElapsedTime = 0
        withPlymouthElapsedTime = 0
        eduroamhighspeedElapsedTime = 0

        Select Case record.getNetwork
            Case "eduroam"
                eduroam = 1
                eduroamElapsedTime = record.ellapsedTime
            Case "BellacostaCafe"
                BellacostaCafe = 1
                BellacostaCafeElapsedTime = record.ellapsedTime
            Case "withPlymouth"
                withPlymouth = 1
                withPlymouthElapsedTime = record.ellapsedTime
            Case "eduroamhighspeed"
                eduroamhighspeed = 1
                eduroamhighspeedElapsedTime = record.ellapsedTime
        End Select

        startTimeString = record.getOpenTime.ToString("hh:mm:ss")
        endTimeString = record.getCloseTime.ToString("hh:mm:ss")
        Dim CurrRec As String = network1 & "," _
                 & network2 & "," _
                 & network3 & "," _
                 & network4 & "," _
                 & startMilliseconds & "," _
                 & convertMsToMinSec(ellapsedTime) & "," _
                 & startDateString & "," _
                 & startTimeString & "," _
                 & endDateString & "," _
                 & endTimeString & "," _
                 & eduroam & "," _
                 & eduroamElapsedTime & "," _
                 & BellacostaCafe & "," _
```

```
                    & BellacostaCafeElapsedTime & "," _
                    & withPlymouth & "," _
                    & withPlymouthElapsedTime & "," _
                    & eduroamhighspeed & "," _
                    & eduroamhighspeedElapsedTime & vbNewLine
            System.IO.File.AppendAllText(path, CurrRec)
        Next
    End Sub

End Class


Public Class Form2

    Dim record As FormClickRecord
    Dim myOwner As Form1

    Public Sub New(aParent As Form1, networkName As String)

        InitializeComponent()
        record = New FormClickRecord
        record.setNetwork(networkName)
        myOwner = aParent

    End Sub

    Private Sub Form2_FormClosing(sender As Object, e As FormClosingEventArgs)
Handles MyBase.FormClosing
        record.closeRecord()
        myOwner.storeClickRecord_2(record)
    End Sub


End Class


Public Class Form3

    Dim record As FormClickRecord
    Dim myOwner As Form1

    Public Sub New(aParent As Form1, networkName As String)

        InitializeComponent()
        record = New FormClickRecord
        record.setNetwork(networkName)
        myOwner = aParent

    End Sub

    Private Sub Form3_FormClosing(sender As Object, e As FormClosingEventArgs)
Handles MyBase.FormClosing
        record.closeRecord()
        myOwner.storeClickRecord_3(record)
    End Sub


End Class


Public Class Form4
    Dim record As FormClickRecord
```

```
    Dim myOwner As Form1

    Public Sub New(aParent As Form1, networkName As String)

        InitializeComponent()
        record = New FormClickRecord
        record.setNetwork(networkName)
        myOwner = aParent

    End Sub

    Private Sub Form4_FormClosing(sender As Object, e As FormClosingEventArgs)
Handles MyBase.FormClosing
        record.closeRecord()
        myOwner.storeClickRecord_4(record)
    End Sub


End Class

Public Class Form5
    Dim record As FormClickRecord
    Dim myOwner As Form1

    Public Sub New(aParent As Form1, networkName As String)

        InitializeComponent()
        record = New FormClickRecord
        record.setNetwork(networkName)
        myOwner = aParent

    End Sub

    Private Sub Form5_FormClosing(sender As Object, e As FormClosingEventArgs)
Handles MyBase.FormClosing
        record.closeRecord()
        myOwner.storeClickRecord_5(record)
    End Sub
End Class


Imports System
Imports System.Collections
Imports System.IO
Imports System.Windows.Forms
Imports System.Drawing
Imports System.Drawing.Drawing2D
Public Class CustomTextBox


    Inherits TextBox

#Region " Component Designer generated code "

    Public Sub New(ByVal Container As System.ComponentModel.IContainer)
        MyClass.New()

        'Required for Windows.Forms Class Composition Designer support
        Container.Add(Me)
    End Sub
```

```
    Public Sub New()
        MyBase.New()

        'This call is required by the Component Designer.
        InitializeComponent()

        'Add any initialization after the InitializeComponent() call

    End Sub

    'Component overrides dispose to clean up the component list.
    Protected Overloads Overrides Sub Dispose(ByVal disposing As Boolean)
        If disposing Then
            If Not (components Is Nothing) Then
                components.Dispose()
            End If
        End If
        MyBase.Dispose(disposing)
    End Sub

    'Required by the Component Designer
    Private components As System.ComponentModel.IContainer

    'NOTE: The following procedure is required by the Component Designer
    'It can be modified using the Component Designer.
    'Do not modify it using the code editor.
    <System.Diagnostics.DebuggerStepThrough()> Private Sub InitializeComponent()
        components = New System.ComponentModel.Container()
    End Sub

#End Region



    Protected Overrides Sub OnTextChanged(ByVal e As System.EventArgs)
        If Not File.Exists(Me.Text) Then
            Me.ForeColor = Color.Red
        Else
            Me.ForeColor = Color.Black
        End If

        MyBase.OnTextChanged(e)
    End Sub
End Class


Public Class FormClickRecord

    Private openTime As DateTime
    Private closeTime As DateTime
    Private network As String

    Public Sub New()
        openTime = Now
        network = ""
    End Sub

    Public Sub New(name As String)
        openTime = Now
        network = name
```

```
    End Sub

    Public Sub closeRecord()
        closeTime = Now
    End Sub

    Public Function getNetwork() As String
        getNetwork = network
    End Function

    Public Function ellapsedTime() As Double
        Dim time As Double
        time = -1
        If (Not (IsDBNull(closeTime))) Then
            time = closeTime.Ticks - openTime.Ticks
            time = time / 10000000
        End If
        ellapsedTime = time
    End Function

    Public Sub setNetwork(name As String)
        network = name
    End Sub

    Public Function getOpenTime() As Date
        getOpenTime = openTime
    End Function

    Public Function getCloseTime() As Date
        getCloseTime = closeTime
    End Function

End Class


Public Class MyPanel
    Inherits System.Windows.Forms.Panel

    Public Sub New()
        Me.BorderStyle = Windows.Forms.BorderStyle.None
    End Sub

    Private bWidth As Integer
    Public Property BorderWidth() As Integer
        Get
            Return Me.bWidth
        End Get
        Set(ByVal value As Integer)
            Me.bWidth = Math.Abs(value)
            Me.Refresh()
        End Set
    End Property

    Private bColor As Color
    Public Property BorderColor() As Color
        Get
            Return Me.bColor
        End Get
        Set(ByVal value As Color)
            Me.bColor = value
            Me.Refresh()
```

```
        End Set
    End Property

    Public Overridable Sub MyPanel_Paint(ByVal sender As Object, ByVal e As
System.Windows.Forms.PaintEventArgs) Handles Me.Paint

        e.Graphics.DrawRectangle(New Pen(Me.bColor, Me.bWidth),
Me.ClientRectangle)

    End Sub
End Class


Option Explicit On
Option Strict On

Imports System.ComponentModel

Public Class TextboxCustBorder

    Inherits TextBox

    Private clrBorder As Color = Color.Black
    Private style As CustomBorderStyles = BorderStyleCustom.CustomColor
    Private blnCustomChange As Boolean

#Region "Properties and Enum"
    'the enumeration for my new property
    Enum CustomBorderStyles As Integer
        None = 0
        FixedSingle = 1
        Fixed3D = 2
        CustomColor = 3
    End Enum

    'New property. It will switch the textbox's borderstyle so it will be drawn
correctly
    <Category("Appearance"), Description("Type of border around the control")> _
    Public Property BorderStyleCustom() As CustomBorderStyles
        Get
            Return style
        End Get
        Set(ByVal value As CustomBorderStyles)
            style = value
            blnCustomChange = True
            If value = CustomBorderStyles.CustomColor Then
                Me.BorderStyle = Windows.Forms.BorderStyle.FixedSingle
            Else
                If value = CustomBorderStyles.Fixed3D Then
                    Me.BorderStyle = Windows.Forms.BorderStyle.Fixed3D
                End If
                If value = CustomBorderStyles.FixedSingle Then
                    Me.BorderStyle = Windows.Forms.BorderStyle.FixedSingle
                End If
                If value = CustomBorderStyles.None Then
                    Me.BorderStyle = Windows.Forms.BorderStyle.None
                End If
            End If
            blnCustomChange = False
        End Set
    End Property
```

```
    'The color of the border (if selected)
    <Category("Appearance"), Description("Color of the Single border if
BorderStyles is CustomColor")> _
    Public Property BorderColor() As Color
        Get
            Return clrBorder
        End Get
        Set(ByVal value As Color)
            clrBorder = value
        End Set
    End Property
#End Region

    'This is so the custom border isn't drawn when the textbox's original
borderstyle is changed
    'Note: I did it this way because I was having a few issues with overloading
the
    'textbox's original BorderStyle property
    Private Sub TextboxCustBorder_BorderStyleChanged(ByVal sender As Object, ByVal
e As System.EventArgs) Handles Me.BorderStyleChanged
        If blnCustomChange = False Then
            Dim int As Integer = CInt(Me.BorderStyle)
            Me.BorderStyleCustom = CType(int, CustomBorderStyles)
        End If
    End Sub

    'Invalidate the textbox so the border is redrawn
    Private Sub TextboxCustBorder_TextChanged(ByVal sender As Object, ByVal e As
System.EventArgs) Handles Me.TextChanged
        Me.Invalidate()
    End Sub

    Protected Overrides Sub WndProc(ByRef m As System.Windows.Forms.Message)
        MyBase.WndProc(m)

        'this is where the actually drawing occurs
        If m.Msg = 15 And Me.BorderStyleCustom = CustomBorderStyles.CustomColor
Then
            Dim g As Graphics = Me.CreateGraphics
            g.DrawRectangle(New Pen(clrBorder, 1), New Rectangle(0, 0, Me.Width -
1, Me.Height - 1))
            g.Dispose()
        End If
    End Sub


End Class


Imports PUVisLabComponents

Public Class TrafficLight
    Inherits ColourDefiner5Level

    Public Overloads Function defineColour(min As Integer, value As Integer, max
As Integer) As Color
        Dim result As Color
        result = Color.Red
        Dim range As Integer
        range = max - min
```

```
        Dim myVal As Integer
        myVal = value - min
        Dim perc As Double
        perc = myVal / range
        If perc >= 0.33D And perc < 0.66D Then
            result = Color.Orange
        ElseIf (perc > 0.66D) Then
            result = Color.Green
        End If
    End Function

End Class
```

- **Fourth Wi-Fi interface software code.**

(*Advanced interface with security meter (Design 2).*

```
Public Class Form1

    Public network1 As Integer = 0
    Public network2 As Integer = 0
    Public network3 As Integer = 0
    Public network4 As Integer = 0

    Public startTime As DateTime
    Public Records As FormClickRecord

    Dim MyPanel1Clicked As Boolean = False
    Dim MyPanel2Clicked As Boolean = False
    Dim MyPanel3Clicked As Boolean = False
    Dim MyPanel4Clicked As Boolean = False

    Dim eduroam As Integer = 0
    Dim BellacostaCafe As Integer = 0
    Dim withPlymouth As Integer = 0
    Dim eduroamhighspeed As Integer = 0

    Public eduroamElapsedTime As Double = 0
    Public BellacostaCafeElapsedTime As Double = 0
    Public withPlymouthElapsedTime As Double = 0
    Public eduroamhighspeedElapsedTime As Double = 0

    Public eduroamAccepted As Integer = 0
    Public eduroamRejected As Integer = 0
    Public eduroamKilled As Integer = 0

    Public BellacostaCafeAccepted As Integer = 0
    Public BellacostaCafeRejected As Integer = 0
    Public BellacostaCafeKilled As Integer = 0

    Public withPlymouthAccepted As Integer = 0
    Public withPlymouthRejected As Integer = 0
    Public withPlymouthKilled As Integer = 0

    Public eduroamhighspeedAccepted As Integer = 0
    Public eduroamhighspeedRejected As Integer = 0
    Public eduroamhighspeedKilled As Integer = 0

Dim clickRecords As List(Of FormClickRecord) = New List(Of FormClickRecord)

    Private Sub Button1_Click(sender As Object, e As EventArgs) Handles
Button1.Click

        Dim win As Form6 = New Form6()

        If Button1.Text = "Connect" Then
            win.ShowDialog(Me)
            If win.isAccepted Then
                Button1.Text = "Disconnect"
                network1 = network1 + 1
                eduroamAccepted = eduroamAccepted + 1
                Button2.Text = "Connect"
                Button3.Text = "Connect"
```

```
                Button4.Text = "Connect"
            ElseIf win.isRejected Then
                eduroamRejected = eduroamRejected + 1
                Button1.Text = "Connect"
            Else
                eduroamKilled = eduroamKilled + 1
                Button1.Text = "Connect"
            End If
        ElseIf Button1.Text = "Disconnect" Then
            Button1.Text = "Connect"
        End If
    End Sub

    Private Sub Button2_Click(sender As Object, e As EventArgs) Handles
Button2.Click

        Dim win As Form7 = New Form7()

        If Button2.Text = "Connect" Then
            win.ShowDialog(Me)
            If win.isAccepted Then
                Button2.Text = "Disconnect"
                network2 = network2 + 1
                BellacostaCafeAccepted = BellacostaCafeAccepted + 1
                Button1.Text = "Connect"
                Button3.Text = "Connect"
                Button4.Text = "Connect"
            ElseIf win.isRejected Then
                BellacostaCafeRejected = BellacostaCafeRejected + 1
                Button2.Text = "Connect"
            Else
                BellacostaCafeKilled = BellacostaCafeKilled + 1
                Button2.Text = "Connect"
            End If
        ElseIf Button2.Text = "Disconnect" Then
            Button2.Text = "Connect"
        End If

    End Sub

    Private Sub Button3_Click(sender As Object, e As EventArgs) Handles
Button3.Click

        Dim win As Form8 = New Form8()

        If Button3.Text = "Connect" Then
            win.ShowDialog(Me)
            If win.isAccepted Then
                Button3.Text = "Disconnect"
                network3 = network3 + 1
                withPlymouthAccepted = withPlymouthAccepted + 1
                Button1.Text = "Connect"
                Button2.Text = "Connect"
                Button4.Text = "Connect"
            ElseIf win.isRejected Then
                withPlymouthRejected = withPlymouthRejected + 1
                Button3.Text = "Connect"
            Else
                withPlymouthKilled = withPlymouthKilled + 1
                Button3.Text = "Connect"
```

```
            End If
        ElseIf Button3.Text = "Disconnect" Then
            Button3.Text = "Connect"
        End If
    End Sub

Private Sub Button4_Click(sender As Object, e As EventArgs) Handles Button4.Click

        Dim win As Form9 = New Form9()

        If Button4.Text = "Connect" Then
            win.ShowDialog(Me)
            If win.isAccepted Then
                Button4.Text = "Disconnect"
                network4 = network4 + 1
                eduroamhighspeedAccepted = eduroamhighspeedAccepted + 1
                Button1.Text = "Connect"
                Button2.Text = "Connect"
                Button3.Text = "Connect"
            ElseIf win.isRejected Then
                eduroamhighspeedRejected = eduroamhighspeedRejected + 1
                Button4.Text = "Connect"
            Else
                eduroamhighspeedKilled = eduroamhighspeedKilled + 1
                Button4.Text = "Connect"
            End If
        ElseIf Button4.Text = "Disconnect" Then
            Button4.Text = "Connect"
        End If
    End Sub


    Public Sub LinkLabel2_LinkClicked(sender As Object, e As
LinkLabelLinkClickedEventArgs) Handles LinkLabel2.LinkClicked
        eduroam = eduroam + 1
        Dim form As Form2
        form = New Form2(Me, "eduroam")
        form.Show()
    End Sub

    Private Sub LinkLabel4_LinkClicked(sender As Object, e As
LinkLabelLinkClickedEventArgs) Handles LinkLabel4.LinkClicked
        BellacostaCafe = BellacostaCafe + 1
        Dim form As Form3
        form = New Form3(Me, "BellacostaCafe")
        form.Show()
    End Sub

    Private Sub LinkLabel6_LinkClicked(sender As Object, e As
LinkLabelLinkClickedEventArgs) Handles LinkLabel6.LinkClicked
        withPlymouth = withPlymouth + 1
        Dim form As Form4
        form = New Form4(Me, "withPlymouth")
        form.Show()
    End Sub

    Private Sub LinkLabel8_LinkClicked(sender As Object, e As
LinkLabelLinkClickedEventArgs) Handles LinkLabel8.LinkClicked
        eduroamhighspeed = eduroamhighspeed + 1
        Dim form As Form5
        form = New Form5(Me, "eduroamhighspeed")
```

```
        form.Show()
    End Sub

    Private Sub MyPanel1_MouseHover(sender As Object, e As EventArgs) Handles
MyPanel1.MouseHover
        MyPanel1.BorderColor = Color.SkyBlue
        MyPanel1.BorderWidth = 2
        MyPanel1.BackColor = Color.AliceBlue
    End Sub

    Private Sub MyPanel1_MouseLeave(sender As Object, e As EventArgs) Handles
MyPanel1.MouseLeave
        MyPanel1.BorderColor = Color.White
        MyPanel1.BorderWidth = 0
        MyPanel1.BackColor = Color.White
    End Sub

    Private Sub MyPanel2_MouseHover(sender As Object, e As EventArgs) Handles
MyPanel2.MouseHover
        MyPanel2.BorderColor = Color.SkyBlue
        MyPanel2.BorderWidth = 2
        MyPanel2.BackColor = Color.AliceBlue
    End Sub

    Private Sub MyPanel2_MouseLeave(sender As Object, e As EventArgs) Handles
MyPanel2.MouseLeave
        MyPanel2.BorderColor = Color.White
        MyPanel2.BorderWidth = 0
        MyPanel2.BackColor = Color.White
    End Sub

    Private Sub MyPanel3_MouseHover(sender As Object, e As EventArgs) Handles
MyPanel3.MouseHover
        MyPanel3.BorderColor = Color.SkyBlue
        MyPanel3.BorderWidth = 2
        MyPanel3.BackColor = Color.AliceBlue
    End Sub

    Private Sub MyPanel3_MouseLeave(sender As Object, e As EventArgs) Handles
MyPanel3.MouseLeave
        MyPanel3.BorderColor = Color.White
        MyPanel3.BorderWidth = 0
        MyPanel3.BackColor = Color.White
    End Sub

Private Sub MyPanel4_MouseHover(sender As Object, e As EventArgs) Handles
MyPanel4.MouseHover
        MyPanel4.BorderColor = Color.SkyBlue
        MyPanel4.BorderWidth = 2
        MyPanel4.BackColor = Color.AliceBlue
    End Sub

    Private Sub MyPanel4_MouseLeave(sender As Object, e As EventArgs) Handles
MyPanel4.MouseLeave
        MyPanel4.BorderColor = Color.White
        MyPanel4.BorderWidth = 0
        MyPanel4.BackColor = Color.White
    End Sub

    Private Sub MyPanel1_MouseClick(sender As Object, e As MouseEventArgs) Handles
MyPanel1.MouseClick
```

```
        CheckBox1.Visible = True
        Button1.Visible = True
        CheckBox2.Visible = False
        Button2.Visible = False
        CheckBox3.Visible = False
        Button3.Visible = False
        CheckBox4.Visible = False
        Button4.Visible = False
    End Sub

    Private Sub MyPanel2_MouseClick(sender As Object, e As MouseEventArgs) Handles
MyPanel2.MouseClick
        CheckBox1.Visible = False
        Button1.Visible = False
        CheckBox2.Visible = True
        Button2.Visible = True
        CheckBox3.Visible = False
        Button3.Visible = False
        CheckBox4.Visible = False
        Button4.Visible = False
    End Sub

    Private Sub MyPanel3_MouseClick(sender As Object, e As MouseEventArgs) Handles
MyPanel3.MouseClick
        CheckBox1.Visible = False
        Button1.Visible = False
        CheckBox2.Visible = False
        Button2.Visible = False
        CheckBox3.Visible = True
        Button3.Visible = True
        CheckBox4.Visible = False
        Button4.Visible = False
    End Sub

    Private Sub MyPanel4_MouseClick(sender As Object, e As MouseEventArgs) Handles
MyPanel4.MouseClick
        CheckBox1.Visible = False
        Button1.Visible = False
        CheckBox2.Visible = False
        Button2.Visible = False
        CheckBox3.Visible = False
        Button3.Visible = False
        CheckBox4.Visible = True
        Button4.Visible = True
    End Sub

    Private Sub MyPanel5_MouseClick(sender As Object, e As MouseEventArgs) Handles
MyPanel5.MouseClick
        CheckBox1.Visible = False
        Button1.Visible = False
        CheckBox2.Visible = False
        Button2.Visible = False
        CheckBox3.Visible = False
        Button3.Visible = False
        CheckBox4.Visible = False
        Button4.Visible = False
    End Sub
```

```
    Private Sub Form1_FormClosing(sender As Object, e As FormClosingEventArgs)
Handles MyBase.FormClosing
        saveData()
    End Sub

    Private Sub Form1_Load(sender As Object, e As EventArgs) Handles MyBase.Load
        startTime = DateTime.Now
        Dim colourSetter As New Framework.Controls.FiveWayColourScheme()
        SecurityLevelExcellent.ColorAlgorithm = colourSetter
        SecurityLevelFair.ColorAlgorithm = colourSetter
        SecurityLevelGood.ColorAlgorithm = colourSetter
        SecurityLevelPoor.ColorAlgorithm = colourSetter
    End Sub

    Private Function convertMsToMinSec(millsec As Long) As String
        Dim result As String
        result = ""
        Dim time As Double
        time = millsec
        time = time / 1000
        time = time / 60
        Dim min As Integer
        Dim sec As Double
        min = Math.Truncate(time)
        time = time - min
        time = time * 60
        sec = time
        result = min.ToString() + ":" + sec.ToString()
        convertMsToMinSec = result
    End Function

    Public Sub storeClickRecord_2(aRecord As FormClickRecord)
        clickRecords.Add(aRecord)
    End Sub

    Public Sub storeClickRecord_3(aRecord As FormClickRecord)
        clickRecords.Add(aRecord)
    End Sub
    Public Sub storeClickRecord_4(aRecord As FormClickRecord)
        clickRecords.Add(aRecord)
    End Sub
    Public Sub storeClickRecord_5(aRecord As FormClickRecord)
        clickRecords.Add(aRecord)
    End Sub

    Private Sub saveData()
        Dim path As String =
Environment.GetFolderPath(Environment.SpecialFolder.Desktop) + "\MyTest3Group.csv"
        Dim currTime As DateTime = DateTime.Now
        Dim startMilliseconds As Long = CLng(startTime.Subtract(New DateTime(1970,
1, 1)).TotalMilliseconds)
        Dim milliseconds = CLng(currTime.Subtract(New DateTime(1970, 1,
1)).TotalMilliseconds)
        Dim ellapsedTime As Long = milliseconds - startMilliseconds
        Dim startDateString As String = startTime.ToString("dd MM yyyy")
        Dim startTimeString As String = startTime.ToString("hh:mm:ss")
        Dim endDateString As String = currTime.ToString("dd MM yyyy")
        Dim endTimeString As String = currTime.ToString("hh:mm:ss")
        Dim frirst As Integer = 1
```

```
If System.IO.File.Exists(path) = False Then
    Dim header As String =
              "eduroam" _
            & ",BellacostaCafe" _
            & ",withPlymouth" _
            & ",eduroam highspeed" _
            & ",StartMilliseconds" _
            & ",Elapsed Time" _
            & ",Start Date" _
            & ",Start Time" _
            & ",End Date" _
            & ",End Time" _
            & ",eduroamClicked" _
            & ",eduroam Elapsed Time" _
            & ",eduroamAccepted " _
            & ",eduroamRejected " _
            & ",eduroamKilled " _
            & ",BellacostaCafe Clicked" _
            & ",BellacostaCafe Elapsed Time" _
            & ",BellacostaCafeAccepted " _
            & ",BellacostaCafeRejected " _
            & ",BellacostaCafeKilled " _
            & ",withPlymouth Clicked" _
            & ",withPlymouth Elapsed Time" _
            & ",withPlymouthAccepted " _
            & ",withPlymouthRejected " _
            & ",withPlymouthKilled " _
            & ",eduroamhighspeed Clicked" _
            & ",eduroamhighspeed Elapsed Time" _
            & ",eduroamhighspeedAccepted " _
            & ",eduroamhighspeedRejected " _
            & ",eduroamhighspeedKilled " & vbNewLine
    System.IO.File.AppendAllText(path, header)
Else
    Dim header As String = "NEW SESSION STARTED" & vbNewLine
    System.IO.File.AppendAllText(path, header)
End If
For Each record As FormClickRecord In clickRecords

    eduroam = 0
    BellacostaCafe = 0
    withPlymouth = 0
    eduroamhighspeed = 0

    eduroamElapsedTime = 0
    BellacostaCafeElapsedTime = 0
    withPlymouthElapsedTime = 0
    eduroamhighspeedElapsedTime = 0

    Select Case record.getNetwork
        Case "eduroam"
            eduroam = 1
            eduroamElapsedTime = record.ellapsedTime
        Case "BellacostaCafe"
            BellacostaCafe = 1
            BellacostaCafeElapsedTime = record.ellapsedTime
        Case "withPlymouth"
            withPlymouth = 1
            withPlymouthElapsedTime = record.ellapsedTime
        Case "eduroamhighspeed"
```

```
                eduroamhighspeed = 1
                eduroamhighspeedElapsedTime = record.ellapsedTime
            End Select

            startTimeString = record.getOpenTime.ToString("hh:mm:ss")
            endTimeString = record.getCloseTime.ToString("hh:mm:ss")
            Dim CurrRec As String = network1 & "," _
                     & network2 & "," _
                     & network3 & "," _
                     & network4 & "," _
                     & startMilliseconds & "," _
                     & convertMsToMinSec(ellapsedTime) & "," _
                     & startDateString & "," _
                     & startTimeString & "," _
                     & endDateString & "," _
                     & endTimeString & "," _
                     & eduroam & "," _
                     & eduroamElapsedTime & "," _
                     & eduroamAccepted & "," _
                     & eduroamRejected & "," _
                     & eduroamKilled & "," _
                     & BellacostaCafe & "," _
                     & BellacostaCafeElapsedTime & "," _
                     & BellacostaCafeAccepted & "," _
                     & BellacostaCafeRejected & "," _
                     & BellacostaCafeKilled & "," _
                     & withPlymouth & "," _
                     & withPlymouthElapsedTime & "," _
                     & withPlymouthAccepted & "," _
                     & withPlymouthRejected & "," _
                     & withPlymouthKilled & "," _
                     & eduroamhighspeed & "," _
                     & eduroamhighspeedElapsedTime & "," _
                     & eduroamhighspeedAccepted & "," _
                     & eduroamhighspeedRejected & "," _
                     & eduroamhighspeedKilled & vbNewLine

            System.IO.File.AppendAllText(path, CurrRec)
        Next
    End Sub

End Class


Public Class Form2

    Dim record As FormClickRecord
    Dim myOwner As Form1

    Public Sub New(aParent As Form1, networkName As String)

        InitializeComponent()
        record = New FormClickRecord
        record.setNetwork(networkName)
        myOwner = aParent

    End Sub

    Private Sub Form2_FormClosing(sender As Object, e As FormClosingEventArgs)
Handles MyBase.FormClosing
```

```
        record.closeRecord()
        myOwner.storeClickRecord_2(record)
    End Sub


End Class

Public Class Form3

    Dim record As FormClickRecord
    Dim myOwner As Form1

    Public Sub New(aParent As Form1, networkName As String)

        InitializeComponent()
        record = New FormClickRecord
        record.setNetwork(networkName)
        myOwner = aParent

    End Sub

    Private Sub Form3_FormClosing(sender As Object, e As FormClosingEventArgs)
Handles MyBase.FormClosing
        record.closeRecord()
        myOwner.storeClickRecord_3(record)
    End Sub

End Class

Public Class Form4
    Dim record As FormClickRecord
    Dim myOwner As Form1

    Public Sub New(aParent As Form1, networkName As String)

        InitializeComponent()
        record = New FormClickRecord
        record.setNetwork(networkName)
        myOwner = aParent

    End Sub

    Private Sub Form4_FormClosing(sender As Object, e As FormClosingEventArgs)
Handles MyBase.FormClosing
        record.closeRecord()
        myOwner.storeClickRecord_4(record)
    End Sub


End Class


Public Class Form5
    Dim record As FormClickRecord
    Dim myOwner As Form1

    Public Sub New(aParent As Form1, networkName As String)


        InitializeComponent()
        record = New FormClickRecord
```

```
        record.setNetwork(networkName)
        myOwner = aParent

    End Sub

    Private Sub Form5_FormClosing(sender As Object, e As FormClosingEventArgs)
Handles MyBase.FormClosing
        record.closeRecord()
        myOwner.storeClickRecord_5(record)
    End Sub
End Class


Public Class Form6

    Private accepted As Boolean = False
    Private rejected As Boolean = False
    Public ReadOnly Property isAccepted As Boolean
        Get
            Return accepted
        End Get
    End Property

    Public ReadOnly Property isRejected As Boolean
        Get
            Return rejected
        End Get
    End Property

    Private Sub closeWin()
        Me.Close()
    End Sub

    Private Sub btnAccept_Click(sender As Object, e As EventArgs) Handles
btnAccept.Click
        accepted = True
        closeWin()
    End Sub

    Private Sub btnReject_Click(sender As Object, e As EventArgs) Handles
btnReject.Click
        rejected = True
        closeWin()
    End Sub


End Class

Public Class Form7

    Private accepted As Boolean = False
    Private rejected As Boolean = False
    Public ReadOnly Property isAccepted As Boolean
        Get
            Return accepted
        End Get
    End Property

    Public ReadOnly Property isRejected As Boolean
        Get
```

```
            Return rejected
        End Get
    End Property

    Private Sub closeWin()
        Me.Close()
    End Sub

    Private Sub btnAccept_Click(sender As Object, e As EventArgs) Handles
btnAccept.Click
        accepted = True
        closeWin()
    End Sub

    Private Sub btnReject_Click(sender As Object, e As EventArgs) Handles
btnReject.Click
        rejected = True
        closeWin()
    End Sub

End Class


Public Class Form8

    Private accepted As Boolean = False
    Private rejected As Boolean = False
    Public ReadOnly Property isAccepted As Boolean
        Get
            Return accepted
        End Get
    End Property

    Public ReadOnly Property isRejected As Boolean
        Get
            Return rejected
        End Get
    End Property

    Private Sub closeWin()
        Me.Close()
    End Sub

    Private Sub btnAccept_Click(sender As Object, e As EventArgs) Handles
btnAccept.Click
        accepted = True
        closeWin()
    End Sub

    Private Sub btnReject_Click(sender As Object, e As EventArgs) Handles
btnReject.Click
        rejected = True
        closeWin()
    End Sub

End Class


Public Class Form9
```

```
    Private accepted As Boolean = False
    Private rejected As Boolean = False
    Public ReadOnly Property isAccepted As Boolean
        Get
            Return accepted
        End Get
    End Property

    Public ReadOnly Property isRejected As Boolean
        Get
            Return rejected
        End Get
    End Property

    Private Sub closeWin()
        Me.Close()
    End Sub

    Private Sub btnAccept_Click(sender As Object, e As EventArgs) Handles
btnAccept.Click
        accepted = True
        closeWin()
    End Sub

    Private Sub btnReject_Click(sender As Object, e As EventArgs) Handles
btnReject.Click
        rejected = True
        closeWin()
    End Sub


End Class
```

```
Imports System
Imports System.Collections
Imports System.IO
Imports System.Windows.Forms
Imports System.Drawing
Imports System.Drawing.Drawing2D
Public Class CustomTextBox


    Inherits TextBox

#Region " Component Designer generated code "

    Public Sub New(ByVal Container As System.ComponentModel.IContainer)
        MyClass.New()

        'Required for Windows.Forms Class Composition Designer support
        Container.Add(Me)
    End Sub

    Public Sub New()
        MyBase.New()

        'This call is required by the Component Designer.
        InitializeComponent()

        'Add any initialization after the InitializeComponent() call
```

```
    End Sub

    'Component overrides dispose to clean up the component list.
    Protected Overloads Overrides Sub Dispose(ByVal disposing As Boolean)
        If disposing Then
            If Not (components Is Nothing) Then
                components.Dispose()
            End If
        End If
        MyBase.Dispose(disposing)
    End Sub

    'Required by the Component Designer
    Private components As System.ComponentModel.IContainer

    'NOTE: The following procedure is required by the Component Designer
    'It can be modified using the Component Designer.
    'Do not modify it using the code editor.
    <System.Diagnostics.DebuggerStepThrough()> Private Sub InitializeComponent()
        components = New System.ComponentModel.Container()
    End Sub

#End Region



    Protected Overrides Sub OnTextChanged(ByVal e As System.EventArgs)
        If Not File.Exists(Me.Text) Then
            Me.ForeColor = Color.Red
        Else
            Me.ForeColor = Color.Black
        End If

        MyBase.OnTextChanged(e)
    End Sub
End Class


Public Class FormClickRecord

    Private openTime As DateTime
    Private closeTime As DateTime
    Private network As String

    Public Sub New()
        openTime = Now
        network = ""
    End Sub

    Public Sub New(name As String)
        openTime = Now
        network = name
    End Sub

    Public Sub closeRecord()
        closeTime = Now
    End Sub

    Public Function getNetwork() As String
        getNetwork = network
```

```
    End Function

    Public Function ellapsedTime() As Double
        Dim time As Double
        time = -1
        If (Not (IsDBNull(closeTime))) Then
            time = closeTime.Ticks - openTime.Ticks
            time = time / 10000000
        End If
        ellapsedTime = time
    End Function

    Public Sub setNetwork(name As String)
        network = name
    End Sub

    Public Function getOpenTime() As Date
        getOpenTime = openTime
    End Function

    Public Function getCloseTime() As Date
        getCloseTime = closeTime
    End Function

End Class


Public Class MyPanel
    Inherits System.Windows.Forms.Panel

    Public Sub New()
        Me.BorderStyle = Windows.Forms.BorderStyle.None
    End Sub

    Private bWidth As Integer
    Public Property BorderWidth() As Integer
        Get
            Return Me.bWidth
        End Get
        Set(ByVal value As Integer)
            Me.bWidth = Math.Abs(value)
            Me.Refresh()
        End Set
    End Property

    Private bColor As Color
    Public Property BorderColor() As Color
        Get
            Return Me.bColor
        End Get
        Set(ByVal value As Color)
            Me.bColor = value
            Me.Refresh()
        End Set
    End Property

    Public Overridable Sub MyPanel_Paint(ByVal sender As Object, ByVal e As
System.Windows.Forms.PaintEventArgs) Handles Me.Paint
```

```
        e.Graphics.DrawRectangle(New Pen(Me.bColor, Me.bWidth),
Me.ClientRectangle)

    End Sub
End Class


Option Explicit On
Option Strict On

Imports System.ComponentModel

Public Class TextboxCustBorder

    Inherits TextBox

    Private clrBorder As Color = Color.Black
    Private style As CustomBorderStyles = BorderStyleCustom.CustomColor
    Private blnCustomChange As Boolean

#Region "Properties and Enum"
    'the enumeration for my new property
    Enum CustomBorderStyles As Integer
        None = 0
        FixedSingle = 1
        Fixed3D = 2
        CustomColor = 3
    End Enum

    'New property. It will switch the textbox's borderstyle so it will be drawn
correctly
    <Category("Appearance"), Description("Type of border around the control")> _
    Public Property BorderStyleCustom() As CustomBorderStyles
        Get
            Return style
        End Get
        Set(ByVal value As CustomBorderStyles)
            style = value
            blnCustomChange = True
            If value = CustomBorderStyles.CustomColor Then
                Me.BorderStyle = Windows.Forms.BorderStyle.FixedSingle
            Else
                If value = CustomBorderStyles.Fixed3D Then
                    Me.BorderStyle = Windows.Forms.BorderStyle.Fixed3D
                End If
                If value = CustomBorderStyles.FixedSingle Then
                    Me.BorderStyle = Windows.Forms.BorderStyle.FixedSingle
                End If
                If value = CustomBorderStyles.None Then
                    Me.BorderStyle = Windows.Forms.BorderStyle.None
                End If
            End If
            blnCustomChange = False
        End Set
    End Property

    'The color of the border (if selected)
    <Category("Appearance"), Description("Color of the Single border if
BorderStyles is CustomColor")> _
    Public Property BorderColor() As Color
```

```
        Get
            Return clrBorder
        End Get
        Set(ByVal value As Color)
            clrBorder = value
        End Set
    End Property
#End Region

    'This is so the custom border isn't drawn when the textbox's original
borderstyle is changed
    'Note: I did it this way because I was having a few issues with overloading
the
    'textbox's original BorderStyle property
    Private Sub TextboxCustBorder_BorderStyleChanged(ByVal sender As Object, ByVal
e As System.EventArgs) Handles Me.BorderStyleChanged
        If blnCustomChange = False Then
            Dim int As Integer = CInt(Me.BorderStyle)
            Me.BorderStyleCustom = CType(int, CustomBorderStyles)
        End If
    End Sub

    'Invalidate the textbox so the border is redrawn
    Private Sub TextboxCustBorder_TextChanged(ByVal sender As Object, ByVal e As
System.EventArgs) Handles Me.TextChanged
        Me.Invalidate()
    End Sub

    Protected Overrides Sub WndProc(ByRef m As System.Windows.Forms.Message)
        MyBase.WndProc(m)

        'this is where the actually drawing occurs
        If m.Msg = 15 And Me.BorderStyleCustom = CustomBorderStyles.CustomColor
Then
            Dim g As Graphics = Me.CreateGraphics
            g.DrawRectangle(New Pen(clrBorder, 1), New Rectangle(0, 0, Me.Width -
1, Me.Height - 1))
            g.Dispose()
        End If
    End Sub


End Class

Imports PUVisLabComponents

Public Class TrafficLight
    Inherits ColourDefiner5Level

    Public Overloads Function defineColour(min As Integer, value As Integer, max
As Integer) As Color
        Dim result As Color
        result = Color.Red
        Dim range As Integer
        range = max - min
        Dim myVal As Integer
        myVal = value - min
        Dim perc As Double
        perc = myVal / range
        If perc >= 0.33D And perc < 0.66D Then
            result = Color.Orange
```

```
        ElseIf (perc > 0.66D) Then
            result = Color.Green
        End If
    End Function


End Class
```

Appendix E - Improved interfaces for MS Outlook for spotting phishing emails (software code)

Requirement: To run the code and for the best experience, use Microsoft Visual Studio 2015 or later version.

- **First interface software code.**

Proposed interface design for the warning message when a phishing email is detected.

```
Public Class Form1

    Dim form As Form2
    Public Sub Form1()
        Panel17.BorderStyle = BorderStyle.None
    End Sub
    Private Sub LinkLabel1_LinkClicked_1(sender As Object, e As
LinkLabelLinkClickedEventArgs) Handles LinkLabel1.LinkClicked
        form = New Form2
        form.Show()
    End Sub


    Private Sub Panel17_MouseHover(sender As Object, e As EventArgs) Handles
Panel17.MouseHover
        Panel17.BackColor = Color.LightGray
    End Sub

    Private Sub Panel17_MouseLeave(sender As Object, e As EventArgs) Handles
Panel17.MouseLeave
        Panel17.BackColor = Color.Empty
    End Sub

    Private Sub Panel18_MouseHover(sender As Object, e As EventArgs) Handles
Panel18.MouseHover
        Panel18.BackColor = Color.LightGray
    End Sub

    Private Sub Panel18_MouseLeave(sender As Object, e As EventArgs) Handles
Panel18.MouseLeave
        Panel18.BackColor = Color.Empty
    End Sub

    Private Sub Panel24_MouseHover(sender As Object, e As EventArgs) Handles
Panel24.MouseHover
        Panel24.BackColor = Color.LightGray
    End Sub

    Private Sub Panel24_MouseLeave(sender As Object, e As EventArgs) Handles
Panel24.MouseLeave
        Panel24.BackColor = Color.Empty
    End Sub

    Private Sub Panel25_MouseHover(sender As Object, e As EventArgs) Handles
Panel25.MouseHover
```

```
        Panel25.BackColor = Color.LightGray
    End Sub

    Private Sub Panel25_MouseLeave(sender As Object, e As EventArgs) Handles
Panel25.MouseLeave
        Panel25.BackColor = Color.Empty
    End Sub

    Private Sub Panel26_MouseHover(sender As Object, e As EventArgs) Handles
Panel26.MouseHover
        Panel26.BackColor = Color.LightGray
    End Sub

    Private Sub Panel26_MouseLeave(sender As Object, e As EventArgs) Handles
Panel26.MouseLeave
        Panel26.BackColor = Color.Empty
    End Sub

    Private Sub Panel20_MouseHover(sender As Object, e As EventArgs) Handles
Panel20.MouseHover
        Panel20.BackColor = Color.LightGray
    End Sub

    Private Sub Panel20_MouseLeave(sender As Object, e As EventArgs) Handles
Panel20.MouseLeave
        Panel20.BackColor = Color.Empty
    End Sub

    Private Sub Panel28_MouseHover(sender As Object, e As EventArgs) Handles
Panel28.MouseHover
        Panel28.BackColor = Color.LightGray
    End Sub

    Private Sub Panel28_MouseLeave(sender As Object, e As EventArgs) Handles
Panel28.MouseLeave
        Panel28.BackColor = Color.Empty
    End Sub

    Private Sub Label15_MouseHover(sender As Object, e As EventArgs) Handles
Label15.MouseHover
        Label15.BackColor = Color.LightGray
        Panel17.BackColor = Color.LightGray
    End Sub

    Private Sub Label15_MouseLeave(sender As Object, e As EventArgs) Handles
Label15.MouseLeave
        Label15.BackColor = Color.Empty
        Panel17.BackColor = Color.Empty
    End Sub

    Private Sub PictureBox6_MouseHover(sender As Object, e As EventArgs) Handles
PictureBox6.MouseHover
        PictureBox6.BackColor = Color.LightGray
        Label15.BackColor = Color.LightGray
        Panel17.BackColor = Color.LightGray
    End Sub

    Private Sub PictureBox6_MouseLeave(sender As Object, e As EventArgs) Handles
PictureBox6.MouseLeave
        PictureBox6.BackColor = Color.LightGray
```

```
        Label15.BackColor = Color.LightGray
        Panel17.BackColor = Color.LightGray
    End Sub


    Private Sub Label16_MouseHover(sender As Object, e As EventArgs) Handles
Label16.MouseHover
        Label16.BackColor = Color.LightGray
        Panel18.BackColor = Color.LightGray
    End Sub

    Private Sub Label16_MouseLeave(sender As Object, e As EventArgs) Handles
Label16.MouseLeave
        Label16.BackColor = Color.Empty
        Panel18.BackColor = Color.Empty
    End Sub

    Private Sub Label22_MouseHover(sender As Object, e As EventArgs) Handles
Label22.MouseHover
        Label22.BackColor = Color.LightGray
        Panel24.BackColor = Color.LightGray
    End Sub

    Private Sub Label22_MouseLeave(sender As Object, e As EventArgs) Handles
Label22.MouseLeave
        Label22.BackColor = Color.Empty
        Panel24.BackColor = Color.Empty
    End Sub

    Private Sub Label23_MouseHover(sender As Object, e As EventArgs) Handles
Label23.MouseHover
        Label23.BackColor = Color.LightGray
        Panel25.BackColor = Color.LightGray
    End Sub

    Private Sub Label23_MouseLeave(sender As Object, e As EventArgs) Handles
Label23.MouseLeave
        Label23.BackColor = Color.Empty
        Panel25.BackColor = Color.Empty
    End Sub

    Private Sub Label24_MouseHover(sender As Object, e As EventArgs) Handles
Label24.MouseHover
        Label24.BackColor = Color.LightGray
        Panel26.BackColor = Color.LightGray
    End Sub

    Private Sub Label24_MouseLeave(sender As Object, e As EventArgs) Handles
Label24.MouseLeave
        Label24.BackColor = Color.Empty
        Panel26.BackColor = Color.Empty
    End Sub

    Private Sub Label18_MouseHover(sender As Object, e As EventArgs) Handles
Label18.MouseHover
        Label18.BackColor = Color.LightGray
        Panel20.BackColor = Color.LightGray
    End Sub
```

```
    Private Sub Label18_MouseLeave(sender As Object, e As EventArgs) Handles
Label18.MouseLeave
        Label18.BackColor = Color.Empty
        Panel20.BackColor = Color.Empty
    End Sub


    Private Sub Label26_MouseHover(sender As Object, e As EventArgs) Handles
Label26.MouseHover
        Label26.BackColor = Color.LightGray
        Panel28.BackColor = Color.LightGray
    End Sub

    Private Sub Label26_MouseLeave(sender As Object, e As EventArgs) Handles
Label26.MouseLeave
        Label26.BackColor = Color.Empty
        Panel28.BackColor = Color.Empty
    End Sub

    Private Sub Panel22_MouseHover(sender As Object, e As EventArgs) Handles
Panel22.MouseHover
        Panel22.BackColor = Color.LightGray
    End Sub
    Private Sub Panel22_MouseLeave(sender As Object, e As EventArgs) Handles
Panel22.MouseLeave
        Panel22.BackColor = Color.Empty
    End Sub

    Private Sub PictureBox18_MouseHover(sender As Object, e As EventArgs) Handles
PictureBox18.MouseHover
        PictureBox18.BackColor = Color.LightGray
        Panel22.BackColor = Color.LightGray
    End Sub

    Private Sub PictureBox18_MouseLeave(sender As Object, e As EventArgs) Handles
PictureBox18.MouseLeave
        PictureBox18.BackColor = Color.LightGray
        Panel22.BackColor = Color.LightGray
    End Sub
    Private Sub Panel27_MouseHover(sender As Object, e As EventArgs) Handles
Panel27.MouseHover
        Panel27.BackColor = Color.LightGray
    End Sub
    Private Sub Panel27_MouseLeave(sender As Object, e As EventArgs) Handles
Panel27.MouseLeave
        Panel27.BackColor = Color.Empty
    End Sub

    Private Sub PictureBox17_MouseHover(sender As Object, e As EventArgs) Handles
PictureBox17.MouseHover
        PictureBox17.BackColor = Color.LightGray
        Panel27.BackColor = Color.LightGray
    End Sub

    Private Sub PictureBox17_MouseLeave(sender As Object, e As EventArgs) Handles
PictureBox17.MouseLeave
        PictureBox17.BackColor = Color.LightGray
        Panel27.BackColor = Color.LightGray
    End Sub
```

```
    Private Sub Panel23_MouseHover(sender As Object, e As EventArgs) Handles
Panel23.MouseHover
        Panel23.BackColor = Color.LightGray
    End Sub
    Private Sub Panel23_MouseLeave(sender As Object, e As EventArgs) Handles
Panel23.MouseLeave
        Panel23.BackColor = Color.Empty
    End Sub

    Private Sub PictureBox20_MouseHover(sender As Object, e As EventArgs) Handles
PictureBox20.MouseHover
        PictureBox20.BackColor = Color.LightGray
        Panel23.BackColor = Color.LightGray
    End Sub

    Private Sub PictureBox20_MouseLeave(sender As Object, e As EventArgs) Handles
PictureBox20.MouseLeave
        PictureBox20.BackColor = Color.LightGray
        Panel23.BackColor = Color.LightGray
    End Sub

    Private Sub Panel35_MouseHover(sender As Object, e As EventArgs) Handles
Panel35.MouseHover
        Panel35.BackColor = Color.DarkBlue
    End Sub

    Private Sub Panel35_MouseLeave(sender As Object, e As EventArgs) Handles
Panel35.MouseLeave
        Panel35.BackColor = Color.SteelBlue
    End Sub

    Private Sub Label45_MouseHover(sender As Object, e As EventArgs) Handles
Label45.MouseHover
        Label45.BackColor = Color.MidnightBlue
        Panel35.BackColor = Color.MidnightBlue
    End Sub

    Private Sub Label45_MouseLeave(sender As Object, e As EventArgs) Handles
Label45.MouseLeave
        Label45.BackColor = Color.SteelBlue
        Panel35.BackColor = Color.SteelBlue
    End Sub


End Class


Public Class Form2
    Private Sub LinkLabel3_LinkClicked(sender As Object, e As
LinkLabelLinkClickedEventArgs) Handles LinkLabel3.LinkClicked
        LinkLabel3.LinkBehavior = System.Windows.Forms.LinkBehavior.NeverUnderline
        Process.Start("https://support.microsoft.com/en-ph/help/4033787/windows-
protect-yourself-from-phishing")
    End Sub

End Class
```

- Second interface software code.

Proposed interface design for the warning message when a suspected phishing email is detected.

```
Public Class Form1

    Dim form As Form2
    Public Sub Form1()
        Panel17.BorderStyle = BorderStyle.None
    End Sub
    Private Sub LinkLabel1_LinkClicked_1(sender As Object, e As
LinkLabelLinkClickedEventArgs) Handles LinkLabel1.LinkClicked
        form = New Form2
        form.Show()
    End Sub


    Private Sub Panel17_MouseHover(sender As Object, e As EventArgs) Handles
Panel17.MouseHover
        Panel17.BackColor = Color.LightGray
    End Sub

    Private Sub Panel17_MouseLeave(sender As Object, e As EventArgs) Handles
Panel17.MouseLeave
        Panel17.BackColor = Color.Empty
    End Sub

    Private Sub Panel18_MouseHover(sender As Object, e As EventArgs) Handles
Panel18.MouseHover
        Panel18.BackColor = Color.LightGray
    End Sub

    Private Sub Panel18_MouseLeave(sender As Object, e As EventArgs) Handles
Panel18.MouseLeave
        Panel18.BackColor = Color.Empty
    End Sub


    Private Sub Panel24_MouseHover(sender As Object, e As EventArgs) Handles
Panel24.MouseHover
        Panel24.BackColor = Color.LightGray
    End Sub

    Private Sub Panel24_MouseLeave(sender As Object, e As EventArgs) Handles
Panel24.MouseLeave
        Panel24.BackColor = Color.Empty
    End Sub

    Private Sub Panel25_MouseHover(sender As Object, e As EventArgs) Handles
Panel25.MouseHover
        Panel25.BackColor = Color.LightGray
    End Sub

    Private Sub Panel25_MouseLeave(sender As Object, e As EventArgs) Handles
Panel25.MouseLeave
        Panel25.BackColor = Color.Empty
    End Sub
```

```
    Private Sub Panel26_MouseHover(sender As Object, e As EventArgs) Handles
Panel26.MouseHover
        Panel26.BackColor = Color.LightGray
    End Sub

    Private Sub Panel26_MouseLeave(sender As Object, e As EventArgs) Handles
Panel26.MouseLeave
        Panel26.BackColor = Color.Empty
    End Sub

    Private Sub Panel20_MouseHover(sender As Object, e As EventArgs) Handles
Panel20.MouseHover
        Panel20.BackColor = Color.LightGray
    End Sub

    Private Sub Panel20_MouseLeave(sender As Object, e As EventArgs) Handles
Panel20.MouseLeave
        Panel20.BackColor = Color.Empty
    End Sub

    Private Sub Panel28_MouseHover(sender As Object, e As EventArgs) Handles
Panel28.MouseHover
        Panel28.BackColor = Color.LightGray
    End Sub

    Private Sub Panel28_MouseLeave(sender As Object, e As EventArgs) Handles
Panel28.MouseLeave
        Panel28.BackColor = Color.Empty
    End Sub

    Private Sub Label15_MouseHover(sender As Object, e As EventArgs) Handles
Label15.MouseHover
        Label15.BackColor = Color.LightGray
        Panel17.BackColor = Color.LightGray
    End Sub

    Private Sub Label15_MouseLeave(sender As Object, e As EventArgs) Handles
Label15.MouseLeave
        Label15.BackColor = Color.Empty
        Panel17.BackColor = Color.Empty
    End Sub

    Private Sub PictureBox6_MouseHover(sender As Object, e As EventArgs) Handles
PictureBox6.MouseHover
        PictureBox6.BackColor = Color.LightGray
        Label15.BackColor = Color.LightGray
        Panel17.BackColor = Color.LightGray
    End Sub

    Private Sub PictureBox6_MouseLeave(sender As Object, e As EventArgs) Handles
PictureBox6.MouseLeave
        PictureBox6.BackColor = Color.LightGray
        Label15.BackColor = Color.LightGray
        Panel17.BackColor = Color.LightGray
    End Sub


    Private Sub Label16_MouseHover(sender As Object, e As EventArgs) Handles
Label16.MouseHover
        Label16.BackColor = Color.LightGray
```

```
        Panel18.BackColor = Color.LightGray
    End Sub

    Private Sub Label16_MouseLeave(sender As Object, e As EventArgs) Handles
Label16.MouseLeave
        Label16.BackColor = Color.Empty
        Panel18.BackColor = Color.Empty
    End Sub

    Private Sub Label22_MouseHover(sender As Object, e As EventArgs) Handles
Label22.MouseHover
        Label22.BackColor = Color.LightGray
        Panel24.BackColor = Color.LightGray
    End Sub

    Private Sub Label22_MouseLeave(sender As Object, e As EventArgs) Handles
Label22.MouseLeave
        Label22.BackColor = Color.Empty
        Panel24.BackColor = Color.Empty
    End Sub

    Private Sub Label23_MouseHover(sender As Object, e As EventArgs) Handles
Label23.MouseHover
        Label23.BackColor = Color.LightGray
        Panel25.BackColor = Color.LightGray
    End Sub

    Private Sub Label23_MouseLeave(sender As Object, e As EventArgs) Handles
Label23.MouseLeave
        Label23.BackColor = Color.Empty
        Panel25.BackColor = Color.Empty
    End Sub

    Private Sub Label24_MouseHover(sender As Object, e As EventArgs) Handles
Label24.MouseHover
        Label24.BackColor = Color.LightGray
        Panel26.BackColor = Color.LightGray
    End Sub

    Private Sub Label24_MouseLeave(sender As Object, e As EventArgs) Handles
Label24.MouseLeave
        Label24.BackColor = Color.Empty
        Panel26.BackColor = Color.Empty
    End Sub

    Private Sub Label18_MouseHover(sender As Object, e As EventArgs) Handles
Label18.MouseHover
        Label18.BackColor = Color.LightGray
        Panel20.BackColor = Color.LightGray
    End Sub

    Private Sub Label18_MouseLeave(sender As Object, e As EventArgs) Handles
Label18.MouseLeave
        Label18.BackColor = Color.Empty
        Panel20.BackColor = Color.Empty
    End Sub


    Private Sub Label26_MouseHover(sender As Object, e As EventArgs) Handles
Label26.MouseHover
```

```
        Label26.BackColor = Color.LightGray
        Panel28.BackColor = Color.LightGray
    End Sub

    Private Sub Label26_MouseLeave(sender As Object, e As EventArgs) Handles
Label26.MouseLeave
        Label26.BackColor = Color.Empty
        Panel28.BackColor = Color.Empty
    End Sub

    Private Sub Panel22_MouseHover(sender As Object, e As EventArgs) Handles
Panel22.MouseHover
        Panel22.BackColor = Color.LightGray
    End Sub
    Private Sub Panel22_MouseLeave(sender As Object, e As EventArgs) Handles
Panel22.MouseLeave
        Panel22.BackColor = Color.Empty
    End Sub

    Private Sub PictureBox18_MouseHover(sender As Object, e As EventArgs) Handles
PictureBox18.MouseHover
        PictureBox18.BackColor = Color.LightGray
        Panel22.BackColor = Color.LightGray
    End Sub

    Private Sub PictureBox18_MouseLeave(sender As Object, e As EventArgs) Handles
PictureBox18.MouseLeave
        PictureBox18.BackColor = Color.LightGray
        Panel22.BackColor = Color.LightGray
    End Sub
    Private Sub Panel27_MouseHover(sender As Object, e As EventArgs) Handles
Panel27.MouseHover
        Panel27.BackColor = Color.LightGray
    End Sub
    Private Sub Panel27_MouseLeave(sender As Object, e As EventArgs) Handles
Panel27.MouseLeave
        Panel27.BackColor = Color.Empty
    End Sub

    Private Sub PictureBox17_MouseHover(sender As Object, e As EventArgs) Handles
PictureBox17.MouseHover
        PictureBox17.BackColor = Color.LightGray
        Panel27.BackColor = Color.LightGray
    End Sub

    Private Sub PictureBox17_MouseLeave(sender As Object, e As EventArgs) Handles
PictureBox17.MouseLeave
        PictureBox17.BackColor = Color.LightGray
        Panel27.BackColor = Color.LightGray
    End Sub

    Private Sub Panel23_MouseHover(sender As Object, e As EventArgs) Handles
Panel23.MouseHover
        Panel23.BackColor = Color.LightGray
    End Sub
    Private Sub Panel23_MouseLeave(sender As Object, e As EventArgs) Handles
Panel23.MouseLeave
        Panel23.BackColor = Color.Empty
    End Sub
```

```
    Private Sub PictureBox20_MouseHover(sender As Object, e As EventArgs) Handles
PictureBox20.MouseHover
        PictureBox20.BackColor = Color.LightGray
        Panel23.BackColor = Color.LightGray
    End Sub

    Private Sub PictureBox20_MouseLeave(sender As Object, e As EventArgs) Handles
PictureBox20.MouseLeave
        PictureBox20.BackColor = Color.LightGray
        Panel23.BackColor = Color.LightGray
    End Sub

    Private Sub Panel35_MouseHover(sender As Object, e As EventArgs) Handles
Panel35.MouseHover
        Panel35.BackColor = Color.DarkBlue
    End Sub

    Private Sub Panel35_MouseLeave(sender As Object, e As EventArgs) Handles
Panel35.MouseLeave
        Panel35.BackColor = Color.SteelBlue
    End Sub

    Private Sub Label45_MouseHover(sender As Object, e As EventArgs) Handles
Label45.MouseHover
        Label45.BackColor = Color.MidnightBlue
        Panel35.BackColor = Color.MidnightBlue
    End Sub

    Private Sub Label45_MouseLeave(sender As Object, e As EventArgs) Handles
Label45.MouseLeave
        Label45.BackColor = Color.SteelBlue
        Panel35.BackColor = Color.SteelBlue
    End Sub


End Class

Public Class Form2
    Private Sub LinkLabel3_LinkClicked(sender As Object, e As
LinkLabelLinkClickedEventArgs) Handles LinkLabel3.LinkClicked

        Process.Start("https://support.microsoft.com/en-ph/help/4033787/windows-
protect-yourself-from-phishing")
    End Sub


End Class
```

- Third interface software code.

Proposed interface design for the warning message when a Spam email is detected.

```
Public Class Form1

    Dim form As Form2
    Public Sub Form1()
        Panel17.BorderStyle = BorderStyle.None
    End Sub
    Private Sub LinkLabel1_LinkClicked_1(sender As Object, e As
LinkLabelLinkClickedEventArgs) Handles LinkLabel1.LinkClicked
        form = New Form2
        form.Show()
    End Sub


    Private Sub Panel17_MouseHover(sender As Object, e As EventArgs) Handles
Panel17.MouseHover
        Panel17.BackColor = Color.LightGray
    End Sub

    Private Sub Panel17_MouseLeave(sender As Object, e As EventArgs) Handles
Panel17.MouseLeave
        Panel17.BackColor = Color.Empty
    End Sub

    Private Sub Panel18_MouseHover(sender As Object, e As EventArgs) Handles
Panel18.MouseHover
        Panel18.BackColor = Color.LightGray
    End Sub

    Private Sub Panel18_MouseLeave(sender As Object, e As EventArgs) Handles
Panel18.MouseLeave
        Panel18.BackColor = Color.Empty
    End Sub

    Private Sub Panel24_MouseHover(sender As Object, e As EventArgs) Handles
Panel24.MouseHover
        Panel24.BackColor = Color.LightGray
    End Sub

    Private Sub Panel24_MouseLeave(sender As Object, e As EventArgs) Handles
Panel24.MouseLeave
        Panel24.BackColor = Color.Empty
    End Sub

    Private Sub Panel25_MouseHover(sender As Object, e As EventArgs) Handles
Panel25.MouseHover
        Panel25.BackColor = Color.LightGray
    End Sub

    Private Sub Panel25_MouseLeave(sender As Object, e As EventArgs) Handles
Panel25.MouseLeave
        Panel25.BackColor = Color.Empty
    End Sub

    Private Sub Panel26_MouseHover(sender As Object, e As EventArgs) Handles
Panel26.MouseHover
        Panel26.BackColor = Color.LightGray
    End Sub
```

```
    Private Sub Panel26_MouseLeave(sender As Object, e As EventArgs) Handles
Panel26.MouseLeave
        Panel26.BackColor = Color.Empty
    End Sub

    Private Sub Panel20_MouseHover(sender As Object, e As EventArgs) Handles
Panel20.MouseHover
        Panel20.BackColor = Color.LightGray
    End Sub

    Private Sub Panel20_MouseLeave(sender As Object, e As EventArgs) Handles
Panel20.MouseLeave
        Panel20.BackColor = Color.Empty
    End Sub

    Private Sub Panel28_MouseHover(sender As Object, e As EventArgs) Handles
Panel28.MouseHover
        Panel28.BackColor = Color.LightGray
    End Sub

    Private Sub Panel28_MouseLeave(sender As Object, e As EventArgs) Handles
Panel28.MouseLeave
        Panel28.BackColor = Color.Empty
    End Sub

    Private Sub Label15_MouseHover(sender As Object, e As EventArgs) Handles
Label15.MouseHover
        Label15.BackColor = Color.LightGray
        Panel17.BackColor = Color.LightGray
    End Sub

    Private Sub Label15_MouseLeave(sender As Object, e As EventArgs) Handles
Label15.MouseLeave
        Label15.BackColor = Color.Empty
        Panel17.BackColor = Color.Empty
    End Sub

    Private Sub PictureBox6_MouseHover(sender As Object, e As EventArgs) Handles
PictureBox6.MouseHover
        PictureBox6.BackColor = Color.LightGray
        Label15.BackColor = Color.LightGray
        Panel17.BackColor = Color.LightGray
    End Sub

    Private Sub PictureBox6_MouseLeave(sender As Object, e As EventArgs) Handles
PictureBox6.MouseLeave
        PictureBox6.BackColor = Color.LightGray
        Label15.BackColor = Color.LightGray
        Panel17.BackColor = Color.LightGray
    End Sub


    Private Sub Label16_MouseHover(sender As Object, e As EventArgs) Handles
Label16.MouseHover
        Label16.BackColor = Color.LightGray
        Panel18.BackColor = Color.LightGray
    End Sub
```

```
    Private Sub Label16_MouseLeave(sender As Object, e As EventArgs) Handles
Label16.MouseLeave
        Label16.BackColor = Color.Empty
        Panel18.BackColor = Color.Empty
    End Sub

    Private Sub Label22_MouseHover(sender As Object, e As EventArgs) Handles
Label22.MouseHover
        Label22.BackColor = Color.LightGray
        Panel24.BackColor = Color.LightGray
    End Sub

    Private Sub Label22_MouseLeave(sender As Object, e As EventArgs) Handles
Label22.MouseLeave
        Label22.BackColor = Color.Empty
        Panel24.BackColor = Color.Empty
    End Sub

    Private Sub Label23_MouseHover(sender As Object, e As EventArgs) Handles
Label23.MouseHover
        Label23.BackColor = Color.LightGray
        Panel25.BackColor = Color.LightGray
    End Sub

    Private Sub Label23_MouseLeave(sender As Object, e As EventArgs) Handles
Label23.MouseLeave
        Label23.BackColor = Color.Empty
        Panel25.BackColor = Color.Empty
    End Sub

    Private Sub Label24_MouseHover(sender As Object, e As EventArgs) Handles
Label24.MouseHover
        Label24.BackColor = Color.LightGray
        Panel26.BackColor = Color.LightGray
    End Sub

    Private Sub Label24_MouseLeave(sender As Object, e As EventArgs) Handles
Label24.MouseLeave
        Label24.BackColor = Color.Empty
        Panel26.BackColor = Color.Empty
    End Sub

    Private Sub Label18_MouseHover(sender As Object, e As EventArgs) Handles
Label18.MouseHover
        Label18.BackColor = Color.LightGray
        Panel20.BackColor = Color.LightGray
    End Sub

    Private Sub Label18_MouseLeave(sender As Object, e As EventArgs) Handles
Label18.MouseLeave
        Label18.BackColor = Color.Empty
        Panel20.BackColor = Color.Empty
    End Sub


    Private Sub Label26_MouseHover(sender As Object, e As EventArgs) Handles
Label26.MouseHover
        Label26.BackColor = Color.LightGray
        Panel28.BackColor = Color.LightGray
    End Sub
```

```
    Private Sub Label26_MouseLeave(sender As Object, e As EventArgs) Handles
Label26.MouseLeave
        Label26.BackColor = Color.Empty
        Panel28.BackColor = Color.Empty
    End Sub

    Private Sub Panel22_MouseHover(sender As Object, e As EventArgs) Handles
Panel22.MouseHover
        Panel22.BackColor = Color.LightGray
    End Sub
    Private Sub Panel22_MouseLeave(sender As Object, e As EventArgs) Handles
Panel22.MouseLeave
        Panel22.BackColor = Color.Empty
    End Sub

    Private Sub PictureBox18_MouseHover(sender As Object, e As EventArgs) Handles
PictureBox18.MouseHover
        PictureBox18.BackColor = Color.LightGray
        Panel22.BackColor = Color.LightGray
    End Sub

    Private Sub PictureBox18_MouseLeave(sender As Object, e As EventArgs) Handles
PictureBox18.MouseLeave
        PictureBox18.BackColor = Color.LightGray
        Panel22.BackColor = Color.LightGray
    End Sub
    Private Sub Panel27_MouseHover(sender As Object, e As EventArgs) Handles
Panel27.MouseHover
        Panel27.BackColor = Color.LightGray
    End Sub
    Private Sub Panel27_MouseLeave(sender As Object, e As EventArgs) Handles
Panel27.MouseLeave
        Panel27.BackColor = Color.Empty
    End Sub

    Private Sub PictureBox17_MouseHover(sender As Object, e As EventArgs) Handles
PictureBox17.MouseHover
        PictureBox17.BackColor = Color.LightGray
        Panel27.BackColor = Color.LightGray
    End Sub

    Private Sub PictureBox17_MouseLeave(sender As Object, e As EventArgs) Handles
PictureBox17.MouseLeave
        PictureBox17.BackColor = Color.LightGray
        Panel27.BackColor = Color.LightGray
    End Sub

    Private Sub Panel23_MouseHover(sender As Object, e As EventArgs) Handles
Panel23.MouseHover
        Panel23.BackColor = Color.LightGray
    End Sub
    Private Sub Panel23_MouseLeave(sender As Object, e As EventArgs) Handles
Panel23.MouseLeave
        Panel23.BackColor = Color.Empty
    End Sub

    Private Sub PictureBox20_MouseHover(sender As Object, e As EventArgs) Handles
PictureBox20.MouseHover
        PictureBox20.BackColor = Color.LightGray
```

```
        Panel23.BackColor = Color.LightGray
    End Sub

    Private Sub PictureBox20_MouseLeave(sender As Object, e As EventArgs) Handles
PictureBox20.MouseLeave
        PictureBox20.BackColor = Color.LightGray
        Panel23.BackColor = Color.LightGray
    End Sub

    Private Sub Panel35_MouseHover(sender As Object, e As EventArgs) Handles
Panel35.MouseHover
        Panel35.BackColor = Color.DarkBlue
    End Sub

    Private Sub Panel35_MouseLeave(sender As Object, e As EventArgs) Handles
Panel35.MouseLeave
        Panel35.BackColor = Color.SteelBlue
    End Sub

    Private Sub Label45_MouseHover(sender As Object, e As EventArgs) Handles
Label45.MouseHover
        Label45.BackColor = Color.MidnightBlue
        Panel35.BackColor = Color.MidnightBlue
    End Sub

    Private Sub Label45_MouseLeave(sender As Object, e As EventArgs) Handles
Label45.MouseLeave
        Label45.BackColor = Color.SteelBlue
        Panel35.BackColor = Color.SteelBlue
    End Sub


End Class
Public Class Form2
    Private Sub LinkLabel3_LinkClicked(sender As Object, e As
LinkLabelLinkClickedEventArgs) Handles LinkLabel3.LinkClicked

        Process.Start("https://support.microsoft.com/en-ph/help/4033787/windows-
protect-yourself-from-phishing")
    End Sub


End Class
```

- **Fourth interface software code.**

Proposed interface design for a notification message when receiving an email from trusted sender.

```
Public Class Form1

    Private Sub Panel17_MouseHover(sender As Object, e As EventArgs) Handles
Panel17.MouseHover
        Panel17.BackColor = Color.LightGray
    End Sub

    Private Sub Panel17_MouseLeave(sender As Object, e As EventArgs) Handles
Panel17.MouseLeave
        Panel17.BackColor = Color.Empty
    End Sub

    Private Sub Panel19_MouseHover(sender As Object, e As EventArgs) Handles
Panel19.MouseHover
        Panel19.BackColor = Color.LightGray
    End Sub

    Private Sub Panel19_MouseLeave(sender As Object, e As EventArgs) Handles
Panel19.MouseLeave
        Panel19.BackColor = Color.Empty
    End Sub

    Private Sub Panel24_MouseHover(sender As Object, e As EventArgs) Handles
Panel24.MouseHover
        Panel24.BackColor = Color.LightGray
    End Sub

    Private Sub Panel24_MouseLeave(sender As Object, e As EventArgs) Handles
Panel24.MouseLeave
        Panel24.BackColor = Color.Empty
    End Sub

    Private Sub Panel25_MouseHover(sender As Object, e As EventArgs) Handles
Panel25.MouseHover
        Panel25.BackColor = Color.LightGray
    End Sub

    Private Sub Panel25_MouseLeave(sender As Object, e As EventArgs) Handles
Panel25.MouseLeave
        Panel25.BackColor = Color.Empty
    End Sub

    Private Sub Panel26_MouseHover(sender As Object, e As EventArgs) Handles
Panel26.MouseHover
        Panel26.BackColor = Color.LightGray
    End Sub

    Private Sub Panel26_MouseLeave(sender As Object, e As EventArgs) Handles
Panel26.MouseLeave
        Panel26.BackColor = Color.Empty
    End Sub

    Private Sub Panel20_MouseHover(sender As Object, e As EventArgs) Handles
Panel20.MouseHover
        Panel20.BackColor = Color.LightGray
    End Sub
```

```
    Private Sub Panel20_MouseLeave(sender As Object, e As EventArgs) Handles
Panel20.MouseLeave
        Panel20.BackColor = Color.Empty
    End Sub

    Private Sub Panel28_MouseHover(sender As Object, e As EventArgs) Handles
Panel28.MouseHover
        Panel28.BackColor = Color.LightGray
    End Sub

    Private Sub Panel28_MouseLeave(sender As Object, e As EventArgs) Handles
Panel28.MouseLeave
        Panel28.BackColor = Color.Empty
    End Sub

    Private Sub Label15_MouseHover(sender As Object, e As EventArgs) Handles
Label15.MouseHover
        Label15.BackColor = Color.LightGray
        Panel17.BackColor = Color.LightGray
    End Sub

    Private Sub Label15_MouseLeave(sender As Object, e As EventArgs) Handles
Label15.MouseLeave
        Label15.BackColor = Color.Empty
        Panel17.BackColor = Color.Empty
    End Sub

    Private Sub PictureBox6_MouseHover(sender As Object, e As EventArgs) Handles
PictureBox6.MouseHover
        PictureBox6.BackColor = Color.LightGray
        Label15.BackColor = Color.LightGray
        Panel17.BackColor = Color.LightGray
    End Sub

    Private Sub PictureBox6_MouseLeave(sender As Object, e As EventArgs) Handles
PictureBox6.MouseLeave
        PictureBox6.BackColor = Color.LightGray
        Label15.BackColor = Color.LightGray
        Panel17.BackColor = Color.LightGray
    End Sub


    Private Sub Label17_MouseHover(sender As Object, e As EventArgs) Handles
Label17.MouseHover
        Label17.BackColor = Color.LightGray
        Panel19.BackColor = Color.LightGray
    End Sub

    Private Sub Label17_MouseLeave(sender As Object, e As EventArgs) Handles
Label17.MouseLeave
        Label17.BackColor = Color.Empty
        Panel19.BackColor = Color.Empty
    End Sub

    Private Sub Label22_MouseHover(sender As Object, e As EventArgs) Handles
Label22.MouseHover
        Label22.BackColor = Color.LightGray
        Panel24.BackColor = Color.LightGray
    End Sub
```

```
    Private Sub Label22_MouseLeave(sender As Object, e As EventArgs) Handles
Label22.MouseLeave
        Label22.BackColor = Color.Empty
        Panel24.BackColor = Color.Empty
    End Sub

    Private Sub Label23_MouseHover(sender As Object, e As EventArgs) Handles
Label23.MouseHover
        Label23.BackColor = Color.LightGray
        Panel25.BackColor = Color.LightGray
    End Sub

    Private Sub Label23_MouseLeave(sender As Object, e As EventArgs) Handles
Label23.MouseLeave
        Label23.BackColor = Color.Empty
        Panel25.BackColor = Color.Empty
    End Sub

    Private Sub Label24_MouseHover(sender As Object, e As EventArgs) Handles
Label24.MouseHover
        Label24.BackColor = Color.LightGray
        Panel26.BackColor = Color.LightGray
    End Sub

    Private Sub Label24_MouseLeave(sender As Object, e As EventArgs) Handles
Label24.MouseLeave
        Label24.BackColor = Color.Empty
        Panel26.BackColor = Color.Empty
    End Sub

    Private Sub Label18_MouseHover(sender As Object, e As EventArgs) Handles
Label18.MouseHover
        Label18.BackColor = Color.LightGray
        Panel20.BackColor = Color.LightGray
    End Sub

    Private Sub Label18_MouseLeave(sender As Object, e As EventArgs) Handles
Label18.MouseLeave
        Label18.BackColor = Color.Empty
        Panel20.BackColor = Color.Empty
    End Sub


    Private Sub Label26_MouseHover(sender As Object, e As EventArgs) Handles
Label26.MouseHover
        Label26.BackColor = Color.LightGray
        Panel28.BackColor = Color.LightGray
    End Sub

    Private Sub Label26_MouseLeave(sender As Object, e As EventArgs) Handles
Label26.MouseLeave
        Label26.BackColor = Color.Empty
        Panel28.BackColor = Color.Empty
    End Sub

    Private Sub Panel22_MouseHover(sender As Object, e As EventArgs) Handles
Panel22.MouseHover
        Panel22.BackColor = Color.LightGray
    End Sub
```

```
    Private Sub Panel22_MouseLeave(sender As Object, e As EventArgs) Handles
Panel22.MouseLeave
        Panel22.BackColor = Color.Empty
    End Sub

    Private Sub PictureBox18_MouseHover(sender As Object, e As EventArgs) Handles
PictureBox18.MouseHover
        PictureBox18.BackColor = Color.LightGray
        Panel22.BackColor = Color.LightGray
    End Sub

    Private Sub PictureBox18_MouseLeave(sender As Object, e As EventArgs) Handles
PictureBox18.MouseLeave
        PictureBox18.BackColor = Color.LightGray
        Panel22.BackColor = Color.LightGray
    End Sub
    Private Sub Panel27_MouseHover(sender As Object, e As EventArgs) Handles
Panel27.MouseHover
        Panel27.BackColor = Color.LightGray
    End Sub
    Private Sub Panel27_MouseLeave(sender As Object, e As EventArgs) Handles
Panel27.MouseLeave
        Panel27.BackColor = Color.Empty
    End Sub

    Private Sub PictureBox17_MouseHover(sender As Object, e As EventArgs) Handles
PictureBox17.MouseHover
        PictureBox17.BackColor = Color.LightGray
        Panel27.BackColor = Color.LightGray
    End Sub

    Private Sub PictureBox17_MouseLeave(sender As Object, e As EventArgs) Handles
PictureBox17.MouseLeave
        PictureBox17.BackColor = Color.LightGray
        Panel27.BackColor = Color.LightGray
    End Sub

    Private Sub Panel23_MouseHover(sender As Object, e As EventArgs) Handles
Panel23.MouseHover
        Panel23.BackColor = Color.LightGray
    End Sub
    Private Sub Panel23_MouseLeave(sender As Object, e As EventArgs) Handles
Panel23.MouseLeave
        Panel23.BackColor = Color.Empty
    End Sub

    Private Sub PictureBox20_MouseHover(sender As Object, e As EventArgs) Handles
PictureBox20.MouseHover
        PictureBox20.BackColor = Color.LightGray
        Panel23.BackColor = Color.LightGray
    End Sub

    Private Sub PictureBox20_MouseLeave(sender As Object, e As EventArgs) Handles
PictureBox20.MouseLeave
        PictureBox20.BackColor = Color.LightGray
        Panel23.BackColor = Color.LightGray
    End Sub

    Private Sub Panel35_MouseHover(sender As Object, e As EventArgs) Handles
Panel35.MouseHover
```

```
        Panel35.BackColor = Color.DarkBlue
    End Sub

    Private Sub Panel35_MouseLeave(sender As Object, e As EventArgs) Handles
Panel35.MouseLeave
        Panel35.BackColor = Color.SteelBlue
    End Sub

    Private Sub Label45_MouseHover(sender As Object, e As EventArgs) Handles
Label45.MouseHover
        Label45.BackColor = Color.MidnightBlue
        Panel35.BackColor = Color.MidnightBlue
    End Sub

    Private Sub Label45_MouseLeave(sender As Object, e As EventArgs) Handles
Label45.MouseLeave
        Label45.BackColor = Color.SteelBlue
        Panel35.BackColor = Color.SteelBlue
    End Sub

End Class
```