2019

Evaluation and Enhancement of Public Cyber Security Awareness

Alotaibi, Faisal Fahad G

Copyright statement

UNIVERSITY OF PLYMOUTH

Evaluation and Enhancement of Public Cyber Security Awareness

by

Faisal Fahad G Alotaibi

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

DOCTOR OF PHILOSOPHY

School of Computing

May 2019

Table of Contents

List of Tables

List of Figures

Acknowledgements

Alhamdulillah (All praise and thanks are due to the Almighty Allah) who always guides me to the right path and has helped me to complete my PhD.

First and foremost, I would like to express my thanks and gratitude to my parents, the ones who can never ever be thanked enough, for the overwhelming love and motivate me and care they bestow upon me, and who have supported me and without whose proper guidance it would have been impossible for me to complete my PhD.

I have no words to acknowledge my indebtedness to my wife for her constant support, abiding faith and who has been struggling with me, hand by hand, step by step, to secure and shape brighter future. I wish to express my love and thanks to 'the beats of my heart,' my kids, Linda and Tala, who are the only source of inspiration to me, and it is their love and innocent smiles that have made the hardship of this task bearable. My deep love and thanks are due to my brothers, sisters and the entire family.

I wish to express my honest gratitude to my supervision team, to my DOS, Professor Steven Furnell for providing me with a wealth of help and support during this project, really this work would have never been completed without his support. I also wish to thank my second supervisor Dr. Ingo Stengel and third supervisor Dr. Maria Papadaki for their time and efforts in making the programme easier and better.

I am grateful to government of Saudi Arabia, the Minister of Military, for granting me the scholarship and sponsoring my undertaking of this PhD programme.

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 University of Plymouth or at another establishment.

Publications (or public presentation of creative research outputs):

Faisal Alotaibi, Steven Furnell, Ingo Stengel and Maria Papadaki ''A Review of Using Gaming Technology for Cyber-Security Awareness'', International Journal for Information Security Research (IJISR), Volume 6 Issue 4, ISSN 2042-4639, 2016, pp. 660.

DOI :https://infonomics-society.org/wp-content/uploads/ijisr/published-papers/volume-6-2016/A-Review-of-Using-Gaming-Technology-for-Cyber-Security-Awareness.pdf

Faisal Alotaibi, Steven Furnell, Ingo Stengel and Maria Papadaki ''Design and Evaluation of Mobile Games for enhancing Cyber Security Awareness '' Journal of Internet Technology and Secured Transaction (JITST), Volume 7, Issue 1, ISSN 2046-3723.

DOI:https://infonomics-society.org/wp-content/uploads/jitst/published-papers/volume-6-2018/Design-and-Evaluation-of-Mobile-Games-for-Enhancing-Cyber-Security-Awareness.pdf

Presentations at conferences:

Faisal Alotaibi, Steven Furnell, Ingo Stengel and Maria Papadaki, '' A survey of cyber-security awareness in Saudi Arabia'' In The 12th International Conference for Internet Technology and Secured Transactions (ICITST), Barcelona, Spain, December 2016, pp. 154.

DOI: https://ieeexplore.ieee.org/document/7856687

Faisal Alotaibi, Steven Furnell, Ingo Stengel and Maria Papadaki, '' Gamifying cyber security awareness via mobile training apps'' In Collaborative European Research Conference (CERC), Karlsruhe University of Applied Sciences – Karlsruhe, Germany, September 2017, pp. 236.

DOI:https://www.cerc-conference.eu/wp-content/uploads/2018/06/CERC-2017-proceedings.pdf

Faisal Alotaibi, Steven Furnell, Ingo Stengel and Maria Papadaki, ‘’ Enhancing cyber security awareness with mobile game‘’ In The 12th International Conference for Internet Technology and Secured Transactions(ICITST), University of Cambridge, UK, December 2017.

DOI: https://ieeexplore.ieee.org/document/8356361

Word count of the main body of thesis: 62532

Signed **Faisal Alotaibi**

Date **25/4/2019**

Abstract

With the spread of the Internet and the technology, Cyberspace has become the life of everyone, which requires them to be aware of the threats of it. Also, to be prepared with the speed of the technology, whether electronic payment, social life, leisure work IOT ،and everything. However, in spite of increasing security practices there has been a rise in the cyber security threats and attacks. As the life is becoming more and more dependent on the technology, the need for cyber security awareness has become an important activity that need to be practiced in order to be safe and secure from the increasing cyber threats. Considering these factors, this thesis focuses on developing and implementing the two cyber security awareness games, mainly Password Protector and Malware Guardian. As cyber security is a vast area and requires various secure practices that need to be adopted the scope of the study is limited to password security and malware protection.

Saudi Arabia is one of the fastest developing countries which has observed a tremendous increase in the use of internet and technology services and also the mobile devices for accessing various services. However, this adoption of technology is relatively new to the larger section, and the security practices that need to followed, may not be fully recognised by the population. Considering these developments, Saudi Arabia is used as the study location for implementing and evaluating the games. Initially a pilot study using a questionnaire based survey is conducted for understanding the level of cyber security awareness relating to the cyber security practices in Saudi Arabia. The results analysed from the study reflected poor understanding and awareness about password protection and malware concepts among the population. One of the interesting aspects identified from the pilot study is that most of the participants preferred mobile based application for generating cyber security awareness.

Accordingly, two mobile games are developed. In order to evaluate the impact of the games, a pre-study test was carried out using an online survey questionnaire to record the understanding of passwords and malware among the participants. Then the mobile games Password Protector and Malware Guardian were distributed to the participants using the download link. The participants used the games for three weeks, and then undertook the same survey that was used before playing the game. The impact of the

games is then analysed by comparing the changes in the awareness levels of the participants after using the games. The results from the study were found to be having positive impact as the awareness levels have increased significantly among the participants. Participants ability to create a strong and complex password has been improved significantly after playing the Password Protection game. Similarly, participants awareness levels about the malware threats and the safety measures that need to be taken such as backup, installing anti-malware software, updates etc. was improved significantly after using the Malware Guardian game. The overall findings were discussed, analysed and correlated with influencing factors and explained in this study. Accordingly, this study has found that the gamification can significantly enhance cyber security awareness.

Chapter One

Introduction

1. Introduction

More than 3 billion Internet users have utilized Internet services across the world and this number is growing continuously (Internetlivestats.com, 2017). Their daily usage includes (but not limited to) web browsing, entertainment (e.g. watching online videos), communication (e.g. making VoIP calls), finance (e.g. online shopping) and office applications (e.g. Google docs). Indeed, many of the traditional desktop applications such as Office are now found as Internet-based services (Microsoft, 2017; Louisville free Public library, 2017). Information Technology and Internet are ubiquitous tools for companies. For example, a fifth of UK business turnover was generated by e-commerce sales alone. Whilst these technological revolutions have changed the nature of business and opened a global marketplace, they have also opened the door to misuse and cybercrime. There are now many different security tools to enable organisations to mitigate information misuse, for example, Authentication, Access control, Anti-Virus, Firewalls, Intrusion Detection Systems and Security Information and Event Management (SIEM).

However, the scale of rise in cybercrimes has been alarming. The cost of cyber breaches in UK alone is estimated to be £ 3.14 million (Ashford, 2015). Similarly, the Business Email Compromise (BEC) scams worldwide were estimated to be more than $ 3 billion (IC3, 2016). The impact of the cybercrime is not just assessed by the costs incurred but also the data privacy, which can affect many consumers. The projected losses for the businesses by the year 2019 due to cybercrime would be $ 2 trillion (Juniper Research, 2016). The numbers of cyber security attacks in the large companies have been decreasing, while in the medium and small sized companies it is increasing effectively, which could be a major concern in the developing countries (Symantec, 2016).

Considering these aspects, this thesis focuses public cyber security threats and on using gaming technology for raising cyber security awareness in one of the developing country, Saudi Arabia.

1.1. Research Overview

With the extensive development across the communication technologies, many nations and organizations are deploying the communication technologies for

automating the processes and to provide cheaper, faster and easier ways of accessing the services for the customers. On the same line, the preference of communication technologies such as emails, mobile technologies like apps etc. is rising exponentially in the recent years.

Automation is being increasingly adopted in the organizations to increase process efficiency and to provide effective services. Technology has become a part of life with many, as everyday activities like shopping, banking, entertainment are being accessed on mobile devices. All these services are managed by effective information exchange through communication technologies. In line with the rise in technology, the crimes associated with the technologies are also on rise. Different methods are being adopted for stealing information. Such activities can be termed as cybercrime, where the computer networks are used to carryout illegal activities (Liu et al., 2012). As most people, businesses and organizations are increasingly relying on the communication technologies, it is very essential that the information being exchanged is secured to prevent misuse.

1.1.1. Saudi Arabia Case Study

Saudi Arabia is one of the fastest developing countries in the Middle East region, which has seen an enormous growth in the use of communication technologies, Internet and mobile technologies in the recent years. It is estimated that about 65.9% of the population have access to Internet which accounts to more than 18 million users. Facebook and Twitter are used by majority of them (Miniwatts Marketing Group, 2016). About 39% of the population using Internet buys products online, and the country's E-commerce business is about $ 520 million (CMO Council Middle East, 2015). The penetration of Internet and the boom in smartphone usage in KSA is relatively new. Therefore, it may be considered that there is a lower understanding of the importance of cyber security and information security measures. Furthermore, several existing studies on cyber security awareness are largely carried out in developed western countries. On the other hand, KSA is vastly different from these countries in terms of culture, social attitudes, language, government regulations and understanding the importance of security. In addition, there are increasing cyber-attacks in Saudi Arabia in the recent years targeting private companies, citizens, government agencies etc.

which may be a serious concern in relation to security and privacy (Reuters, 2013; Bronk et al., 2013; Al-Hussein, 2017; Bodhani, 2017; Shamseddine and Kalin, 2017).

Shamoon Malware which attacked Saudi Aramco in 2012 has resurfaced in 2016 and affected large number of workstations of Saudi Civil Aviation agency and other companies operating in Saudi Arabia (Pauli, 2016; Albano & Kessem, 2017; Perlroth & Krauss, 2018). Similarly, Triton Malware attacked Saudi Aramco safety systems (Triconex), which provides emergency shutdown functionality; a failure in emergency shutdown may lead to devastating results which could incur serious losses (Groll, 2017). Similarly, Microsoft study on Saudi Arabia has revealed three major cyber threats which includes ransomware, low hanging fruits, botnets and malware; which can cause various damages in the security systems (Al-Mayman, 2018). There is a rise in the number of security attacks in the recent years, and the effect of the attacks has been resulting in severe losses. In addition, there are very few studies identified in relation to the cyber security awareness; and no study identified using the gamification as an approach to increase cyber security awareness in the context of Saudi Arabia. In addition, the rapid increase in the mobile and internet usage in Saudi Arabian families (99.16% in 2018) has increased the risk of cyber threats, where the internet adoption has largely increased in short duration with people who are less aware of cyber security threats (Mubasher, 2019).

To increase awareness about cyber security, it is essential that the users are provided with training. Serious games can be an effective method to provide training to the users. Serious games are games that are designed with a purpose rather than just intended for pure entertainment. They are proved to be effective tools for training and achieving a behavioural change. Such methods of using games for training is also referred as games-based learning approaches. Though games-based learning methods are mainly utilised in school education, increasingly, these methods are also adopted in healthcare, advertising, behavioural change, and recently in cyber security training (Hendrix et al., 2016). Considering these factors, the case of Saudi Arabia is selected, where there is an urgent need to increase cybesecurity awareness practices.

The game based learning (GBL) method is one of the effective techniques to create awareness and educate the users, and it has several advantages. The obvious advantage is that games-based learning method provides an interactive approach to

train or educate the users about a specific program. It enables the players to acquire skills and to enable thought processes in a fun and interactive way. The adaptability and flexibility of games approaches enables to design the game to suit almost every training subject possible (Boyle, 2011). A well-designed game enables the user to enter a virtual environment that is similar to the real environment and would enable the player to draw connection between the learning in the virtual environment to the real world. The games-based approach would motivate the player to move towards the goal with required actions and also see the consequences without facing penalties in the real life. Further, when compared to the traditional method of training, games-based methods are more engaging, relatively cost effective, easily transferrable to a large number of trainees, customised to each player, etc. (Trybus, 2014).

Considering these factors, to address the public security threats and concerns in Saudi Arabia, the cyber security awareness creation through GBL method could have various positive implications. Based on this concept, the aim and objectives of this thesis are developed.

1.2. Motivation

There is a rising trend observed in the cyber-attacks in Saudi Arabia. In 2013, a series of attacks targeted several government websites which crashed various websites including the interior ministry website. The business organizations and the government agencies are facing huge challenges in the country with the increase in sophisticated and innovative cyber-attacks launched by hacker activists and foreign governments (Reuters, 2013). Another cyber-attack took place in 2012 targeting Saudi Aramco, an oil and gas company and one of the major sources of income to the Saudi government, resulting in damaging about 30,000 computers, using Shamoon malware, which is considered to be one of the most destructive cyber-attacks targeted at a single company (Bronk et al., 2013). Considering these issues there is an urgent need to promote cyber security awareness and deploy effective security mechanisms in order to combat the rising threats.

Lack of awareness is one of the major problems identified by various researchers for increasing public cyber security threats and concerns (Brujin and Janssen, 2017; Mehta and Singh, 2013; Clark et al., 2014; Rowan and Josh, 2014), and various

programs and initiatives were suggested for increasing the cyber security awareness (Pusey and Sadera, 2011; Paulsen et al., 2012; Hayani et al., 2015; Mackenzie and Maged, 2015; Choi et al., 2013). Therefore, there is a need to promote awareness creation methods to increase the knowledge among the public with regards to the cyber security safety measures. Gamification in this scenario can be an effective medium for raising cyber security awareness, and various studies have implemented this technique and found positive results in increasing the awareness of the users (Shih et al., 2011; Tian et al., 2010; Trybus, 2014; Arachchilage and Love, 2014; Gondree et at., 2013; Kayali et al., 2014).

These factors of rising Internet users and cyber security threats in Saudi Arabia, need for cyber security awareness among the public, and the effective outcomes about the use of gaming technology in various studies, motivated in conducting this thesis work.

1.3. Aims and Objectives

The main aim of this research study is to suggest an effective solution (gaming application) for creating cyber security and rising awareness in Saudi Arabia, and the related objectives are stated below.

- To conduct a public users perspective study to assess the needs and expectations of the people in Saudi Arabia relating to the cyber security awareness programs and to assess their awareness levels.
- To design and develop effective gaming application to increase the cyber security awareness in most commonly found public cyber security threats and risks.
- To evaluate the games in improving the knowledge and awareness levels of the people, and to assess the adoption, acceptance, usability, learning, and enjoyment aspects of the games developed.

1.4. Contributions of Research

The major research contributions include the following.

- A detailed literature review about public cyber security threats, practices, awareness techniques, and applications used for awareness and a systematic

review of major games-based applications, and popular games used for raising cyber security awareness.

- A preliminary study on the cyber security threats in Saudi Arabia, current status and practices, and the needs and requirements for raising awareness levels among the people.
- Design and develop 12 gaming awareness applications concerned with most common public cyber security threats (Password Protector and Malware Guardian Games for people in Saudi Arabia).
- An evaluation study of two gaming applications (Password Protector and Malware Guardian Games) in raising the awareness levels of the public along with evaluation of usability, learning, and enjoyability aspects relating to the games.

1.5. Thesis Structure

The rest of the thesis is arranged in the following chapters.

Chapter two: Cyber security. The literature review includes the information about various cyber security concepts: practices, awareness, challenges in combating cybercrime, the role of users in this process, the use of application-based techniques for cyber security, and public cyber security threats. This chapter presents an overview about the cyber security, threats associated with it, and the current practices for combating threats, and the need for effective methods.

Chapter three: Cyber security in Saudi Arabia. This chapter reviews the current situation in Saudi Arabia with respect to cyber security threats. The chapter reviews the previous studies conducted in the Saudi Arabia, assesses the current situation through a pilot study conducted using online survey process investigating the aspects of the levels of Internet and mobile usage, current cyber security safety practices, and the level of awareness among the people.

Chapter four: Gamification. This chapter presents an overview about the use of gaming technology for creating awareness, a systematic review of studies focusing on the use of gaming technologies for cyber security awareness and a review of popular cyber security games used for raising awareness about cyber threats.

Chapter five: Designing Issue-Focused Mobile games. This chapter presents an overview of games-based learning process; discusses the ideas of 12 games focusing on various cyber security threats and risks with prototype models and the justifications for selecting the two games Password Protector and Malware Guardian for further development.

Chapter six: Design and Development. This chapter discusses the design and development process of both Password Protector and Malware Guardian games, explaining the idea and story; conceptualization and design; technologies used; development process, testing and evaluation approach.

Chapter seven: Results and Analysis. This chapter discusses the evaluation process of the games using a pre and post study survey process for assessing the increase in the awareness levels of the game users. Additionally, heuristic evaluation approach is used to evaluate usability, learnability, and enjoyability aspects of both the games.

Chapter eight: Summary and Conclusions. This chapter discusses the findings in this thesis, explains the research contributions, and proposes the possible extensions for future works.

Chapter Two

Cyber Security Challenges Facing End-Users

2. Cyber Security: Definition

The concept of cyber security has routed from the Cyber space, which has been defined from various perspectives. It is important to understand the concept of cyber space before understanding the cyber security. The meaning of cyber space has been modified numerous times since the large-scale adoption of Internet from its early roots of ARPANET. The US department of Defence, which can be considered as the god-father of Internet has given more than 12 definitions to the cyber space, as its scope has been changing from the time to time. Its initial definition was mainly focused on communications over computer networks, which was then continuously modified to fix all the aspects that are rapidly being integrated with Internet. It was defined by Pentagon as 'the global domain' within the information environment consisting of the inter-dependent network of information technology infrastructures, including Internet, telecommunications networks, computer systems, and embedded processors and controllers (Singer and Friedman, 2014). This definition reflects the scope and the large number of systems that are integrated with Internet. Cyber security is concerned with all these aspects considered in defining the cyber space, protecting and safeguarding them.

Cyber security thus defined as the process involving various operations in protecting and safeguarding software (core technologies, processes, programs etc.), hardware (Processors, computers, systems), people, and data from damage, injury or unauthorised access (Beyer and Brummel, 2015). According to European Union Agency for Network and Information Security (2017), "*Cyber security covers all aspects of prevention, forecasting, tolerance, detection; mitigation, removal, analysis and investigation of cyber incidents. Considering the different types of components of the cyber space, cyber security should cover the following attributes: Availability, Reliability, Safety, Confidentiality, Integrity, Maintainability (for tangible systems, information and networks) Robustness, Survivability, Resilience (to support the dynamicity of the cyber space), Accountability, Authenticity and Non-repudiation (to support information security)*".

2.1 Need for Cyber Security

The reason for the need for cyber security is the existence of cyber threats. Activities by miscreants that can negatively impact the integrity of the components of the cyber space can be referred to as cyber threats. The range of cyber threats has been increasing rapidly in accordance with growing technology and security features. In such situations, it is necessary to coordinate and update the cyber security related aspects from time to time. The end users are the main target group who can be employees in organizations or general public who are impacted by a security threats or attacks. US Department of Homeland Security (2016) identified various types of threats observed in cyberspace which includes child exploitation, banking and financial frauds, and intellectual property violations and other activities that can have substantial human and economic consequences.

The nature and the scope of cyber-attacks have been changing rapidly in line with the introduction of new technology and applications in the market place. The views of policy makers towards cyber security are also changing and the measures are being put in place to deal effectively with cyber-attacks. Various governments are recognizing the importance of cyber security and are making it as a priority in their agenda. Fonesca and Rosen (2017) has stated that Cyber security is one of the most pressing issues on the US national security agenda. Berman (2013) stressed the importance of planning to combat cyber threats and attacks by adopting security audit and building a responsive strategy. Bogdanov (2015) has identified some major issues which include the following.

- Social Media would be the perfect platform for cyber-attacks.
- Malware would be often delivered from trusted servers that have been hacked.
- Banking, finance, and healthcare sectors would be targeted through mobile malware.
- A wider spectrum of connected devices would be available for hackers.
- The new threats revolutionise the way security systems are built.

There are different types of cyber attacks. Of them, some of the most common ones are Ransomware, malwares, virus, budgetary constraints, social engineering, identity theft, kill chains and others. For a safe interaction with cyber space, it is essential for computers to be resistant to these attacks. Cyber security is identified as a complex task. As the types of attacks and attackers evolve every day using different attacks, and new threats emerge rapidly, it can be a complex task to effectively implement cyber security process.

According to Ponemon Institute Report in 2013, 234 MNCs across six countries were found to be victim of malware attacks, out of which 57% experienced Distributed Denial of Service (DDoS) attacks, with attacks noticed 1.3 times a week, costing $7.2 million annually (Kaul and Prasad, 2015). In 2014, cache of credentials of 360 million accounts and 1.25 billion email addresses was put on sale on online black market, which is considered to be one of the biggest data breaches. This data was acquired through continuous attacks on Google, Yahoo, and Microsoft for almost three weeks (Watkins, 2014). Considering the scope of losses and impact, the cyber-attacks can cause, it is very much essential to put in place the best and effective systems to combat cyber-attacks.

Security against cyber threats is very important for the organizations and generally they adopt measures to ensure cyber security. The worldwide spending for cyber security is projected to reach 101 billion by 2018 (FireEye, 2017). However, despite considerable investment and adoption of cyber security measures, globally, organizations continue to be victims of cyber attacks and at several instances they lose vital assets due to the attacks. Therefore, adoption of cyber security measures needs more focus and better practices need to be applied to increase its effectiveness. It is essential for organizations to ensure implementation of cyber security in its operations at all aspects of their organizations and monitor that all stakeholders are aware and follow the cyber security measures. Thus, there is a need to understand the cyber security practices, challenges, and solutions for effective implementation of cyber security measures.

Hruza et al. (2014) have found that the traditional security measures are no longer effective in combating cyber-attacks, as the advanced and persistent cyber-attacks keep growing innovatively with an ability to penetrate the traditional security systems

and remain undetected for months. The study also suggested that finding a mathematical formula to calculate the proportion of forces (cyber-attacks) and means in field of cyber warfare has become a new trend, which suggests that the attacks are growing rapidly and new measures are being put in place for calculating the attacks apart from the security and defence measures.

As the cyberspace includes almost all entities in the current society, including businesses, organizations, government, society on online platforms, and also development sectors like healthcare, education; there is need to integrate all the entities in developing cyber security strategy, and updating the process from time to time to adopt the changing practices and technology. Moslemzadeh et al. (2013) stated that Cybercrime (attacks) is a transnational crime which must be subjected to universal jurisdiction through cooperation among the different nations across the globe. The paper expresses the nature of cyber-attacks which are not bound by geographical boundaries, has to be dealt with cooperation, and a cooperative strategy is one of the most important points in combating the cyber-attacks. Choucri et al. (2013) argued that the current instructional landscape for combating cybercrime is still under construction. Considering the scope and the impact of cyber-attacks, it is essential that effective combating systems are put in place quickly in order to minimise the amount of losses.

Across the globe, there are various organizations taking part in this process through cooperative strategy. For example, a joint group of Cyber security Coordination Group (CSSG), European Committee for Electrotechnical Standardization (CENELEC), and the European Telecommunications Standards Institute (ETSI) was formed with an objective to coordinate cyber security standards within their organizations in the fields of IT Security, Network and Information Security and Cyber security (European Union Agency for Network And Information Security, 2015). Five different domains in cyber security were identified by the group which includes communications security, operations security, information security, military security, and physical security. Adopting the strategy various cooperative organizations are formed including global Standard Development Organizations (SDO) LIKE ISO, ITU; Industry specific forums like OASIS, W3C, TCG; etc. covering the areas of security feature provision, security assurance, threat sharing, and organizational management for secure operations.

Thus, cyber security is a globally recognized phenomenon and hence organizations and nations are cooperation to develop a global cooperative strategy for cyber security.

2.2. Ensuring Cyber security: Frameworks and Methods of Practice

Ensuring highest levels of cyber security is crucial and hence a systematic methodology need to be followed while adopting cyber security measures. There are different approaches available for ensuring safety from cyber threats and attacks. Studies present different types of methodology and frameworks that can be adopted by organizations in order to implement a robust cyber security system in their organizations. Some of the approaches from the literature and important frameworks in this regard are discussed below.

An important approach as identified by Adele (2016) is to promote cyber security culture at international, national, organizational, and individual level in order to minimise the risks of cyber threats. Cyber security Culture Research Methodology (CSeCRM) was proposed by Adele (2016) for measuring cyber security culture. This approach can be applied at all institution levels across the globe. The aim of the CSeCRM is that it provides a quantitative methodology that can be used to develop a reliable and valid measuring instrument is used to measure cyber security culture in an organization and target group. The results that can be obtained from the measuring instrument can then be used to identify actions that can be applied to bring change to the cyber security culture at an organizational, national and international level. The below figure provides an outline of the different phases in the CSeCRM methodology.

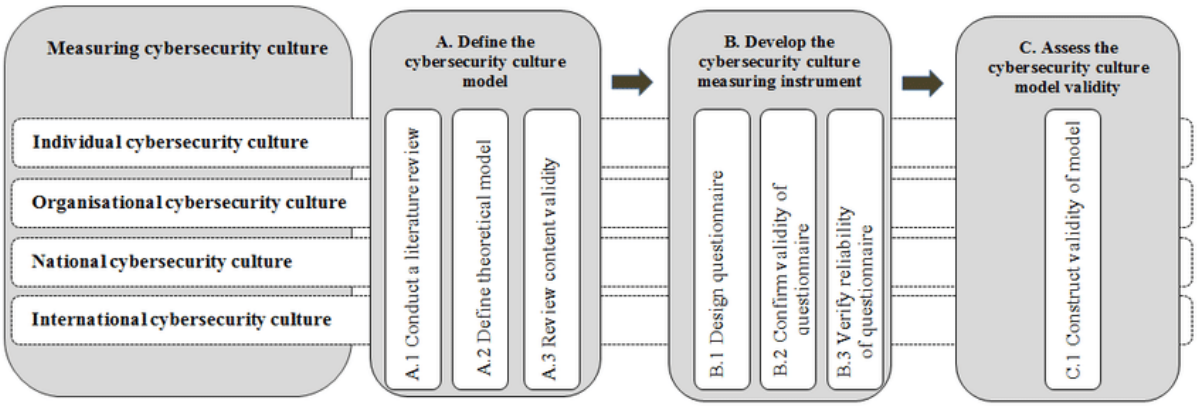


Figure 2. 1 Cyber security culture research methodology (CSeCRM) (Adele, 2016)

One of the important framework for implementing cyber security in organizations is the NIST framework. (NIST) National Institute of Standards and Technology (2014) proposed a framework for critical infrastructure cyber security, with core structure containing the functions as shown in Figure 2.1.

Function Unique Identifier	Function	Category Unique Identifier	Category
ID	Identify	ID.AM	Asset Management
		ID.BE	Business Environment
		ID.GV	Governance
		ID.RA	Risk Assessment
		ID.RM	Risk Management Strategy
		ID.SC	Supply Chain Risk Management
PR	Protect	PR.AC	Identity Management and Access Control
		PR.AT	Awareness and Training
		PR.DS	Data Security
		PR.IP	Information Protection Processes and Procedures
		PR.MA	Maintenance
		PR.PT	Protective Technology
DE	Detect	DE.AE	Anomalies and Events
		DE.CM	Security Continuous Monitoring
		DE.DP	Detection Processes
RS	Respond	RS.RP	Response Planning
		RS.CO	Communications
		RS.AN	Analysis
		RS.MI	Mitigation
		RS.IM	Improvements
RC	Recover	RC.RP	Recovery Planning
		RC.IM	Improvements
		RC.CO	Communications

Figure 2. 2 Core Elements of NIST Cyber security Framework(NIST,2018)

As can be seen in Figure 2.1, the NIST cyber security framework defines five important functions that needs to be defined in an organization for cyber security. The functions in the framework define basic cyber security activities that needs to be planned and defined at the highest management level and includes: Identify, Protect, Detect, Respond, and Recover. Further, each function has many categories. The categories are the subdivisions of the function in groups of cyber security outcomes (e.g. Asset

Management, Access Control). Categories are further divided in to Subcategories in to specific outcomes of technical or management activities.

The informative resources for NIST framework are specific standards or practices which illustrate a method to achieve the outcomes related to each subcategory (National Institute of Standards and Technology, 2014). The NIST Cyber security framework 2014, can be used not only by the infrastructure firms such as banks and financial institutions but also by the private organizations. The framework is flexible and adoptable within organization of any size that has the risk of cyber-attacks (Lei, 2014; Shackelford, 2014).

Beyer and Brummel (2015) identified the training as an important aspect of good cyber security practices, and highlighted the following important factors in providing effective cyber security training for end users of computer networks.

- The current user training operations formed by One-Size-Fits-All approach is ineffective as the training process has to be developed specifically to the end users considering their roles and responsibilities.
- Effective Methods must be developed for assessing the needs; for training and measuring the effectiveness of training process.
- An interdisciplinary team must be developed to develop the training process and foresee the implementation.
- The role of HR is important in forming the team and adopting interdisciplinary approach.

Whether a cyber security strategy is being developed at regional or national or international level, it should consider all stakeholders including the organizations both public and private, governments, and most importantly the end users who can be employees or public. Microsoft has proposed a National strategy for cyber security (Goodwin and Nicholas, 2013) by considering the following points.

- Adopting a risk based approach for national cyber security.
- Outlining clear priorities and security baselines.
- Coordinating threat and vulnerability warnings.
- Building incident response capabilities.

- Creating public awareness, workforce training, and education to ensure effective cyber security awareness implementation.
- Promote research and technology investments in cyber security.
- Structuring international engagement for building a consensus on cyber security practices.

The DETER project is a research based community that conducts research on the cyber security practices and analyses the threats and helps stakeholders developing defence mechanisms against the attacks. It provides testbed facilities for developers to test technologies against cyber security attacks. Futher, the project also provides cyber security education for organizations

Among all the framework and approaches discussed, it can be noted that there is a strong emphasis on training and awareness on cyber security. Awareness about the importance of cyber security is important as being alert enables the users to adopt measures as well prevent attacks. . In a recent survey conducted by on the students in Los Angeles, it was found that the problem with cyber security is not the lack of knowledge but the ability to use it in real world situations (Slusky and Navid, 2012). Awareness can be created through various approaches like education, promotion, advertisements etc. The awareness programs must not only focus on dispersing knowledge but also aim at making the people efficient in using the knowledge in real time situations

Most of the frameworks discussed were mostly developed for organizations. However, there was no framework found designed specifically for the end users who are public and common Internet users, who access internet for their needs and to access general services.

2.3. Lack of Cyber security Awareness

One of the reasons for increased cyber attacks is the lack of awareness about cyber security and is one of the major factors resulting in greater losses from the cyber attacks. Cyber security is a complex process that is intangible and hard to grasp, as it involves various considerations and need for various skills and knowledge to be safe from the cyber threats. At organizational level, the vulnerability to cyber attacks is

increasingly high and the management are required to create policies for effective measures and need to be easily accessible for the employees of the organization.

Bruijn and Janssen (2017) have found that complications in policy making are also an important factor in increasing the complexity of cyber security and increases the lack of awareness among the employees. They suggested that evidence based framing could result in societal and political awareness. Limited visibility, socio-technological complexity, ambiguous impact relating to strong incentives given by the affected parties to hide the impact, and the contested nature of fighting are the main factors identified by Bruijn and Janssen (2017) while explaining why the cyber security is not receiving enough attention. The study has highlighted the need for increased role of government, organizations and the public in promoting the cyber security awareness program through a cooperative and integrated strategy.

A study has found that the lack of awareness and improper training of the law enforcement officers as one of the major issues in combating cybercrime. It reflects the importance and the need for training and awareness programs among the end users. The study has also found that employed users are more aware of cyber laws compared to the non-employed users highlighting the need to raise awareness among the general public (Mehta and Singh, 2013). The Dutch government as a part of its National Cyber security Strategy stressed the importance of increasing cyber resilience through participation, encouraging private entities and voluntary participation through a bottom-up approach in formulating strategies for cyber security framework and awareness (Clark et al., 2014). These studies highlight the importance of the role of government and private organizations in creating the cyber security awareness.

In a survey conducted by Rowan and Josh (2014), it was found that the students are not fully aware of the cyber security aspects and the use of personal information online on the mobile applications, and the security risks associated with it. The study has highlighted that the current privacy policies are ineffective and emphasis must be laid on including the cyber security as the part of curriculum to prepare students for their mobile lifestyles. Education is one of the major approaches for creating cyber security awareness. However, it is important to ensure that the educators have enough knowledge and skills about cyber security concepts. Pusey and Sadera (2011)

investigated the preservice teachers' knowledge and preparedness in cyber security concepts through a survey. They have found that the participated teachers were not prepared to model or teach cyber security concepts and suggested the teachers' education through training. The various approaches in creating cyber security awareness have created confusion among the people and the educators in gaining a holistic view of the available resources and the concepts to be taught. With improper education, people may be more prone to cyber threats with unbalanced and inconsistent knowledge. To handle such issues The National Initiative for Cyber security Education (NICE) program was started with an objective of creating cyber security awareness, education, training, and workforce development (Paulsen et al., 2012). Tobey et al. (2014) used cyber security competitions for engaging users, as a part of creating cyber security awareness. They have found positive results in enhancing the skills and knowledge of the participants through competitions.

In a systematic review of approaches to assessing cyber security awareness conducted by Hayani et al. (2015), it was found education and learning processes integrated with technology applications can result in creating cyber security awareness more effectively compared to traditional approaches like education, advertisements and promotions. Mackenzie and Maged (2015) has developed an attacker centric gamified approach for creating cyber security awareness which has resulted in effective positive outcomes in the improvement of skills and knowledge about cyber security issues among the participants. A similar study conducted by Choi et al. (2013) on the employees of a government organization found that the user awareness of monitoring and cyber security activities significantly reduced the intention of misuse. It is evident from the study that the awareness about cyber security not only helps in preventing from the cyber threats but also in developing cyber ethics of using cyberspace ethically and avoiding any misuse. All the studies reviewed have found that cyber security awareness is an effective approach in order to target the threats, misuse, and attacks in cyberspace.

2.4. Importance of Creating Cyber security Awareness among Users

The users of cyber space (Public and employees) are the main actors who can play an effective role in building defensive measures against cyber-attacks. However, lack of awareness, behavioural actions, and attitudes can be the major causes in building

effective defence mechanisms. Mittal (2016) has stated that the humans are the weakest link in cyber security and suggested an integrated model to improve the user's behaviour in cyberspace by strengthening the factors having positive impact and by reducing the factors that have negative impact. In a study Whitty et al. (2015) conducted by it was found that the younger participants who scored high on self-monitoring were more likely to share passwords compared to the older people. Sharing passwords is one of the risky approaches towards ensuring cyber safety. The lack of cyber security awareness among the younger people is one of the major reasons found for adopting less secure strategy among the younger population. Therefore, awareness creation is one of the major solutions to combat cyber-attacks.

There are various approaches available for creating cyber security awareness such as web-based training materials, contextual training and embedded training. Abawajy (2012) has stated that with operating systems and programmes being more secured, the focus of the cyber-attacks is now being shifted to human elements. In his study text-based, game-based and video based delivery methods of cyber security information was assessed. The study has found that the combined delivery methods are more effective than the individual security awareness delivery methods. McKenna et al. (2015) have identified the importance of the role of users in cyber security and suggested the user-centric designs for building cyber security visualizations, where the emphasis is laid on increasing the role of users in adopting preventive measures in combating cyber threats and attacks.

Supporting the users' awareness, Ben-Asher and Gonzalex (2015) evaluated the role of users knowledge in detecting cyber-attacks. It was found that the knowledge can help in identifying the relevant cues for classifying events; facilitate integration of cues in detecting the malicious network events and increases the awareness about the cyber-attacks by assessing the events. Doyle (2017) has stated that it is everyone's responsibility to remind the users of cyberspace through formal and informal awareness programs that preventing cyber-attack starts with them. There are many ways the users can start with securing themselves from cyber-attacks. Teymourlouei (2015) has suggested selecting strong and different passwords, keeping the personal information confidential, using anti-virus softwares, avoiding public Wi-Fi's, safe browsing like disabling password reminders, blocking pop-ups, setting Internet

security zone level etc., regular software updates, using firewalls, being cautious while downloading free software (freeware), avoiding P2P (Peer to Peer) downloads, using email security, incident reporting, and most importantly regular backup for preventing the data loss as the major ways to be adopted by the users to prevent themselves from a cyber-attack.

2.5. Application based approaches for combating Cyber security and creating Awareness

There are effective measures being carried out in the field of cyber security. For example, the European Union's General Data Protection Regulation, which is yet to be launched would regulate how the companies should obtain, store, process and secure the personal data of EU citizens, and any infringements would attract a fine of up to 20 million euros. New technologies like Artificial Intelligence, Machine Learning (ML), Deep Learning are slowly being implemented in building effective security systems that can handle the changing natures of cyber threats (Sowells, 2017). Machine Learning models have been achieving effective results with more accuracy when compared to the traditional techniques in the recent years (Fdez-Riverola et al., 2007; Almeida et al., 2010). The successful implementation of ML techniques by Gmail, not just for filtering spam and phishing emails, but also other abuses like Denial-of-Service (DoS), virus delivery, and other imaginative attacks has led to the increasing dependency on ML techniques (Taylor et al, 2007).

While new technologies like Artificial Intelligence and Machine Learning techniques are used in the systems to provide cyber security, there are other applications such as cyber security education mobile application, online portals for security awareness and games-based applications are being increasingly investigated and developed for creating cyber security awareness. Cyber security is now being considered as one of the important factor in any software development process, and also in releasing the updates. Woods (2017) stated that the companies are having tough task in selecting either innovation or security while building application. However, by promoting and creating cyber security awareness and integrating this process through applications could achieve better results. As discussed in the previous sections methods like text-based, video-based, and game-based approaches through applications are increasingly being adopted for cyber security awareness (Abawajy, 2012). Among

these, game-based applications are being proved effective in creating cyber security awareness especially among the younger generation, who are new to and lack awareness in cyberspace.

The games-based learning method has several advantages. The obvious advantage is that games-based learning method provides an interactive approach to train or educate the users about a specific program. It enables the players to acquire skills and to enable thought processes in a fun and interactive way. The adaptability and flexibility of games approaches enables to design the game to suit almost every training subject possible (Boyle, 2011). A well-designed game enables the user to enter a virtual environment that is similar to the real environment and would enable the player to draw connection between the learning in the virtual environment to the real world. The games-based approach would motivate the player to move towards the goal with required actions and also see the consequences without facing penalties in the real life. Further, when compared to the traditional method of training, games-based methods are more engaging, relatively cost effective, easily transferrable to a large number of trainees, customised to each player, etc. (Trybus, 2014).

GBL is a process which uses exercises (competitive/scoring) to motivate users in learning according to specific learning objectives (Teed, 2017). Usually the games involve an interesting and interactive narrative specifically designed to meet the learning objectives. Scoring is one of the major aspects of the game which is essential for developing the interest among the users. Another important aspect is GBL environment, which must be effective and encourage the users to learn and adapt (Oblinger, 2006). Many research studies were conducted and still being conducted to analyse the impact of gaming in creating awareness about various activities in various fields. It was suggested that though GBL do not result in better performance in some instances, they do not generally result in worse performance, and may have additional benefit of a more positive attitude toward the subject of GBL. The performance in GBL can be attributed to various aspects including its environment, visual appeal, interactivity etc. (Ke, 2008). It was found that using immersive environments in the game, where all the said aspects were effectively designed would result in significant improvements in the learning aspect of the users (Virvou et al., 2005).

2.5. Essentials of a Cyber Security Awareness Program

The cyber security is a wide spectrum which integrates all stakeholders including public and private entities, regulating organizations, and the common people. Almost all the cyber-attacks directly or indirectly affect the common people. It is interesting to note that about 46% of the world population is connected to Internet. More than 90% of the data breaches are discovered by external parties and 63% of the data breaches are caused by weak, or default or stolen passwords. Humans being part of the every ICT systems are the weakest links who are prone to cyber-attacks. Humans are bound by many influencing factors including agendas, influences, beliefs, faults, priorities, and trust. It is possible that even the hardened system with efficient and effective security systems in place can be breached through simple technique like social engineering. End users in this context are Potential Defenders who must recognize observable phishing cues and lures embedded in computer-mediated messages that commonly appear in websites, e-mails and social networks. As such, they need systematic, coordinated and integrated training to understand trust decisions across these modalities (Beyer and Brummel, 2015).

About 30% of the phishing emails are opened by the users, and 500,000 attacks take place against Fortinet every minute (Australian Computer Society, 2016). Human factor causes 35% of the data breaches and it is alarming to note that there are 2,802,478,934 web users using “123456” as their password in 2014 (Crucial Research, 2014). These findings suggest that the humans or general public activities are one of the major causes which are making it easy for the cyber attackers in enforcing cyber-attacks. One of the major reasons for this situation is the rapid growing number of Internet users, and the lack of awareness about cyber security among them. In a report published by WaterIsac (2015), creating cyber security awareness and using strong passwords are the two important cyber security measures outlined in the top 10 measures. The following major people related issues in cyber security were identified by Crucial Research (2014).

- Lack of knowledge and awareness
- A relaxed culture
- Ineffective training programs
- Lack of management training

- An environment that does not encourage teamwork
- Cultural differences

Addressing these issues by organizations, governments and other organizations can effectively improve the cyber security aspects among the people. As discussed in previous sections Teymourlouei (2015) has suggested various methods such as backup, using anti-malware program, creating strong passwords etc. using which the people can monitor, diagnose, and prevent any cyber-attack. Moreover, savvy users likely require different training content than naïve users. They need training tailored to their particular learning needs in order to make smart decisions in cyber space (Beyer and Brummel, 2015). For the end users who have no or very few awareness about cyber security, the awareness programs must be developed with the information about basic security measures. Similarly, for end users who have some knowledge, the awareness programs must be developed considering their knowledge levels and the new threats arising.

Baig (2017) has suggested 10 security tools for online protection in the fields of encryption, vulnerability scanning, penetration testing, and anti-spymail security. The use of Anti-Virus, Anti-Spyware, and Other Protective Software is promoted through various methods as a part of raising cyber security awareness (Bambenek, 2017). However, the threats keep changing and the old software security tools may not recognise the new threats emerging daily. To tackle such issues, regular updating of security tools must be done. The software updates patch vulnerabilities and makes the tool ready to detect the new emerging threats (Mangus, 2017). The importance of software updates is recognised as an effective approach by the people in various studies (Dhananjay et al., 2016; Bada and Sasse, 2014; Williams et al., 2017).

However, it is also essential to create awareness about steps to be taken in the event of an attack. Backup is one of the important strategies to prevent the data loss in the event of a cyber security attack. The importance of data backup is recognised by many organizations and has adopted effective backup strategies to prevent any damage from cyber-attacks (Abrams, 2017). Additionally, various studies suggested data backup is an effective measure to prevent any loss or damage caused by a cyber-attack (Ismail et al., 2016; Xia et al., 2014; Brinda et al., 2015).

After the attack, one of the most important step is to report the incident, so that the necessary actions can be taken by the responsible authorities to prevent any further damage caused by the cyber-attack. There are various aspects which need to be considered in the process of incident reporting from the perspective of end users like who should they report to? How should they report? And how to assess if they have come across an incident that need to be reported? There are few organizations formed specifically for this process like Computer Emergency Response Teams (CERTs) that have operations across the globe (Bada et al., 2014). The end users can report to such organizations or any other organizations they may aware of at their regional or national level. While reporting incidents and disclosing it can help in preventing damage Johnson (2014) argues that it is essential to learn as much as possible from the previous cyber-attacks without disclosing information that might encourage future attacks, which is an important aspect to be considered. This makes incident reporting a complex task as how the reporting process should be established and how the secrecy must be maintained. Therefore, it is essential to have a clear and effective strategy on incident reporting and the people should be made aware of it and the awareness programs must encourage them to be responsible in reporting the incidents.

2.6. Summary

This chapter has reviewed various aspects related to cyber security, the practices adopted in cyber security, cyber security awareness, the role of users in combating cyber-attacks and the challenges involved, and the use of applications for cyber security awareness, and the public security threats among the end users. It was identified that the cyber security requires collaborative strategy among the public, private and other regulating organizations along with public to target rising cyber threats. Few studies have found that the human factor as the weakest link in combating cyber-attacks, which needs to be enforced with the responsibility to combat cybercrime through effective awareness programs. The review has found various applications used for creating cyber security awareness among which gaming applications proved to be effective. The public security threats reviewed has found various attacks including malware, phishing, freeware, ransomware etc., and the steps to be taken by the public have been reviewed. These include backup, installing security programs

like antivirus, incident reporting, creating strong passwords, regular updating of the applications etc. These techniques are used in assessing the awareness levels of the participants in Saudi Arabia, and the outcomes are explained in the next chapter.

Chapter Three

Cyber Security in Saudi Arabia

3. Cyber security in the context of Saudi Arabia

Saudi Arabia is one of the fastest developing countries in the Middle East region, which has been using the technology as an important resource in every aspect of development. The use of Internet technologies can be found in public sectors and other institutions like schools, hospitals, and other private organizations. It was estimated that there are more than 18 million Internet users with 65.9% population penetration of Internet, and more than 12 million Facebook users (Miniwatts Marketing Group, 2015; W3C, 2014). Social networking is one of the highly involved aspects of Internet usage with Facebook and Twitter being popular in the region. Additionally, about 39% (12% of the total population) of the adult Internet users buy products online and pay online for services (CMO Council, 2015). The country is the second largest E-commerce market in the Middle East region with stats accounting to $520 million (CMO Council, 2015).

There is a rising trend observed in the cyber-attacks in Saudi Arabia. In 2013, a series of attacks targeted several government websites which crashed various websites including the interior ministry website. The business organizations and the government agencies are facing huge challenges in the country with the increase in sophisticated and innovative cyber-attacks launched by hacker activists and foreign governments (Reuters, 2013). Another cyber-attack took place in 2012 targeting Saudi Aramco, an oil and gas company and one of the major sources of income to the Saudi government, resulting in damaging about 30,000 computers, using Shamoon malware, which is considered to be one of the most destructive cyber-attacks targeted at a single company (Bronk et al., 2013). According to al-Hussein (2017), there were 60 million cyber-attacks witnessed by the Saudi Arabia in 2015, which is expected to increase rapidly in the future, as the hackers are changing their strategy on a daily basis. The National Cyber Security Centre (NCSC) said that a new advanced cyber-attack using Powershell malware through email phishing was targeted at Saudi government agencies causing much disruption in the services (Bodhani, 2017). Similarly, Saudi's General Entertainment Authority (GEA) was also been a victim of cyber-attacks in 2017 in Sausi Arabia (Shamseddine and Kalin, 2017).

Though Saudi Arabia has seen a rapid increase in Internet usage and cyber-attacks in the recent years, there are no proper country specific legislations placed in terms of

cyber security. The country is follows European Network and Information Security Agency (ENISA) for formulating National Information Security Strategy (ENISA, 2015b). With respect to technicality, it has not formulated any standards and framework for accreditation or certification of public sector professionals (ITU, 2015). There is no specific policy or roadmap for governance for taking organizational measures, and no framework developed for intra-state, intra-agency, and public sector partnership cooperation in the process of cyber security incident management (ITU, 2015). However, in the international spectrum, it is the member of ITU-IMPACT, and participates in related programs including APWG, OIC-CERT, The Honeynet Project (ITU, 2015). To enhance cooperation and awareness, the country conducts Cyber Defence Summit, which focuses on incident and knowledge sharing and network platform to address cyber security and the stakeholders include government agencies, private companies in banking, oil and gas, and other industries etc. (CDS, 2015).

Moreover, Saudi Arabia has a long way to go in developing and implementing the cyber security strategy, as the country mostly relies on international agencies in this aspect. Therefore, there is a need for extensive research studies towards enhancing cyber security and awareness in the country.

As the reliance of Saudi citizens on Internet for various activities increases, the issues of cybercrime and providing cyber security also increase. Therefore, it is essential for the Saudi government to adopt a national policy to tackle the issues of cybercrime. To facilitate towards this goal, it is important for extensive research studies to be carried out towards enhancing cyber security and awareness in the country.

3.1 Cyber Security Awareness Survey

This survey aims to investigate and collect information about the general perception of cyber security awareness among citizens in Saudi Arabia. As there are no prior studies in relation to the identification of cyber security awareness among Saudi Arabian people, and socio-cultural, economic and political diversification and difference between Saudi Arabia and other regions, it is essential that there is a need to identify the level of cyber security awareness in order to develop effective security solutions. There are various approaches for analysing the level of cyber security awareness; however, the information need to be reliable, accurate, and can be

compared and analysed. The review of previous studies, government reports, articles and other publications regarding the awareness levels of the people may be few important sources. However, the time of data collection in different articles may be different and this may create ambiguity in data analysis. Qualitative approaches such as interviews may be an effective approach for determining the level of awareness among the people, but it would take enormous time to gather responses from a large set of sample population. Considering these aspects, an online questionnaire-based survey could be an effective approach for collecting the data about the level of awareness among the Saudi population, which can be reliable, accurate, and can be analysed scientifically and objectively (Laaksonen, 2018). In addition, it is a cost-effective method that can collect large amounts of data within a short time (Allen, 2017). The data collected can be quantified and analysed to identify various relevant issues related to the cyber security awareness. Therefore, a questionnaire based online survey can be an effective tool in this aspect to reach large section of population, which will seek to understand people's level of awareness concerning cybercrime, cyber security awareness, and how well equipped they are to combat cybercrime and its related threats. In addition, it will establish whether any of the participants have been a victim of cybercrime, and, if so, whether or not they reported the crime to the relevant authority.

3.1.1. Purpose of the Survey

The main objective of the survey is to raise awareness on cyber security by collecting the following information:

a) Understand/assess the current level of cyber security awareness.
b) Understand/assess current cyber security practices.
c) Understand/assess knowledge about the threats and sources of cybercrime knowledge and where this information was obtained.
d) Identify participants' views concerning the challenges of combating cybercrime.
e) Identify participants' views concerning their role in combating cybercrime.
f) Understand participants' level of awareness and what they do if they become a victim.

3.1.2. Research methods

A quantitative research methodology is adopted in this research as it was the most suitable approach to understand the level of cyber security awareness and knowledge amongst users. The quantitative approach enables identifying the level of awareness and knowledge amongst the participant and is often used to verify different ideas using large number of participants (Fowler, 2014). An online survey approach is used to carry out the quantitative research. Online survey is a convenient approach as it allows participation of variety of people in population which is often difficult to access by traditional methods such as face to face interviews. Further, participants from different locations and background can be easily requested to take part in the survey.

3.1.3. Methodology of the survey

This survey collects data from participants in the Kingdom of Saudi Arabia. The survey is designed to provide answers to the following questions:

- What is the current level of Cyber security awareness among citizens?
- What are the current cyber security practises in use?
- What is their level of cybercrime knowledge?
- Where do they get their knowledge about cybercrime?
- What do they think their role is in combating cybercrime?
- What do they think are the challenges in combating cybercrime?
- What do they think about application-based cyber security awareness which can be used on their devices to help raise their awareness and understanding of key cyber security;
- What they do if and when they become a victim of cybercrime?

The research involved one survey. The survey was designed to measure perceptions and knowledge among the general public. Various statistical analysis techniques are used in analysing the survey results. The Pearson correlation coefficient (r) is used to measure the strength of a linear association between two variables. The value of 'r' can range from +1 to -1. If the value of r=0, it can be analysed that there is no association between the two variables. If the value of 'r' is greater than 0, it indicates a positive association; i.e. if the value of one variable increases, then the value of another variable also increases. If the value of 'r' is

less than 0, then it indicates negative association; i.e. if the value of one variable increases, then the value of other variable decreases (Welkowitz et al., 2006). The Pearson correlational coefficient for variables X and Y are calculated using the following formula, where n is the number of entries considered in each group and $\bar{X}$ and $\bar{Y}$ are the means.

$$r_{XY} = \frac{\sum_{i=1}^{n}(X_i - \bar{X})(Y_i - \bar{Y})}{\sqrt{\sum_{i=1}^{n}(X_i - \bar{X})^2}\sqrt{\sum_{i=1}^{n}(Y_i - \bar{Y})^2}}$$

This technique can be used for comparing various variables and the relationship between them. For example, the cybercrime experience and the applications used by the participants can be compared and analysed. It will help in determining how both variables are associated. Usually, by using security applications, the experience of cyberattacks must be reduced. However, this may be analysed by comparing the data for both variables, and various reflections can be presented.

The standard error is another metric used in the data analysis, which represents the accuracy with which a sample represents a population. It is the deviation of sample mean from the actual mean of a population and termed as Std Err. It indicates the reliability of mean. A small Std Err indicates that the sample mean is more accurate and reflects the actual population (Welkowitz et al., 2006). It is calculated by using the formula

$$\sigma_M = \frac{\sigma}{\sqrt{N}}$$

where σ is the standard deviation of the original distribution and N is the sample size. These tests validates the data and its reliability; and can also be used for comparing various variables in the data analysis.

3.1.4. The survey of the general public

The survey consisted of 22 questions and is organized into four sections;

— **Section A: Focus on demographics:**

This section contains 8 general questions about the participants, such as their gender, age, education, type of digital device(s) and connectivity service used, and the purpose of using Internet.

— **Section B: Cyber security practices**

This section contains 5 questions about general cyber security practices. The questions will investigate participants' level of knowledge concerning computer operating systems and security solutions. The survey questions also seek to understand the level of awareness of each participant concerning digital device security, cyber threat awareness, password security levels, data backup, and the use of cyber security tools and applications. In addition, this section reports the level of confidence of the participants on the privacy of information obtained through social network and through Internet via a personal Wi-Fi connection.

— **Section C: Cybercrime awareness**

This section contains 7 questions related to citizens' knowledge of cybercrime and awareness of its risks. They examine the behaviour of Internet users in the field of cyber security, whether they have experienced a cybercrime or been a victim of it, the level of anxiety felt about cybercrime, and who citizens would contact if they experienced or were a victim of it. Questions about the sources of awareness and knowledge cover all participants, while the rest of the chapter is based on the attitudes and experiences only of those who have ever used Internet.

— **Section D: Incident reporting**

This section contains 2 questions to identify peoples' awareness of whether they have been a victim of cybercrime, their knowledge towards reporting of the crime, and also to investigate the challenges of reporting cybercrime incidents.

3.1.5. Validation of the survey

A pilot study is a rehearsal to the main study to be conducted in the research (Milne, Orbell and Sheeran, 2002; Compeau and Higgins, 1995; Sonderegger and Sauer, 2010). It helps the researcher to determine whether the study and the approach used to conduct the study would lead to reliable and valid results. If any problems are encountered during the pilot study, then suitable adjustments are made to the methodology and approach before conducting the main study. A quantitative analysis, based on Likert style questionnaire approach was adopted to evaluate the game design framework described in this study .

The first pilot test for the survey was conducted on 29th April 2015 with a group of Saudi citizens, particularly with PhD students. The survey outcomes were collected by distributing hard copy versions of the survey to the participants and were asked to answer them on the provided copy.

Twelve participants took part in the survey. Eight of the 12 participants were from the Centre for Security, Communications and Network Research (CSCAN) and the remaining five were from different educational backgrounds in the areas of business, Biology, Statistics and Mathematics, education and Computing. Therefore, efforts were made to ensure that the pilot survey had participants from diverse backgrounds so that it could be verified whether the survey was easily comprehensible for diverse participants. For participants from Security, (CSCAN), their comments were taken in real-time whilst they undertook the survey. Other participants were asked to test the survey using their personal computer, in their own time. A common feedback across most participants was that they preferred a shorter and simpler version of the survey and found the pilot survey to be lengthy. This feedback was incorporated for our study and the total number of questions were reduced from 38 to 22.

Each participant took about 22 minutes to complete the survey. Overall, the participants were able to understand most of the questions except for a few of them who experienced difficulties in answering them. Some respondents had difficulties in answering the questions due to the use of cyber security jargons in the questions such as backup, cryptography and firewall. This comment was considered and the survey

was modified by providing definitions to all cyber security jargons to enable participants to answer the question accordingly.

The next pilot testing phase was conducted by translating the survey into Arabic language and by distributing hard copy versions of it to the participants. This survey was completed by 16 participants. Four of the participants were from the Centre for Security, (CSCAN) security background, and the remaining twelve were from different educational backgrounds. This again ensured that participants not specifically working in the computing area could understand the questions in the survey. The non-computing background participants were from backgrounds including Medicine, Coastal Engineering, Computing and Arts. Again, the participant composition tested whether the survey could be understood by people from different backgrounds. For participants from the Centre for Security, (CSCAN) security background, their comments were taken in real-time whilst they undertook the survey. Other participants were asked to take part in the survey on a hard copy version of the survey. Similar to the previous survey, most of the participants commented about the length of the survey.

3.1.6. Filtering mechanism

Questions One to Nine were designed to collect demographic information about the participants of the questionnaire, such as gender, age, education along with the general information about their skill level of using Internet and digital devices, type of digital devices being used, type of connectivity services used to access Internet, and type of activities on Internet that they engage in (in this question also needed to know if the respondents used public Wi-Fi. This data provided background knowledge about each participant and was used to further analyze the impact of background on their responses. The target respondents are those who are 18 years old and above. The age gap was then divided into ten years blocks.

Question 10. Some of the most commonly used security tools and applications for laptops, Tablets, mobiles, etc. are given below. Select which of these you have used on your digital devices. Tick all that apply.

Question 11. Some security practices are described below. Please choose your common reaction for each practice.

Question 12. What digital devices do you have Internet security on (e.g. anti-virus)?

Question 13. If you use Internet security (e.g. anti-virus), is this kept up to date in terms of threat filters and signatures?

Questions 10 – 13 allows to understand what the common cyber security practises are applied by the participant. Question 10 would help to get information about the commonly used tools and applications for cyber security processes which include various tools such as anti-virus and firewall and some practises such as software update and backup. Question 12 asks on what devices the security tools are used and question 13 asks the participants whether their security tools are regularly updated.

In question 11, security practises were listed and the participants asked to choose their actions from options: always, sometimes, and never. The practises listed would generate knowledge about how cautious people are while interacting with the cyber space and also help identify the most commonly followed security practises by the participants. Since the use of social networking websites is popular amongst the public, two questions were created in the Table aimed at the social networking activities of respondents and their awareness of divulging personal information over Internet. Also establishing security applications/controls that respondents were using. Lists of the security terms were based on a combination of these from various sources. Each item was based on the literature (i.e. these are the standards of safety online).

Question 14. How do you keep yourself updated about cybercrime? Tick all that apply

Question 15. What is your opinion of each of the following statements? Select the appropriate response for each.

Question 16. There are several activities that constitute cybercrimes. How often have you experienced or been victim of the following situations? Select the appropriate response for each.

Question 17. Some of the most common cybercrimes are presented below. What is your opinion of each of the following statements? Select the appropriate response for each.

Questions 14-17 are about understanding the awareness participants have about cybercrime. The first question in this regard was to know what their “source” cybercrime knowledge is. It helps us to identify the important sources of information about cybercrime. Question 15 is framed in order to understand the level of cybercrime knowledge participants have. They are asked to give responses to several statements which intend to understand their awareness about topics such as precautions to be taken to avoid vulnerability, the threat and vulnerability to their personal information online, legal aspects of cybercrimes and others. The opinions are collected based on how strongly they agree/disagree with the statement. Similarly, question 16 intends to understand their level of knowledge about cybercrime by asking them to identify how often they have encountered cybercrimes. The question also would help to understand whether the participants were able to identify the activities as cybercrime or not. Question 17 also lists common cybercrimes and asks the participants how much concerned they are about encountering or being victim of such cybercrimes.

18. What do you feel about the threat of cyber crimes in the future?

19. Considering each of the following parties, please rate the extent to which you believe they are responsible for raising awareness of cyber crime

20. What do you think the role of the government should be in combating cybercrimes? Please tick all that apply

21. Application-based cyber security awareness refers to an application that can be used on your device/s to help raise your awareness and understanding of key cyber security issues (e.g. cybercrime prevention, data protection, virus protection, safe social networking, password security, device security, web browser security, email security, and more).

With this in mind, please choose your most appropriate response to the following statements:

The questions from 18 to 21 are about the participants concern about cybercrimes and its potential impact. Question 18 tries to understand the concern or “fear” participants have about cybercrime future and whether they believe if it will be combated in the

future. Similarly, extending question18, in question 19, the participants are asked who they consider are more responsible for tackling cybercrime. The options include whether the user itself or if the responsibility be shared by multiple parties including the government. Question 20 helps us to understand the participant response about how much they think the government must take actions and frame laws about combating cybercrime. The options range from no role to enacting stricter laws and monitoring. The responses will help us understand what the people expect the government to do in combating cybercrime. In question 21, the participants are asked if they believe an application which provides information about cyber security be useful to them. They are asked to rate various statements based on whether they consider such an application to be useful to them or not.

Q 22. Have you been a victim of cybercrime? (E.g. lost data or email account, device infected with virus or spyware, stole your picture/s or digital device/s).

Question 22 The final question is about incident response. Here, the focus is to understand what actions the participants have taken whenever they have been a victim of a cybercrime. The responses to this question would help us to understand whether people consider cybercrime incidents seriously and take action or not. The question is subdivided based on the response the participants give to the main question. If the participant say he/she has been a victim of a cybercrime, they will be asked if they have taken actions against it by reporting or not. If they have not been a victim ever, then they will be asked what actions they would take in case they encounter an incident.

3.1.7. Survey findings

This research aims to examine cybercrime and cyber security in the Kingdom of Saudi Arabia. Using a questionnaire Saudi participant from the general public have answered several questions enquiring about:

- Levels of Internet use;
- Current level of cybercrime awareness among *citizen* at KSA;
- Current cyber security practices their do have;
- Level of cybercrime knowledge; Attitude towards cybercrime;

- Their role can be in combating cybercrime; Challenges in combating cybercrime;
- What do they think about application-based cyber security awareness which can be used on their devices to help raise their awareness and understanding of key cyber security;
- What do they do when they become a victim?

The results will be reported in three main sections, the first of which will include demographic details and general information about Internet use and digital devices used. This is followed by a section aiming to report findings with regard to cybercrime awareness while the third and main section will be concerned with participants' security practices.

Section A: Participant Demographics

This section included general demographic details including gender and age of participants along with their level of qualification. Internet and digital devices level of use and skills were also enquired while asking about the general purposes of Internet use. It is essential to determine such information as it might have impact on cyber security and related topics in this study.

1- Gender and Age

Overall 629 Saudi participants took part in this study, of those participants there were 440 male participants (70%) and 189 female participants (30%). Participants' age was divided into four categories where 85% of the participants were below the age of 40. As can be seen in the graph below, 268 participants had an age between 18-29 years (42.6%) and 267 participants had an age between 30-39 years of age (42.4%). Only 78 participants had an age between 40-49 years (12.4%) and finally 16 were 50 years old or more (2.5%).

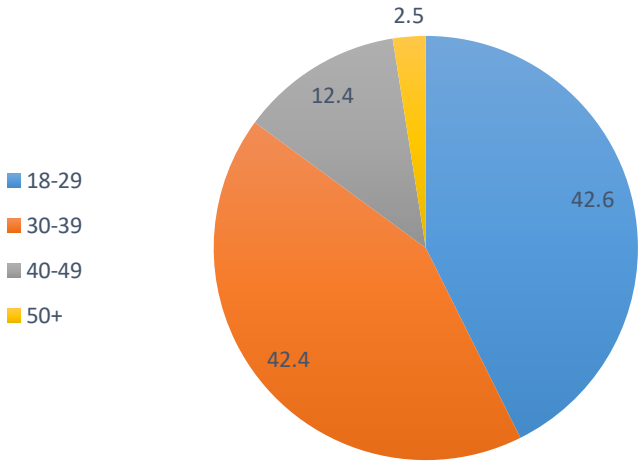


Figure 3.1 Percentages of participants across age groups

2- Level of Qualification

The questionnaire also asked about the highest qualification achieved by the participants. Their education varied three categories where 325 participants (51.7%) had an undergraduate degree and 197 participants had postgraduate degrees (31.3%) only 107 participants had a lower level of education in the form of school level (17%). Overall it can be observed that 83% of the participants had qualification at undergraduate level or higher.

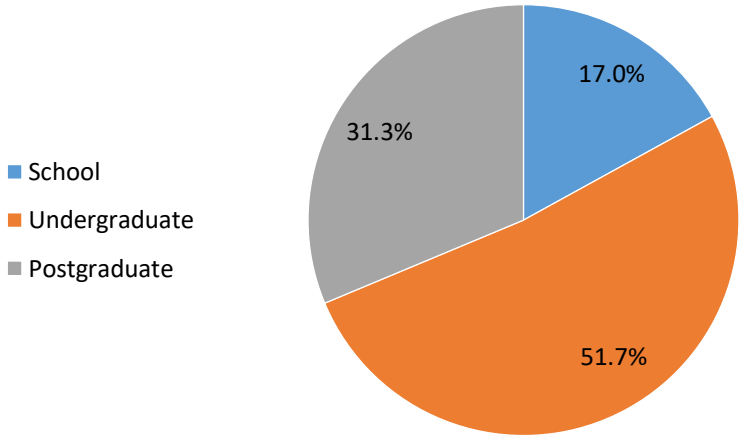


Figure 3.2 Percentages of participants' educational levels

3- Frequency of using Internet

The frequency of using Internet or Internet related devices was assessed using three categories (frequently throughout the day, once or twice a day and less frequently). A total of 569 participants (90.5%) stated that they use Internet or Internet related devices frequently throughout the day while the rest 60 (9.5%) stated that the use it once or twice a day. No one stated that they use it to lesser extent. These results reflect high internet usage which may come along with the high risk: prone to cyber-attacks if the safety measures are not practiced. As identified by Mittal (2016) humans are the weakest link in cyber security and were found to be more prone to threats if necessary, security mechanisms were not implemented. Similarly, Whitty et al. (2015) found weak passwords as one of the common practices adopted by internet users.

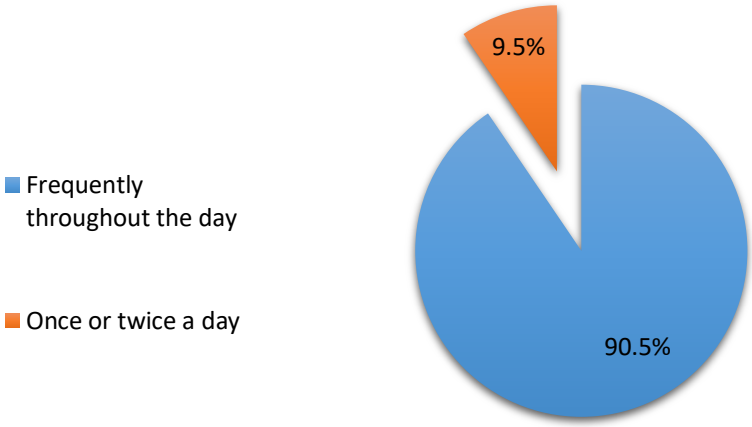


Figure 3.3 Percentages of participants' use of Internet

4- Internet/ Digital devices skills level

To determine Internet/digital devices skill level participants were asked to tick one of three options: beginners/basic, intermediate or expert. 304 participants (48.3%) stated that they have an Intermediate skill level in using Internet or digital devices (e.g. able to install moderately complicated software, make modifications to the settings of the computer, and have a good understanding of hardware and software). This was followed by 246 participants (39.1%) who stated that they have a Beginner/Basic skill level (e.g. start devises, go to specified web page, use Word, use social media). Finally, 79 participants (12.6%) selected the expert skill option (e.g. IT practitioner, computer engineering, database administration, network engineering). These results indicate that only very few participants have good knowledge levels about internet and related devices, as majority of the participants consider themselves to be intermediary

or beginner in terms of internet skills possessed, which may lead to various risky operations such as not backing-up data, using weak passwords, accessing internet from public hotspots for secured operations such as online banking etc. Therefore, it can be assessed that there is a need to increase the internet and technology education and awareness.

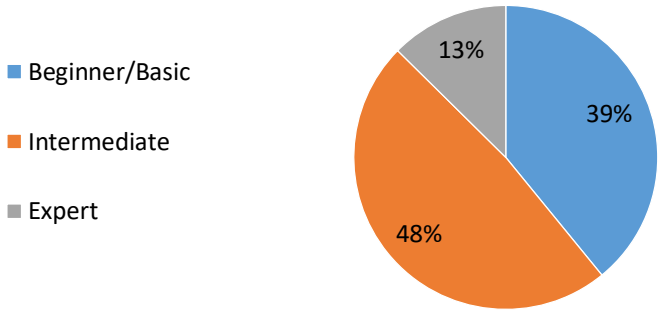


Figure 3.4 Percentages of participants' across skills' level

5- Digital devices used regularly:

Participants were asked to state which of four digital devices they use regularly. Here participants could select multiple devices. In doing so it was shown that 568 (90.3%) use Smart phones while 377 (59.9%) stated that they use laptop computers. 210 (33.4%) of the participants stated that they use desktop computers while 173 (27.5%) stated that they use Tablets regularly.

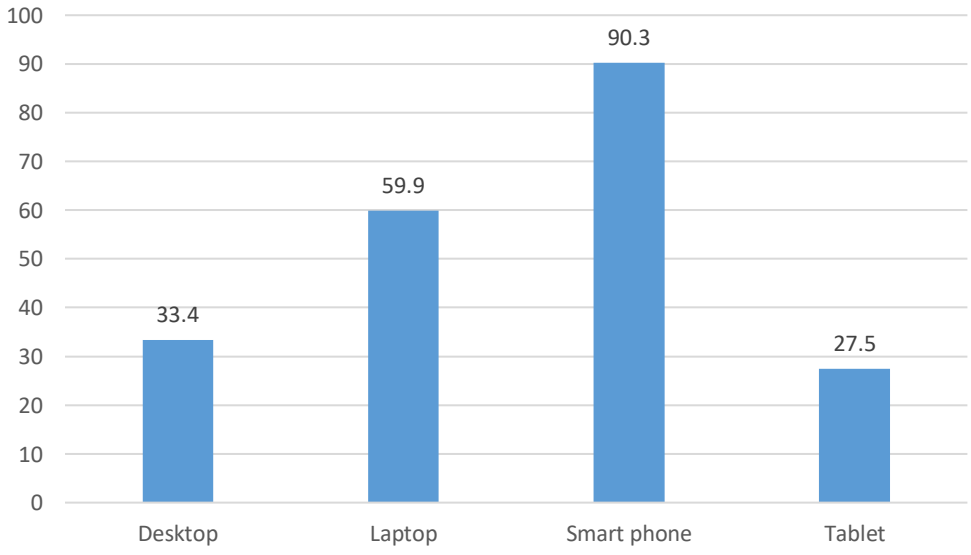


Figure 3.5 Percentages of digital devices used regularly

6- Connectivity services used:

When asked what type of connectivity services participants use in their daily activities they 515 (81.9%) stated that they use Private Wi-Fi (e.g. in your home) while 437 (69.5%) explained that they use Mobile/cellular phone network (e.g. 3G/4G). 155 (24.6%) stated that connectivity service used is Public Wi-Fi (e.g. in coffee shop). 86 (13.7%) of the participants state connectivity comes in the form of Broadband (wired). Only 3 (0.5%) participants stated that they do not know the type of connectivity service they use. There are considerable numbers of participants using public Wi-Fi, which can be associated with security risks, as it is an open network. Though the large number of users using secured internet connection, the risk of security attacks can still be a concern based on how and what sources they access.

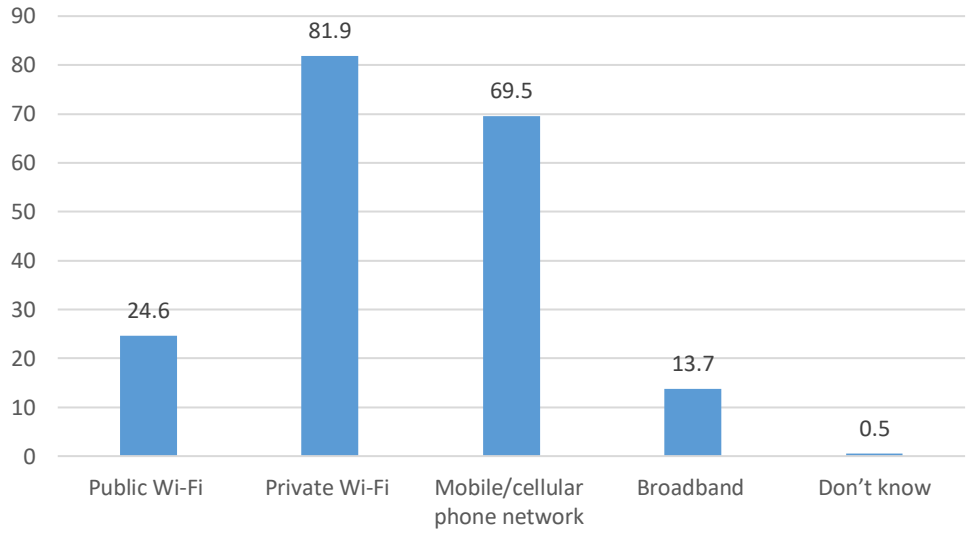


Figure 3.6 Connectivity services used by participants

7- Purposes of Internet use

Internet has many purposes and participants in this study were asked to select one or more of 6 purposes. The majority of 527 (83.8%) stated that they use Internet for social networking, while 481 (76.5%) selected that they use it for education or information seeking (news, articles). 413 (65.7%) of the participants showed that they use Internet for government services, online banking, e-commerce, etc. 385 (61.2%) stated that Internet is used for online Communication (e.g. email, Skype, etc.). Furthermore 195 (31%) used Internet for entertainment purposes (e.g. playing games). Finally, 156 (24.8%) appeared to use Internet for professional reasons (e.g. remote access VPNs).

Entertainment and communication, social networking, and information seeking are associated with high security risks such as malware, social engineering, viruses respectively. These are the few major purposes for which majority of the participants are accessing internet. As, the recent security attacks are targeting government and other private companies (Reuters, 2013; Bronk et al., 2013; Al-Hussein, 2017; Bodhani, 2017; Shamseddine and Kalin, 2017) in Saudi Arabia, accessing these sources also could increase the risk of security attacks. The purposes of internet usage in Saudi Arabia, thus reflect the high risk of cyber security attacks.

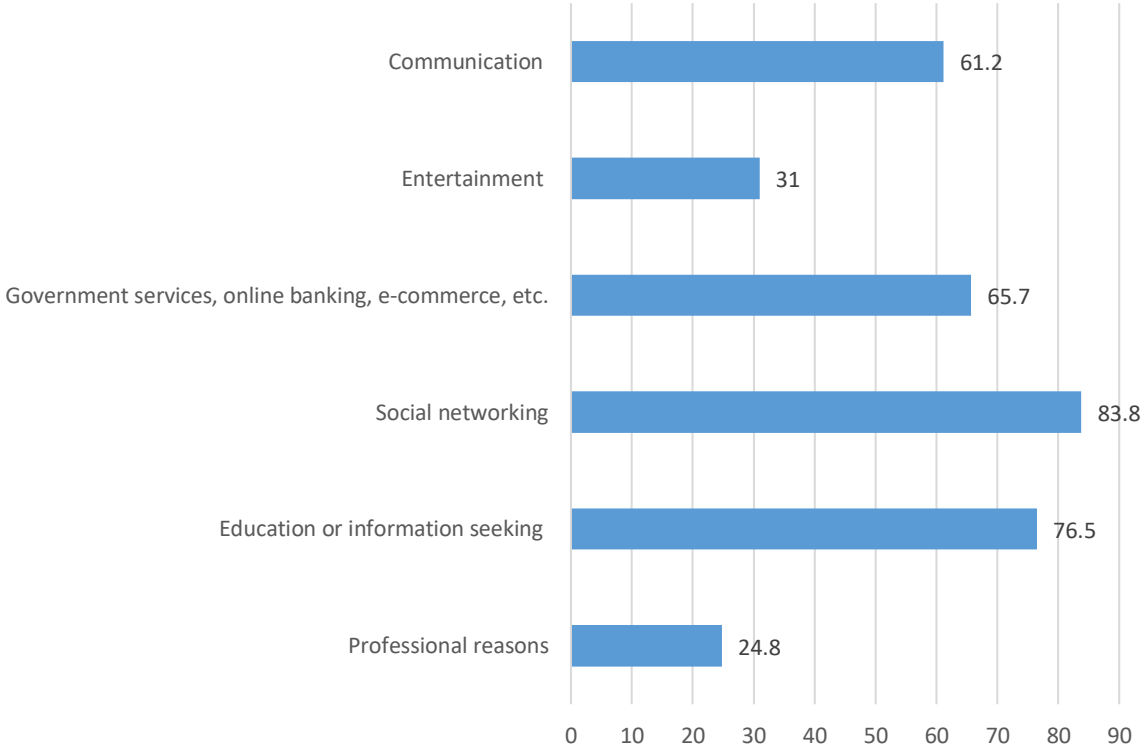


Figure 3.7 The purposes of Internet use

Section B: Cyber Security Practices

1- Operating systems used desktop/laptop and mobile phones

As for the operating systems used participants were asked to state which they use on their desktop or laptop computer. In doing so it was evident that the majority of 188 (29.9%) participants use Windows 7 and 161 participants (25.6%) use Windows 8. In the third place came Windows 10 which was used by 106 (16.9%) participants, this was followed by 93 (14.8%) participants who use Macintosh and 52 (8.3%) who use Windows XP. Only 15 (2.4%) used Linux operating system and 6 (1%) used older Windows versions. 7 (1.1%) stated that they do not know what operating system they use on their computers. Large number of participants using older versions of operating systems including Windows XP/7/8 etc., which may have many security drawbacks. Without having good antivirus and malware protections, these users may be prone to security attacks, when they use older versions of operating systems.

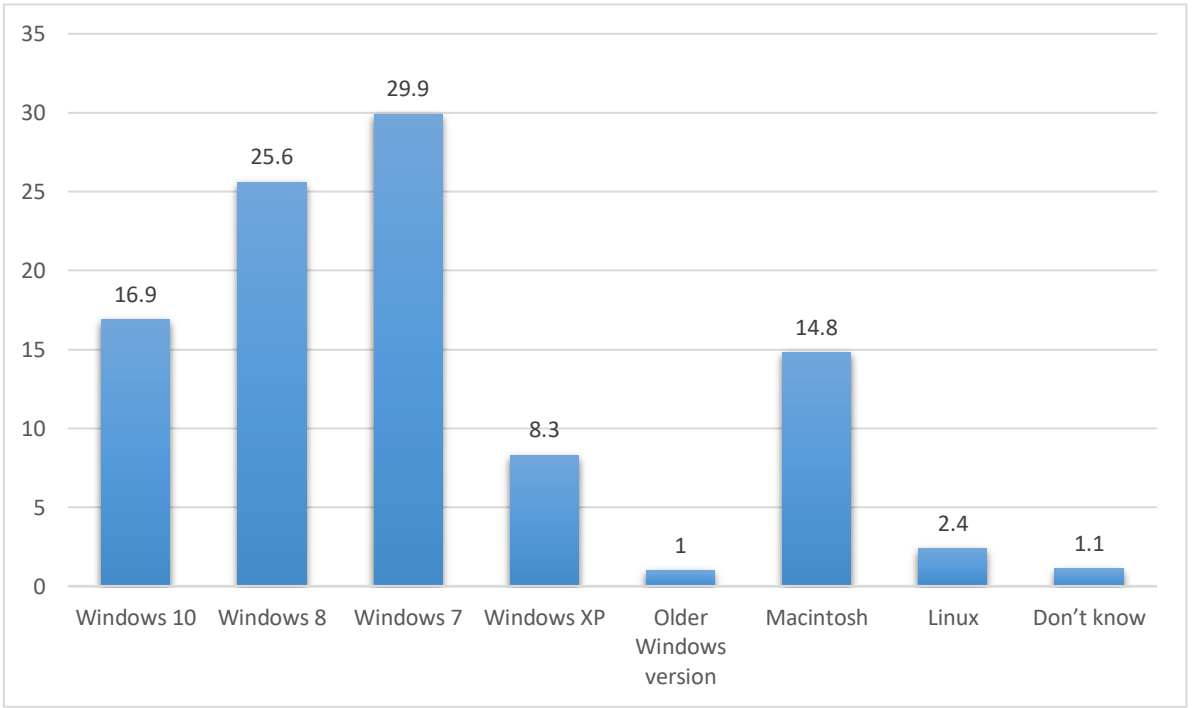


Figure 3.8 The operating systems used on computers

As for the operating systems used on mobile phones, participants were asked to select out of 6 options. The majority appeared to use Android operating system as it was selected by 268 (42.8%) of the participants followed by 266 (42.3%) who used iOS. On the other hand other operating systems were used much less, 77 participants

(12.2%) used Windows phone operating system while 29(4.6%) used Blackberry. Only 3 participants (0.5%) used Symbian operating system. 42 (6.7%) of the participants did not seem to know the mobile operating system they use. Similar to the Computer operating systems, majority of the participants are using open sourced OS such as Android, which may increase security risks. However, there are considerable number of participants using iOS, which is comparatively secured, but limited in the freedom of accessibility of various applications and ease of use compared to Android phones. The Android and other mobile operating system users were about 60%, which can be prone to various security threats if they do not practice safety measures such as installing anti-malware software in mobiles, frequent updates and backups etc.

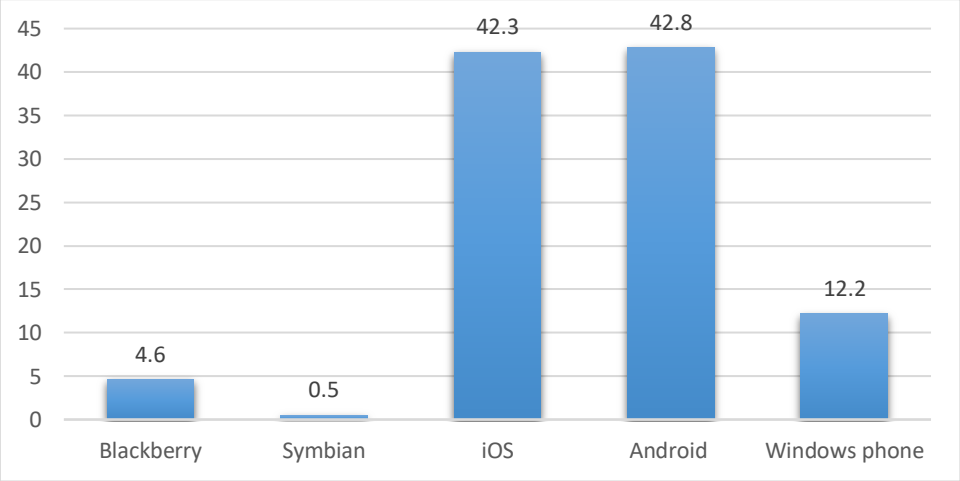


Figure 3.9 The operating systems used on computers

2- Commonly used security tools and applications:

This section is concerned with the security tools used on digital devices (laptops, Tablets, mobile phones etc.). They were asked to select which of 7 options tools they use on their digital devices. Participants were asked to tick all suitable options. In doing so it was found that the majority of 391 participants (62.2%) use Anti-virus tools and 297 (47.2%) participants use Authentication tools (e.g. password, PIN). Also, 244 (38.8%) participants used Software updates for security while 241 participants (38.3%) use Backup tools. 215 participants (34.2%) stated that they used Firewall. Encryption was used by 54 (8.6%) participants and equally 54 (8.6%) stated that they use no security tools. Almost all the security practices have received lower responses except Antivirus, indicating poor awareness levels among the participants regarding the

various security measures. Only Anti-Virus is being used as a safety feature by majority of the participants, while rest of the approaches were not effectively practiced indicating poor awareness levels and lack of knowledge.

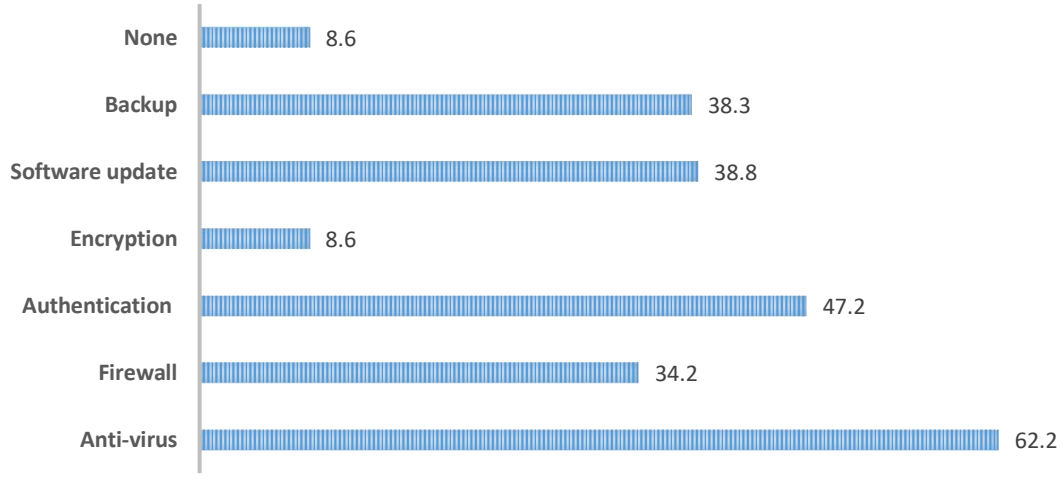


Figure 3.10 Commonly used cyber security tools and applications

3- Security practices are described below:

Participants were given 13 items to rate with regard to cyber security practices. As can be seen in Table 3.1 below answers were categories into three categories, never, sometimes and always. By looking at the answers in the always category it is evident that the main security practice to receive the highest percentage is “I am aware of the danger when clicking on banners, advertisements or pop-up screens that appear when surfing Internet” (63.6%) followed by “I regularly install software updates” and thirdly “I give due attention to privacy settings on my social media account(s) (e.g. Facebook) (40.9%). Items such as “I read the terms and conditions carefully before using any website” (18.9%) “I feel safe when using public Wi-Fi” (18.8%) appeared to be the least practiced among the security practices by looking at the “always” answer. Majority of the participants based on the results are adopting poor security practices such as not changing passwords regularly, not updating the system frequently, not maintaining a back-up, frequently opening links in social media posts etc. In addition, almost 67% of the participants responded that they feel that their devices are not safe, which is one of the major concerns of security among the participants.

Table 3.1 Security practices and participants' answer on three categories based on frequency and percentages

Security practices	Never	Sometimes	Always
I check the legitimacy of a website before accessing it	115	311	203
	18.3	49.4	32.3
I create a password that contains my personal information (e.g. last name, date of birth)	196	248	185
	31.2	39.4	29.4
I am aware of the danger when clicking on banners, advertisements or pop-up screens that appear when surfing Internet	50	179	400
	7.9	28.5	63.6
I give due attention to privacy settings on my social media account(s) (e.g. Facebook)	149	223	257
	23.7	35.5	40.9
Social media services protect my personal information	187	349	93
	29.7	55.5	14.8
Security practices	**Never**	**Sometimes**	**Always**
I read the terms and conditions carefully before using any website	258	252	119
	41.0	40.1	18.9
I change the passwords of important accounts (such as online banking) frequently	215	280	134
	34.2	44.5	21.3
I feel safe when using public Wi-Fi	239	272	118
	38.0	43.2	18.8

I feel my digital devices (computer, smartphones) has no value to hackers, they do not target me	125	326	178
	19.9	51.8	28.3
I regularly install software updates	38	248	343
	6.0	39.4	54.5
I am careful about clicking on links in an email or social media post	226	260	143
	35.9	41.3	22.7
I keep sensitive data in my device/s	184	263	182
	29.3	41.8	28.9
I create backup copies of my device/s data	130	281	218
	20.7	44.7	34.7
I feel that my device/s are secure	67	356	206
	10.7	56.6	32.8

4- Digital devices and Internet security:

Further information were gathered with regard to what digital devices participants have Internet security applied on. It was evident that laptop computers were most secured, this was answered by 443 (70.4%) participants. This was followed by smart phones where 251 (39.9%) participants stated that they Internet security on. 183 (29.1%) of the participants stated that they have Internet security installed on their desktop computer while 66 (10.5%) have Internet security installed on their Tablets. 41 (6.5%) of the participants stated that they have no security on any and finally 32 (5.1%) stated that they do not know if they have Internet security on any of the digital devices they have.

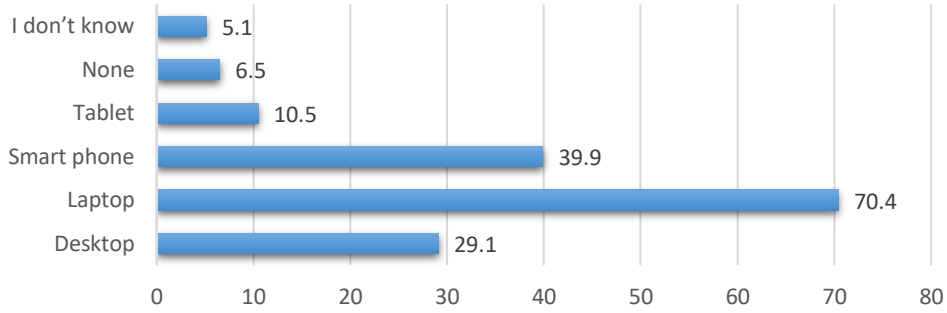


Figure 3.11 Digital devices that have Internet security applied

5- Keeping updated using threat filters and signatures:

Furthermore, participants were asked, in case they use Internet security, is such security kept up to date in terms of filters and signature. In answering this question, it was shown that 299 (47.5%) have their threat filters and signatures automatically updated while 163 (25.9%) stated that they have it manually updated. Nearly, 167 (26.6%) stated that they do not know if they are keeping such security measures updated. Though automatic update is a good practice only 47% of the participants are following this practice, which is one of the major concerns in security practices. In addition, there are considerable number of participants who are not aware of back-ups, reflecting the poor knowledge levels of security practices among the Saudi Arabian participants.

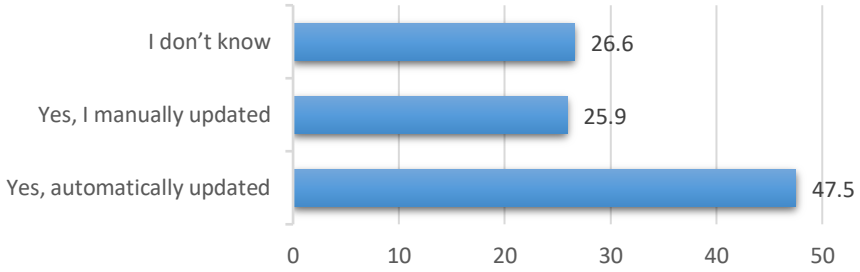


Figure 3.12 updating security using threat filters and signatures

Section C: Cybercrime Awareness

Cybercrime awareness was investigated through a number of questions related to Online and offline resources used to gain knowledge; Opinions about Cyber security and cybercrime; Experiencing cybercrime; Cybercrime concerns; Threat of

cybercrimes in the future; Parties responsible for raising awareness; Role of the government; Application-based cyber security awareness.

1- Online and offline resources used to gain knowledge

This section is concerned about cybercrime awareness. Firstly, participants were asked which online resources do they use when trying to update themselves and gain knowledge about cybercrime. It was shown that the majority of 409 (65%) use Internet general sources (websites, emails, blogs), this was followed by 184 (29.3) who gain such knowledge through TV, news and radio while 147 (23.4%) stated that they gain such awareness from Internet service providers (ISPs). 126 (20%) stated that government websites are the main source for cybercrime awareness and 115 (18.3%) rely on automatic updates. Application security awareness is used by 62 (9.9%) participants), and 150 (23.8%) participants stated that they do not feel that they keep themselves updated. Majority of the participants rely on internet, emails, and blogs for learning security practices; however, these sources are not completely reliable and they can also sometimes mislead the users which can lead to serious outcomes of information mislead. These results indicate lack of awareness among the participants about good security practices.

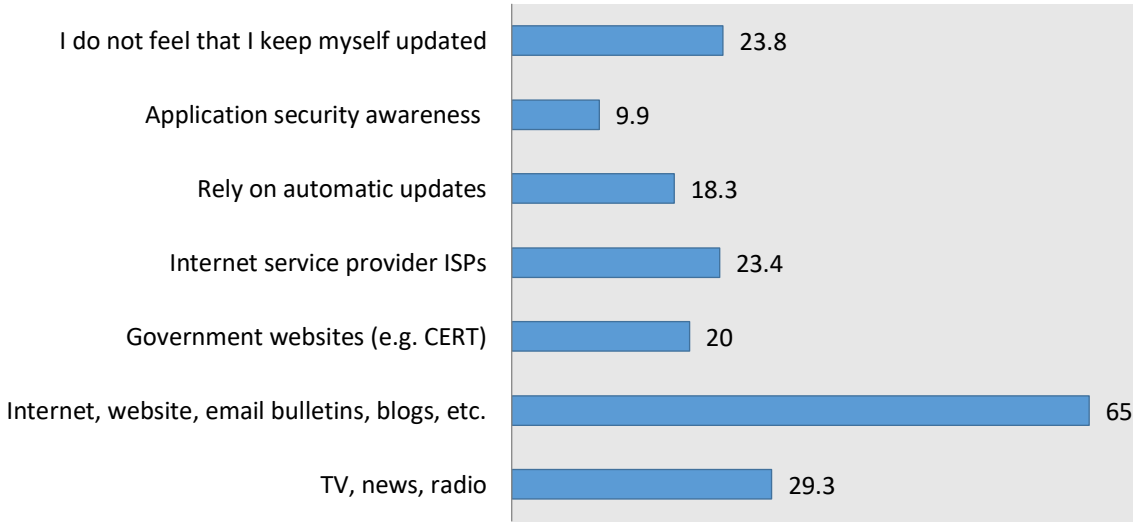


Figure 3.13 Online resources used to increase cybercrime awareness

Secondly, participants were asked about the offline resources they use to increase awareness about cybercrime. It was shown that newspapers, magazines and posters were the main source that was answered by 264 (42%) of the participants. This was followed by government or professional reports, selected by 171 (27.2%) participants. Professional activities were a source of increasing awareness among 142 participants (22.6%) while 122 (19.4%) gain knowledge of cybercrime through Internet services providers (ISPs) offline resources, this was answered by 122 (19.4%) participants. Finally, 177 (28.1%) stated that they do not feel that they keep themselves updated using offline sources. Similar to the online resources, majority of the participants do not effectively use the offline sources for increasing their awareness about security threats.

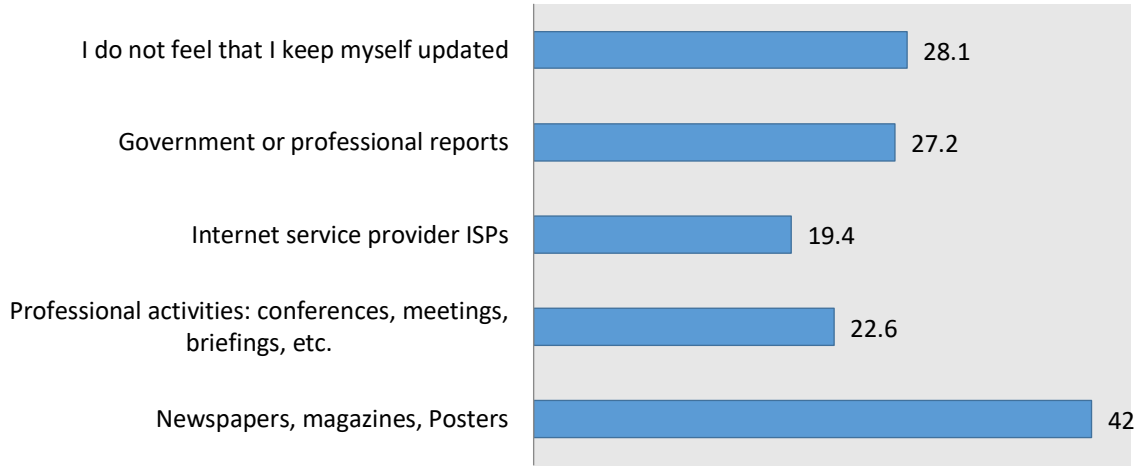


Figure 3.14 Offline resources used to increase cybercrime awareness

2- Opinions about cyber security and cybercrime:

Opinions about cyber security and cybercrime were evaluated using 7 statements as can be seen in Table 3.2. Participants were asked to rank their opinions based on 5-points liker scale. The highest ranked statement based on the mean of agreement was “I think one should avoid disclosing personal information online” (M=4.52), this was followed by “I am willing to accept increased Internet surveillance from the government if it can enhance Internet security” (M=4.14) and thirdly “I feel that the risk of becoming a victim of cybercrime has increased in the past year” (M=4.10). The least ranked items were “I feel informed about the threat of cybercrime” (M=3.85) and “I feel that I am well protected against cybercrime” (M=3.17).

Table 3.2 Frequency and percentages along with descriptive statistics for the opinions on cyber security and cybercrime

Statement	Strongly disagree	Disagree	Natural	Agree	Strongly Agree	Mean	Std.	Rank
I think one should avoid disclosing personal information online	7	23	49	151	399	4.52	0.80	1
	1.1	3.7	7.8	24	63.4			
I feel that the risk of becoming a victim of cybercrime has increased in the past year	4	17	126	265	217	4.10	0.83	3
	0.6	2.7	20	42.1	34.5			
I am concerned that my online personal information is not secure enough	8	55	116	253	197	3.93	0.96	5
	1.3	8.7	18.4	40.2	31.3			
I feel that I am well protected against cyber crime	38	148	177	192	74	3.17	1.08	7
	6	23.5	28.1	30.5	11.8			
I am willing to accept increased Internet surveillance from the government if it can enhance Internet security	30	51	81	167	300	4.14	1.03	2
	4.8	8.1	12.9	26.6	47.7			
I believe that the laws in effect are effective in managing the cybercrime problem	14	47	126	236	206	3.96	0.96	4
	2.2	7.5	20	37.5	32.8			
I feel informed about the threat of cyber crime	17	56	155	221	180	3.85	1.03	6
	2.7	8.9	24.6	35.1	28.6			

3- Experiencing cybercrime:

There are several activities that constitute cybercrimes. In this section participants were asked about how often they have experienced or been victim of the following 6 situations. Answers to such situation were either I do not know (not aware), never experienced, occasionally experienced or often experienced. By looking at their answers in Table 3.3 it can be seen that the most often experienced situation is receiving phishing emails (30.5%) followed by malware infection to devices (27.5%) and thirdly accidently encountering websites promoting hatred and religious extremism (18.1%). But by looking at the occasionally experienced situations, malware (45.5%) comes first followed by phishing emails (37.4%) and cyberattacks (30%). These results indicate that majority of the participants were victims of cyber-attacks and there are considerable number of participants who do not know if they were victims, which is one of the serious issues reflecting the lack of awareness about security threats and good security practices. Lack of awareness among the participants whether they have experienced cyber attack or not clearly indicate the seriousness of the situation.

Table 3.3 Frequency and percentages of participants' experience of cybercrime

Activities	Do not know	Never	Occasionally	Often
Received phishing emails (e.g. asking for money, personal information or bank account details)	43	159	235	192
	6.8	25.3	37.4	30.5
Identity theft (somebody stealing your personal data and impersonating you, e.g. tweeting under your name)	58	315	156	100
	9.2	50.1	24.8	15.9
Malware (e.g. virus) infection of a device	70	100	286	173
	11.1	15.9	45.5	27.5
Being unable to access online services (e.g. banking services) because of cyberattacks.	82	273	189	85
	13.0	43.4	30.0	13.5
	52	291	172	114

Accidentally encountering material that promotes hatred or religious extremism	8.3	46.3	27.3	18.1
Online extortion (a demand for money to avert or stop extortion, or to avert scandal)	84	312	129	104
	13.4	49.6	20.5	16.5

4- Cybercrime concerns:

Participants were presented with 5 of the most common cybercrimes and were asked about their concerns with encountering each on a 5-point likert scale. Two items were recoded for reliability purposes and were described here in the recoded. As can be seen in Table 3.4 The main concern was found to be phishing emails (Mean (M)=2.64) which received agreement and strong agreement by almost 32% of the participants. This was followed by identity theft (M=2.38) where almost 26% agreed or strongly agreed with this concern. Accidently encountering materials promoting hatred and extremism was the third highest rated concern (M=2.11) where almost 18% agreed or strongly agreed with it.

Table 3.4 Participants' answers in the cybercrime concerns' scale

Statement	SD	D	N	A	SA	Mean	Std.	Rank
I am concerned about identity theft (somebody stealing your personal data and impersonating you, e.g. tweeting under your name)	223	166	75	108	57	2.38	1.4	2
	35.5	26.4	11.9	17.2	9.1			
I am not concerned about accidentally encountering child pornography online ®	426	113	51	17	22	1.56	.10	5
	67.7	18.0	8.1	2.7	3.5			
I am concerned about receiving phishing emails (e.g. asking for money, personal information or bank account details)	169	164	92	131	73	2.64	1.38	1
	26.9	26.1	14.6	20.8	11.6			
	235	215	118	34	27	2.05	1.08	4

I am concerned about not being able to access online services (e.g. banking services) because of cyber-attacks. ®	37.4	34.2	18.8	5.4	4.3			
I am concerned about accidentally encountering material that promotes hatred or religious extremism	300	129	79	73	48	2.11	1.32	3
	47.7	20.5	12.6	11.6	7.6			

5- Threat of cybercrimes in the future

The feeling about the threat of cybercrimes in the future was asked by given participants four options to choose from. It was evident that the majority of 459 (73%) think that the threats will become a more serious issue in the future, which is a serious concern among the participants. And 68 (10.8%) think that the threats will vanish eventually while 41 (6.5%) think there will be no significant change regarding threat of cybercrimes in the future. 60(9.5%) thought of other opinions regarding cybercrimes threat.

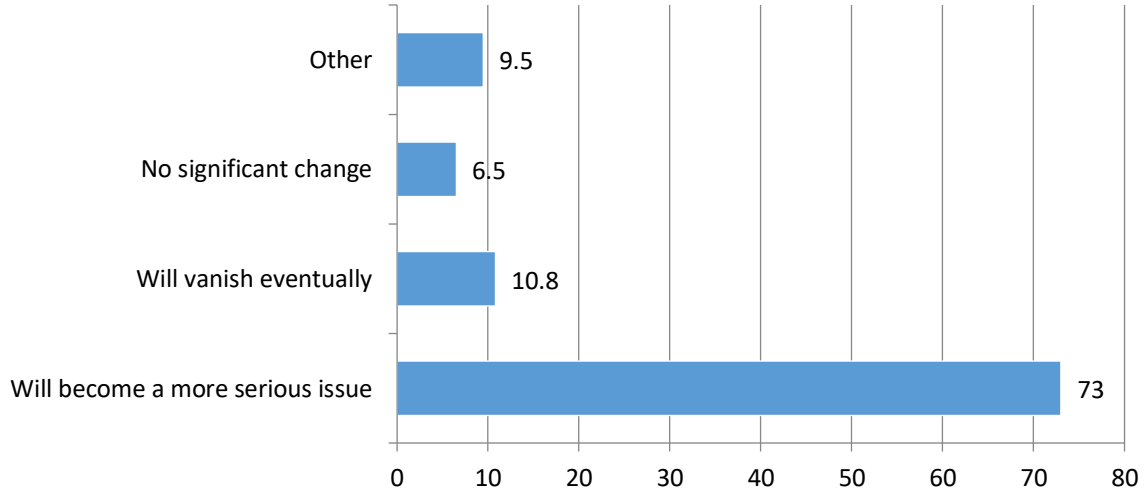


Figure 3.15 Future expectation of cybercrime

6- Parties responsible for raising awareness:

Participants were asked to consider the parties responsible for raising awareness when it comes to cybercrime. As can be seen in Table 3.5 and using a 5-point agreement Likert scale it was evident that the media is the main responsible part (M=4.62); almost 92% of the participants agree or strongly agree that this party should

be held responsible. This was followed by the government as a responsible party (M=4.54), 91% of the participants showed agreement and strong agreement. Thirdly it was Internet services providers (M=4.46) where 88% showed agreement and strong agreement. Other parties were also agreed to be responsible for raising awareness as they have generated more agreement overall.

Table 3.5 Participants' answers in the parties responsible for raising awareness scale, including descriptive statistics

Responsible	SD	D	N	A	SA	Mean	Std.	Rank
The government	8	11	34	158	418	4.54	0.78	2
	1.3	1.7	5.4	25.1	66.5			
The media	4	10	37	116	462	4.62	0.72	1
	0.6	1.6	5.9	18.4	73.4			
Those offering online/Internet-based services (e.g. banks, online retailers, telecommunication companies, etc.)	6	13	54	167	389	4.46	0.81	3
	1.0	2.1	8.6	26.6	61.8			
User itself	5	25	84	194	321	4.27	0.9	5
	0.8	4.0	13.4	30.8	51.0			
Education system	8	17	53	156	395	4.45	0.86	4
	1.3	2.7	8.4	24.8	62.8			

7- Role of the government

The role of the government in preventing cybercrime answered based on 6 categories. The majority of 424 participants (67.4%) explained that the government should have stricter laws and punishment for cybercrimes. Also, 344 (54.7%) explained that the government should play a role in making people aware of cybercrimes, while 261 (45.8%) think that the government should monitor organisations and their misuse of customer information. 261 (41.5%) think that the government should work toward providing a global cyber security framework. 66 participants (10.5%) think that the government has no role to play, and 49 (7.8%) do not know what role the government can play in combating cybercrimes.

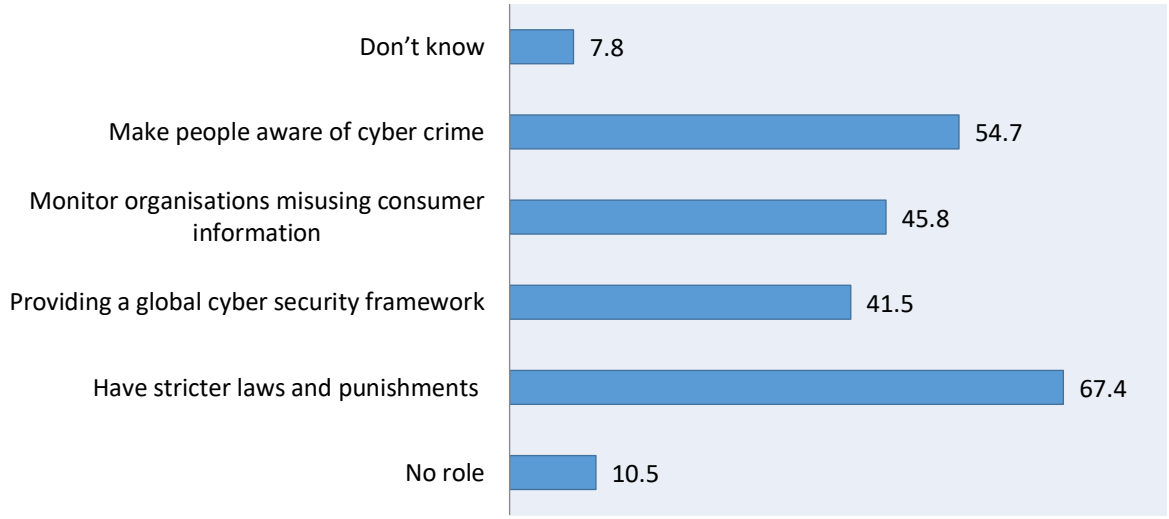


Figure 3.16 The role of government in combating cybercrime

8- Application-based cyber security awareness:

Furthermore, participants were asked about application-based cyber security awareness that can be used on your device/s to help raise your awareness and understanding of key cyber security issues (e.g. cybercrime prevention, data protection, virus protection, safe social networking, password security, device security, web browser security, email security, and more). Participants were given 5 options as can be seen in Table 3.6. The results indicated that there is high agreement level with the statement "Application-based cyber security awareness is necessary" (M=4.54). Followed by the statement that "Such awareness would increase my performance in

protecting my device/s from cybercrime" (M=4.41) and thirdly "This awareness would enable me to detect cybercrime on my device/s" (M=4.38). Clearly there was overall agreement with all statement showing the importance of application-based cyber security awareness.

Table 3.6 Participants' answers in the application-based cyber security awareness scale, including descriptive statistics

Statement	Strongly disagree	Disagree	Natural	Agree	Strongly Agree	Mean	Std.	Rank
Application-based cyber security awareness is necessary	10	3	48	146	422	4.54	0.79	1
	1.6	.5	7.6	23.2	67.1			
This type of awareness is already available to me ®	19	63	66	219	262	4.02	1.1	4
	3.0	10.0	10.5	34.8	41.7			
Such awareness would increase my performance in protecting my device/s from cybercrime	9	9	57	195	359	4.41	0.83	2
	1.4	1.4	9.1	31.0	57.1			
This awareness would enable me to detect cybercrime on my device/s	5	12	62	211	339	4.38	0.80	3
	.8	1.9	9.9	33.5	53.9			
I feel this type of awareness would not be useful for protecting my device/s from cybercrime ®	42	66	133	197	191	3.68	1.2	5
	6.7	10.5	21.1	31.3	30.4			

Section D: Incident Reporting

Participants were asked whether or not they have been victims to cybercrime, in doing so it was evident that 212 (33.7%) experienced cybercrime while the rest (189) did not do. Of those who experienced cybercrime only 23 (10.8%) reported the crime and the rest did not report it. Those who said that they have reported the crime only 6 (26%) reported to the police, 4 (17.3%) reported to the Saudi CERT, 3 (13%) reported to the Saudi e-Government Portal while 2 (8%) reported to the Committee for the Promotion of Virtue and the Prevention of Vice. The rest of the participants reported to other parties.

Those who did not report were asked to state the reason/s. in doing so 117 (61.9) stated “I did not know who to write report about cybercrime” and 75 (39.6%) said “I think that there is no value of reporting” and 56 (29.6%) said “I did not know how to describe or write reports about cybercrime”.

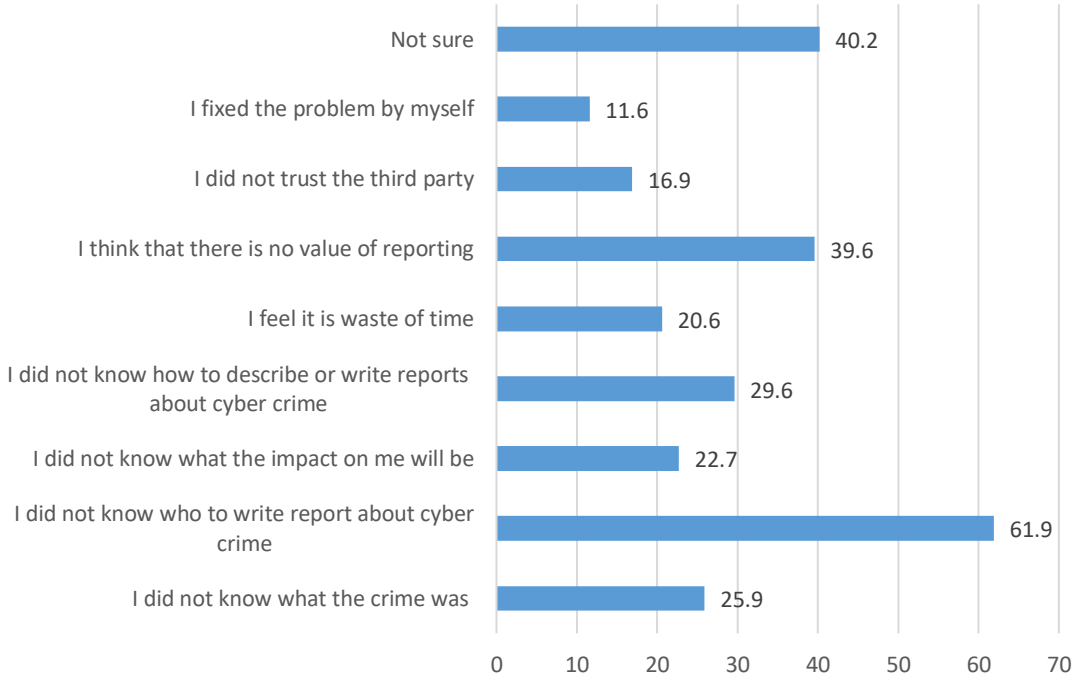


Figure 3.17 The way cybercrime is dealt with among those who experienced it in the past

If No, If you become a victim of cybercrime would you like to report it?

Those who did not experience cybercrime were asked to state their opinion on whether or not they will report such incidents. In doing so 352 (84.4%) stated that they will

report while 65 (15.6%) said they will not report. Of those who said yes, 156 (44.31%) said “Do not know but will ask friends for advice”; 133 (37.3%) stated that they will report to the Saudi e-government; 93 (26.4%) explained that they will report to the Police while 87 (24.7%) will report to the Saudi CERT. finally 69 (19.6%) stated that they will report to “Committee for the Promotion of Virtue and the Prevention of Vice”.

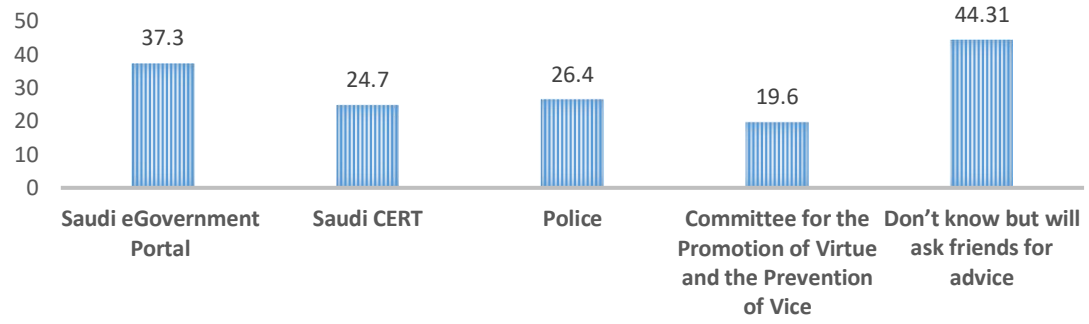


Figure 3.18 Reporting cybercrime if experienced in the future among those who did not experience it in the past

Those who said that they will not report if they experience cybercrime, 35 (53.8%) stated that they will not report because “I do not know who to write report about cybercrime” and 22 (33.8%) said they will not report the cybercrime because “I do not know what the impact on me will be”. 21 participants (32.3%) said that they do not trust the third party when reporting an incident.

Figure 3.19 The reason why cybercrime will not be reported among participants’ who will choose not to report it

3.1.8. Survey Results Analysis

3.1.8.1 Reliability and Computing:

Overall there were 5 scales that were measure on a 5-point Likert scale, namely Opinions about cyber security and cybercrime, Cybercrime concerns, experience of cybercrime, Parties responsible for raising awareness and Application-based cyber security awareness. Likert scale is a good option for measuring behavioural patterns such as change in attitude towards a particular problem or concept by a person, which can be used as an effective approach for comparison (Fowler, 2015). As the questions in the survey are related to the change in behaviours led by awareness, Likert scales is the good strategy for measuring the responses in the survey. The reliability of those scales was tested using Cronbach's alpha. To ensure that the items are all suitable to be tested for reliability items a number of items were re-coded e.g. from negative to positive (see earlier reported scales) in order to have verbally consistent items (5->1, 1→5, 2→4, 4→, 3=3). After doing so the reliability was calculated for each of the scale as can be seen in Table 3.7. Usually, the Cronbach's alpha value greater than 0.70 reflects a high internal consistency, Accordingly, the reliability of all five scales appeared to be higher than 70% indicating a good reliability i.e. items within each scale are consistent with each other leading to the understanding that they are measuring for the same thing.

Table 3.7 The reliability coefficient for each of the selected four scales

Scales	n	Cronbach's alpha
Opinions about cyber security and cybercrime	7	0.72
Experience of cybercrime	6	0.77
Cybercrime concerns	5	0.72
Parties responsible for raising awareness	5	0.76
Application-based cyber security awareness	5	0.72

Following the recoding and the reliability an average score was calculated for each, where all items were added and divided by the total number or items within the scale. This enabled the researcher to look at each scale as a whole. Table 3.8 shows the general descriptive statistics of these scales.

Table 3.8 Descriptive statistics of the four scales

Descriptive Statistics					
	N	Minimum	Maximum	Mean	Std. Deviation
	Statistic	Statistic	Statistic	Statistic	Statistic
Opinions about cyber security and cybercrime	629	1.00	5.00	3.95	.59
	629	1.00	4.00	2.61	.61
Cybercrime concerns	629	1.00	4.00	2.61	.61
Parties responsible for raising awareness	629	1.00	5.00	2.15	.85
Application-based cyber security awareness	629	1.00	5.00	4.47	.58
Opinions about cyber security and cybercrime	629	1.00	5.00	4.21	.66

3.1.8.2 Correlation between the 5 scales:

Using person's correlation coefficient, this section investigates the relationship between four man scales within the questionnaire, namely; Experiencing cybercrime; Cybercrime concerns; Parties responsible for raising awareness; Application-based cyber security awareness. Pearson's correlation coefficient can present a positive or a negative correlation between scales, while it will only be of significance if its probability is smaller than 5% ($p<0.05$). By looking at Table 3.9 it is evident that opinions about cyber security and cybercrime is positively and significantly correlated with experiencing cybercrime, $r(629)=0.23$, $p=0.000$. This indicates that the more they have experienced cybercrime the more likely they are to agree with opinions about cyber security and cybercrime. Opinions also had a significant positive correlation with parties responsible for raising awareness, $r(629)=0.2$, $p=0.000$ and with application based cyber security awareness $r(629)=0.164$, $p=0.000$. However there was a significant negative correlation with cybercrime concerns, $r(629)=-0.10$, $p=0.000$. The more agree on the opinions scale the less they agree with the cybercrime concerns' scale.

Experiencing Cybercrime was significantly and positively correlated with cybercrime concerns $r(629)=0.112$, $p=0.005$ and with parties responsible for raising awareness, $r(629)=0.08$, $p=0.046$. This indicates that the more the experience cybercrime the more they agree with cybercrime concerns and parties responsible for raising awareness.

Furthermore the responsible parties scale showed a negative correlation with cybercrime concerns $r(629)=-0.17$, $p=0.000$, meaning that more they think parties should be held responsible the less they agree with the concerns. A positive correlation was found between responsible parties and application based cyber security awareness scale, $r(629)=0.18$, $p=0.000$. Higher agreement with parties responsible is correlated with higher agreement on the application based cyber security awareness scale.

Table 3.9 Pearson's correlation coefficient and the significance level of correlations between scales

Correlations						
?Scales?		1	2	3	4	5
1.Opinions	Pearson Correlation	1	.234**	-.107**	.196**	.164**
	Sig. (2-tailed)		.000	.007	.000	.000
	N	629	629	629	629	629
2.Experiencing Cybercrime	Pearson Correlation	.234**	1	.112**	.079*	-.010
	Sig. (2-tailed)	.000		.005	.046	.798
	N	629	629	629	629	629
3.Concerns	Pearson Correlation	-.107**	.112**	1	-.168**	-.260**
	Sig. (2-tailed)	.007	.005		.000	.000
	N	629	629	629	629	629
4.Responsible parties	Pearson Correlation	.196**	.079*	-.168**	1	.181**
	Sig. (2-tailed)	.000	.046	.000		.000
	N	629	629	629	629	629
5.Applications	Pearson Correlation	.164**	-.010	-.260**	.181**	1
	Sig. (2-tailed)	.000	.798	.000	.000	
	N	629	629	629	629	629
**. Correlation is significant at the 0.01 level (2-tailed).						
*. Correlation is significant at the 0.05 level (2-tailed).						

3.1.8.3 Gender Effect:

Independent Samples t-test was used to investigate whether or not the gender has a significant effect on the way participants rate the four scales (Opinions about cyber security and cybercrime; Cybercrime concerns; Parties responsible for raising awareness; Application-based cyber security awareness). This test allows to see which of the genders has a higher level of agreement while indicting whether or not the difference is significant. By looking at the descriptive Table 3.10 It can be seen that male participants had higher mean scores across all scales but not the application based cyber security awareness scale. By looking at the results from the t-test it was evident that significant difference exists only in the Opinions about cyber security and cybercrime scale where male participants (M=3.99) had higher agreement compared to female participants (M=3.85). Significance was found at t(627)=2.89, p=0.004.

Table 3.10 Group statistics for each of the genders across the four scales

Group Statistics					
	GENDER	**N**	**Mean**	**Std. Deviation**	**Std. Error Mean**
Opinions	Male	440	3.10	.58	.03
	Female	189	3.85	.60	.04
Cybercrime concerns	Male	440	2.18	.88	.04
	Female	189	2.07	.76	.06
Parties responsible	Male	440	4.5	.57	.03
	Female	189	4.42	.61	.04
Applications	Male	440	4.18	.68	.03
	Female	189	4.26	.60	.04

3.1.8.4 Internet usage effect:

The effect of Internet use on the four scales was examined, and as can be seen in Table 3.11 the results are mixed. By looking at the results from the t-test significant differences were found in parties responsible for increasing cybercrime awareness where participants who frequently use Internet throughout the day showed higher agreement (M=4.49) compare to those who use it once or twice (M=4.19). Significance was found at t(627)=3.85, p=0.01. No significant differences were found on the other scales (p>0.05).

Table 3.11 Group statistics for each of the category of usage across the four scales

	How often do you use Internet and Internet-related services?	**N**	**Mean**	**Std. Deviation**	**Std. Error Mean**
Opinions	Frequently throughout the day	569	3.95	.60	.03
	Once or twice a day	60	3.95	.49	.06
Cybercrime concerns	Frequently throughout the day	569	2.13	.85	.04
	Once or twice a day	60	2.29	.81	.10
Parties responsible	Frequently throughout the day	569	4.5	.53	.02
	Once or twice a day	60	4.20	.90	.12
Applications	Frequently throughout the day	569	4.21	.67	.03
	Once or twice a day	60	4.12	.52	.07

3.1.8.5 Gender association with security practices:

Gender association with other questions was measured through chi-Square and using Cross-tabulations. Chi-square allows the researcher to test the association between two items that are considered categorical, and significant results indicate significant association. A cross-tabulated (Table 3.12) indicates further descriptive of the association. In here only significant finding are reported. Gender had only a significant association with "I change the passwords of important accounts (such as online banking) frequently" $X^2(2,629)=10.32$, $p=0.006$. Clearly it can be seen in Table 3.12 that male participants are more likely to change passwords frequently compared to females.

Table 3.12 The association between gender and changing passwords

			I change the passwords of important accounts (such as online banking) frequently			**Total**
			Never	**Sometimes**	**Always**	
GENDER	**Male**	Count	134	202	104	440
		% within	30.5%	45.9%	23.6%	100.0 %
	Female	Count	81	78	30	189
		% within	42.9%	41.3%	15.9%	100.0 %
Total		Count	215	280	134	629
		% within	34.2%	44.5%	21.3%	100.0 %

3.1.8.6 Education with security tools:

A significant association was found between education level and the use of anti-virus as a protection method X^2 (2,629)=21.18, p=0.000. Table 3.13 indicates that the higher the qualification the more likely the participant is to use anti-virus to protect against cybercrime and increase cyber security. Education also had a significant association with the use of Firewall, X^2 (2, 629)=8.32, p=0.016. Table 3.13 Shows that the higher the qualification the more likely participants are to use Firewall as method of security when using Internet. Similarly, a significant association was found between education and Authentication, X^2 (2,629)= 12.79, p=0.002. Again, participants with higher qualification are more likely to use Authentication (e.g. passwords, pin numbers etc.). It appeared that the less educated participants are the more likely they are to use no method of cyber security (None) X^2 (2,269)=21.26, p=0.000.

Table 3.13 A crosstab Table showing the association between education and different security tools used

EDUCATION			***Anti-virus***		Total
			No	Yes	
	School	Count	57	50	107
		% within	53.30%	46.70%	100.00%
	Undergraduate	Count	128	197	325
		% within	39.40%	60.60%	100.00%
	Postgraduate	Count	53	144	197
		% within	26.90%	73.10%	100.00%
Total		Count	238	391	629
		% within	37.80%	62.20%	100.00%

			Firewall		Total
			No	Yes	
	School	Count	81	26	107
		% within	75.70%	24.30%	100.00%
	Undergraduate	Count	216	109	325
		% within	66.50%	33.50%	100.00%
	Postgraduate	Count	117	80	197
		% within	59.40%	40.60%	100.00%
Total		Count	414	215	629
		% within	65.80%	34.20%	100.00%
			Authentication (e.g. password, PIN)		Total
			No	Yes	
	School	Count	73	34	107
		% within	68.20%	31.80%	100.00%
	Undergraduate	Count	165	160	325
		% within	50.80%	49.20%	100.00%
	Postgraduate	Count	94	103	197

		% within	47.70%	52.30%	100.00%
Total		Count	332	297	629
		% within	52.80%	47.20%	100.00%
			None		Total
			No	Yes	
	School	Count	86	21	107
		% within	80.40%	19.60%	100.00%
	Undergraduate	Count	301	24	325
		% within	92.60%	7.40%	100.00%
	Postgraduate	Count	188	9	197
		% within	95.40%	4.60%	100.00%
Total		Count	575	54	629
		% within	91.40%	8.60%	100.00%

3.1.8.7 Education with role of government:

The association between education and the government role in combating cybercrime yielded to some significant results. A significant association as found with “Have stricter laws and punishments for cybercrimes” X^2 (2,269)=13.15, p=0.001. The higher the education level the more participants agree that the government should have stricter laws and punishments for cybercrimes.

Education also had association with “Work towards providing a global cyber security framework” X^2 (2,629)=12.23, p=0.02. Higher qualification again showed agreement with providing a global cyber security framework. Also, education was associated with

the role of government in “Monitor organisations misusing consumer information” X^2 (2,629)=23.19, p=0.000; and “making people aware f cybercrime” X^2 (2,629)=14.52, p=0.001. Those with lower education showed that they are more likely to say “I do not know” when asked of the government role, X(2,629)=10.56, p=0.005. See Table 3.14.

Table 3.14 A crosstab Table showing the association between education and the roles of the government

Education			**Have stricter laws and punishments for cyber crimes**		**Total**
			no	Yes	
	School	Count	49	58	107
		% within	45.80%	54.20%	100.00%
	Undergraduate	Count	106	219	325
		% within	32.60%	67.40%	100.00%
	Postgraduate	Count	50	147	197
		% within	25.40%	74.60%	100.00%
Total		Count	205	424	629

	Work towards providing a global cyber security framework		Total
	no	Yes	

	School	Count	77	30	107
		% within	72.00%	28.00%	100.00%
	Undergraduate	Count	190	135	325
		% within	58.50%	41.50%	100.00%
	Postgraduate	Count	101	96	197
		% within	51.30%	48.70%	100.00%
Total		Count	368	261	629
		% within	58.50%	41.50%	100.00%

			Monitor organisations misusing consumer information		Total
			no	Yes	
	School	Count	79	28	107
		% within	73.80%	26.20%	100.00%
	Undergraduate	Count	173	152	325
		% within	53.20%	46.80%	100.00%
	Postgraduate	Count	89	108	197

		% within	45.20%	54.80%	100.00%
Total		Count	341	288	629
		% within	54.20%	45.80%	100.00%
			Make people aware of cyber crime		Total
			no	Yes	
	School	Count	65	42	107
		% within	60.70%	39.30%	100.00%
	Undergraduate	Count	145	180	325
		% within	44.60%	55.40%	100.00%
	Postgraduate	Count	75	122	197
		% within	38.10%	61.90%	100.00%
Total		Count	285	344	629
		% within	45.30%	54.70%	100.00%
			Do not know		Total
			no	Yes	
	School	Count	91	16	107

		% within	85.00%	15.00%	100.00%
	Undergraduate	Count	301	24	325
		% within	92.60%	7.40%	100.00%
	Postgraduate	Count	188	9	197
		% within	95.40%	4.60%	100.00%
Total		Count	580	49	629
		% within	92.20%	7.80%	100.00%

3.1.8.8 Internet Usage and security tools:

Chi-square test was conducted to measure the association between Internet usage and security tools. It was found that there is a significant association with the use of anti-virus X^2 (1,629) =5.39, p=0.02 showing that those who use Internet frequently throughout the day are more likely to use anti-virus, and are more likely to use firewall X^2 (1,629)=5.92, p=0.015, and lastly they are more likely to use software updates, X^2 (1,629)=4.10, p=0.043 (see Table 3.15).

Table 3.15 Crosstab Tables showing the association between education and security tools/applications

Crosstab					
How often do you use Internet and Internet-related services? Frequently throughout the day			10. Anti-virus		Total
			no	Yes	
	Frequently throughout the day	Count	207	362	569
		% within	36.40%	63.60%	100.00%

	Once or twice a day	Count	31	29	60
		% within	51.70%	48.30%	100.00%
Total		Count	238	391	629
		% within	37.80%	62.20%	100.00%
			Firewall		Total
			no	Yes	
	Frequently throughout the day	Count	366	203	569
		% within H	64.30%	35.70%	100.00%
	Once or twice a day	Count	48	12	60
		% within	80.00%	20.00%	100.00%
Total		Count	414	215	629
		% within	65.80%	34.20%	100.00%
			Software update		Total
			no	Yes	
	Frequently throughout the day	Count	341	228	569
		% within	59.90%	40.10%	100.00%
	Once or twice a day	Count	44	16	60
		% within	73.30%	26.70%	100.00%

Total	Count	385	244	629
	% within	61.20%	38.80%	100.00%

3.1.8.9 Internet skills and security tools:

Skills' level in using Internet and digital devices was significantly associated with the use of Anti-virus X^2 (2,269)=32.10, p=0.00, where those with better skills are more likely to use antivirus. Similar association was found with the use of Firewall, X^2 (2,629)=62.59, p=0.000. Also there was association with the use of Encryption, X^2 (2,629)=42.93, p=0.000; Software updates X^2 (2,629)=17.20, p=0.000, As well as backup, X^2 (2,629)=31.43, p=0.000. Finally, those who have lower Internet and digital devices skills are more likely to use no security means, X^2 (2,629)=12.87, p=0.002 (see Table 3.16).

Table 3.16 A crosstab showing the association between Internet skills and security tools used

What are your Internet/ Digital devices skills level?			**10. Anti-virus**		**Total**
			no	Yes	
5	Beginner/Basic	Count	121	125	246
		% within	49.20%	50.80%	100.00%
	Intermediate	Count	105	199	304
		% within	34.50%	65.50%	100.00%
	Expert	Count	12	67	79
		% within	15.20%	84.80%	100.00%
Total		Count	238	391	629
		% within	37.80%	62.20%	100.00%
			Firewall		Total

			no	Yes	
	Beginner/Basic	Count	191	55	246
		% within	77.60%	22.40%	100.00%
	Intermediate	Count	200	104	304
		% within	65.80%	34.20%	100.00%
	Expert	Count	23	56	79
		% within	29.10%	70.90%	100.00%
Total		Count	414	215	629
		% within	65.80%	34.20%	100.00%

			Encryption		Total
			no	Yes	
	Beginner/Basic	Count	239	7	246
		% within	97.20%	2.80%	100.00%
	Intermediate	Count	278	26	304
		% within	91.40%	8.60%	100.00%
	Expert	Count	58	21	79
		% within	73.40%	26.60%	100.00%
Total		Count	575	54	629
		% within	91.40%	8.60%	100.00%

	Software update	Total

			no	Yes	
	Beginner/Basic	Count	167	79	246
		% within	67.90%	32.10%	100.00%
	Intermediate	Count	185	119	304
		% within	60.90%	39.10%	100.00%
	Expert	Count	33	46	79
		% within	41.80%	58.20%	100.00%
Total		Count	385	244	629
		% within	61.20%	38.80%	100.00%

			Backup		Total
			no	Yes	
	Beginner/Basic	Count	178	68	246
		% within 5.	72.40%	27.60%	100.00%
	Intermediate	Count	180	124	304
		% within	59.20%	40.80%	100.00%
	Expert	Count	30	49	79
		% within	38.00%	62.00%	100.00%
Total		Count	388	241	629
		% within	61.70%	38.30%	100.00%

	None	Total

			no	Yes	
	Beginner/Basic	Count	215	31	246
		% within	87.40%	12.60%	100.00%
	Intermediate	Count	281	23	304
		% within	92.40%	7.60%	100.00%
	Expert	Count	79	0	79
		% within	100.00%	0.00%	100.00%
Total		Count	575	54	629
		% within	91.40%	8.60%	100.00%

3.1.8.10 Internet skills and security practices

A chi-square test was also used to determine the association between skills' level in using Internet and digital devices with cyber security practices. Evidence showed that there is a significant association between skills and "I check the legitimacy of a website before accessing it" X^2 (4,629)=43.00, p=0.000. Higher skills are associated with better check.

Skill level was also associated with "I am aware of the danger when clicking on banners, advertisements or pop-up screens that appear when surfing Internet" X^2 (4,629)=25.88, p=0.000. those with higher skills showed more awareness. Also a significant association was found with "I give due attention to privacy settings on my social media account(s) (e.g. Facebook)" X^2 (4,629)=40.39, p=0.000 and with "I change the passwords of important accounts (such as online banking) frequently" X(4,629)=38.55, p=0.000. Participants with higher skills are more likely to give more attention to privacy settings and to change passwords.

Furthermore, a significant association was found between skill level and "I feel safe when using public Wi-Fi" X^2 (4,629)=25.14, p=0.000 and with "I feel my digital devices (computer, smartphones) has no value to hackers, they do not target me" X^2 (4,629)=26.13, p=0.000. Clearly here those with high levels of Internet skills are less

likely to feel safe when using public Wi-Fi and less likely to think that digital devices have no value to hackers.

And finally a significant association was found between skills level of Internet and digital devices use and "I regularly install software updates" X^2 (4,629)=23.15, p=0.000. Those with higher skills are more likely to regularly install software updates.

Table 3.17 A crosstab Table showing the association between Internet skills and security practices

			I check the legitimacy of a website before accessing it			**Total**
			Never	Sometimes	Always	
5.What are your Internet/ Digital devices skills level?	Beginner/Basic	Count	64	116	66	246
		% within	26.00%	47.20%	26.80%	100.00%
	Intermediate	Count	46	168	90	304
		% within	15.10%	55.30%	29.60%	100.00%
	Expert	Count	5	27	47	79
		% within	6.30%	34.20%	59.50%	100.00%
Total		Count	115	311	203	629
		% within	18.30%	49.40%	32.30%	100.00%

	I am aware of the danger when clicking on banners, advertisements or pop-up screens that appear when surfing Internet			Total
	Never	Sometimes	Always	

5.What are your Internet/ Digital devices skills level?	Beginner/Basic	Count	26	89	131	246
		% within	10.60%	36.20%	53.30%	100.00%
	Intermediate	Count	23	77	204	304
		% within	7.60%	25.30%	67.10%	100.00%
	Expert	Count	1	13	65	79
		% within	1.30%	16.50%	82.30%	100.00%
Total		Count	50	179	400	629
		% within	7.90%	28.50%	63.60%	100.00%

			I give due attention to privacy settings on my social media account(s) (e.g. Facebook)			Total
			Never	Sometimes	Always	
5.What are your Internet/ Digital devices skills level?	Beginner/Basic	Count	86	81	79	246
		% within	35.00%	32.90%	32.10%	100.00%
	Intermediate	Count	57	118	129	304
		% within	18.80%	38.80%	42.40%	100.00%
	Expert	Count	6	24	49	79
		% within	7.60%	30.40%	62.00%	100.00%
Total		Count	149	223	257	629
		% within	23.70%	35.50%	40.90%	100.00%

			I change the passwords of important accounts (such as online banking) frequently			Total
			Never	Sometimes	Always	
5.What are your Internet/ Digital devices skills level?	Beginner/Basic	Count	115	92	39	246
		% within	46.70%	37.40%	15.90%	100.00%
	Intermediate	Count	89	148	67	304
		% within	29.30%	48.70%	22.00%	100.00%
	Expert	Count	11	40	28	79
		% within	13.90%	50.60%	35.40%	100.00%
Total		Count	215	280	134	629
		% within	34.20%	44.50%	21.30%	100.00%
			I feel safe when using public Wi-Fi			Total
			Never	Sometimes	Always	
5.What are your Internet/ Digital devices skills level?	Beginner/Basic	Count	74	109	63	246
		% within	30.10%	44.30%	25.60%	100.00%
	Intermediate	Count	120	136	48	304
		% within	39.50%	44.70%	15.80%	100.00%
	Expert	Count	45	27	7	79
		% within	57.00%	34.20%	8.90%	100.00%

Total		Count	239	272	118	629
		% within	38.00%	43.20%	18.80%	100.00%
			I feel my digital devices (computer, smartphones) has no value to hackers, they do not target me			Total
			Never	Sometimes	Always	
5.What are your Internet/ Digital devices skills level?	Beginner/Basic	Count	39	120	87	246
		% within	15.90%	48.80%	35.40%	100.00%
	Intermediate	Count	58	163	83	304
		% within	19.10%	53.60%	27.30%	100.00%
	Expert	Count	28	43	8	79
		% within	35.40%	54.40%	10.10%	100.00%
Total		Count	125	326	178	629
		% within	19.90%	51.80%	28.30%	100.00%
			I regularly install software updates			Total
			Never	Sometimes	Always	
5.What are your Internet/ Digital devices	Beginner/Basic	Count	20	113	113	246
		% within	8.10%	45.90%	45.90%	100.00%
	Intermediate	Count	15	119	170	304

skills level?		% within	4.90%	39.10%	55.90%	100.00%
	Expert	Count	3	16	60	79
		% within	3.80%	20.30%	75.90%	100.00%
Total		Count	38	248	343	629
		% within	6.00%	39.40%	54.50%	100.00%

3.2. Discussion

This chapter presented the major findings from the survey and how different aspects are correlated with respect to the cybercrime and cyber security awareness. One of the important findings is that the cybercrime experience was positively correlated with the cybercrime concerns, reflecting the main point that the more experience and awareness the people have the more they realise the importance of cyber security concerns and the parties responsible for cyber security awareness. Gender effect on the cyber security was observed only in the opinions of cyber security concerns and crime where male participants showed higher understanding than female participants. In addition, male participants were more likely to change the security passwords compared to the female participants. The participants with high internet usage reflected higher importance about cyber security concerns, awareness and parties responsible, and are more likely to use anti-virus compared to those with low internet usage. Similarly, the participants with internet skills are more likely to use security tools and adopt good security practices compared with those with poor internet skills.

These findings reflect the basic answer to the research question that the more aware the users the more likely they were to adopt the better security practices. Therefore, it can be considered that raising cyber security awareness could be one of the effective solutions in addressing the problems associated with the cyber security. In addition, majority of the participants were young, considering which gamification could be the effective approach to be considered as a part of the study for raising cyber security awareness. Moreover, majority of the participants were having high educational

qualification (Post-graduate), and most of the participants were found to be using internet frequently on mobile devices and next on the computers. Therefore, mobile game application could be one of the best possible solutions for raising cyber security awareness. Additionally, majority of the participants were found to be not using the security features such as backup, software updates, encryption, authentication, firewall and only anti-virus was found to be using by 60% of the participants. Additionally, the analysis indicated that the participants were having lack of knowledge about the resources (both online and offline) which can help them to protect from cyber threats. Such poor awareness and security practices among the participants were one of the major reasons and motivation behind selecting the two mobile games focusing on malware and password protection for raising awareness. Also, majority of the participants preferred mobile based application for raising cyber security awareness, which further supported the idea of developing the mobile games for raising awareness. Some of the major findings from the survey are presented in the following sections.

Some of the key findings of the survey was that there is a high usage of Internet on largely daily basis amongst participants. Another important observation was that over 90% participants use smartphones primarily for Internet access for various activities including banking, shopping activities. The general observation was that even though the survey shows good IT literacy amongst users, the cyber security literacy was weak amongst them. It was observed that apart from anti-virus and firewall as a relatively common cyber security practice, the participant`s responses showed that they have relatively less cyber security awareness and have weaker practices such as creating easy passwords.

One of the ways of combating cybercrime is by creating awareness and adopting better cyber security practices. A majority of survey responses indicated that the users are insecure about their data security and are willing to adopt better practices to secure their devices and data. These findings can be correlated with the studies (Shamseddine and Kalin, 2017; al-Hussein, 2017) which have found increasing number of cyber-attacks in the recent years in Saudi Arabia. The survey responses also indicated that a cyber security awareness application would enable the users to improve their cyber security practices. Therefore, it is important more awareness is

created. Designing an application which can provide information or train users about best cyber security practices can be an effective way to increase cyber security awareness. The widespread use of smartphones could be exploited to design such application which can be easily installed and accessed by users. Various studies (Shih et al., 2011; Tian et al., 2010; Trybus, 2014) have found positive results in application based security awareness creation, which further supports the idea of using mobile application for creating cyber security awareness.

The key findings of the survey are that there is a high usage of Internet mostly on daily basis amongst participants. Similar results were found by Shamseddine and Kalin (2017). Another important observation was that over 90% participants use smartphones primarily for Internet access for various activities including banking, shopping activities. The general observation was that even though the survey shows good IT knowledge amongst users, the cyber security awareness was weak amongst them. It was observed that apart from anti-virus and firewall as relatively common cyber security practices, the participants' responses showed that they have relatively less cyber security awareness and have weaker practices such as creating easy passwords. Though Saudi Arabia has experienced a significant growth in the use of technologies but use of security technologies (and the extent of related awareness) has not kept pace, and citizens are experiencing problems and prefer an effective role of responsible organizations in improving cyber security awareness and support the concept of using mobile applications for increasing security awareness among them. It is clearly evident from the survey results as majority of the participants has experienced cyber-attacks.

3.3. Summary

The survey results in the context of Saudi Arabia, has identified that creating awareness and adopting better cyber security practices among the people is one of the effective ways of combating cybercrime. The survey responses in the study has indicated that the users are insecure about their data security and are willing to adopt better practices to secure their devices and data. The survey responses also indicated that a cyber security awareness application would enable the users to improve their cyber security practices. Therefore, it is important that different approaches for creating cyber security awareness in Saudi Arabia must be developed and deployed

to combat cybercrime. As preferred by the participants a mobile application for this purpose can be an effective approach in combating cybercrime and raising awareness. However, the application needs to be engaging users and effective in educating and training the users.

The results from the survey have shown that the cyber security awareness levels among the end users in Saudi Arabia are very poor. Most of the participants are aware of security practices such as using security tools, updating the software, creating strong passwords, data backup, reporting an incident, laws and regulations, role of government etc. The results show that there is an urgent need to increase the security awareness among the end users in Saudi Arabia, as the nature of threats is changing daily and the number of threats is increasing rapidly. With the rapid increasing Internet using population, an application-based security awareness program can be more effective as majority of the participants were not aware of it or very few participants knew about it.

Therefore, the awareness programs must be developed in such a way that it perfectly meets the changing needs of the people and considers the lifestyles and cultural practices in the country and must be engaging. Gamification in this aspect could be one of the effective solutions as studies have found it to be effective in creating awareness (Gondree et at., 2013; Kayali et al., 2014). Considering these factors, the next chapter reviews various studies and mobile applications coupled with gaming technology for generating security awareness in KSA.

Chapter Four

Gamification of Cyber Security

4. Gamification

4.1. Introduction

Creating awareness about cyber security is an important requirement towards combating cybercrimes effectively. In the previous chapter, study conducted an extensive survey in Saudi Arabia where more than 600 participants took part. The survey investigated various topics such as levels of Internet use; current level of public of cyber security awareness; common cyber security practices used by them; understanding of cybercrime knowledge and attitude towards cybercrime.

From the survey, it was observed that almost 91% of the participants use Internet very frequently with at least 50% of the participants having intermediate and higher levels of Internet literacy. It was also observed that 90% of the participants use smartphones as their most regularly used device for Internet access, indicating the high usage of smartphones in KSA. Another important observation is that participants use internet widely for purposes such as banking, online shopping, government services, social networking, and entertainment.

Such high usage of Internet and Internet based applications via smartphones puts user`s data under risk to hackers. An increased awareness about cyber security can enable users to effectively combat threats to their data privacy and security. Thus, it is important that users are fully aware of the consequences of their interaction in the cyber space. A smartphone application for cyber security awareness is an effective method of updating users about the vulnerability of the data on their devices.

To increase awareness about cyber security, it is essential that the users are provided with training. There are various modes of creating cyber security awareness like education, promotion etc. However, it is essential that these modes have to be effective in creating an impact on the users. It was evident from the study conducted through the survey discussed in previous chapter that the participants are interested in application-based security awareness programs. Additionally, the increasing number of mobile and Internet users in Saudi Arabia adds as an advantage for developing the applications for better security awareness. However, it must be considered that the application must be engaging the users in learning process.

Serious games can be an effective method to provide training to the users. Serious games are designed with a purpose rather than just intended for pure entertainment. They are proved to be effective tools for training and achieving a behavioural change. Such methods of using games for training is also referred as games-based learning approaches. Though games-based learning methods are mainly utilized in school education, increasingly, these methods are also adopted in healthcare, advertising, behavioural change, and recently in cyber security training (Hendrix et al., 2016). As creating awareness is a process that results in change in the behaviour towards a particular problem and considering lack of awareness as one of the major factors for increasing cyber threats assessed from the previous chapters, a game-based application for cyber security awareness could be an effective approach in meeting the goal of enhancing cyber security awareness. Considering these factors, the aim and objectives of the study in this chapter are explained as follows.

Aims and Objectives

The aim of the study in this chapter is to investigate and review the effectiveness of gaming technologies in creating cyber security awareness. Accordingly, the objectives of the study include the following.

- Understand the concept of games and their use in creating awareness.
- Conduct a systematic review of the studies focused on the use of gaming technology for creating cyber security awareness.
- Review popular games designed for cyber security awareness.

4.2. Gamification

Learning through mobile games is an educational process where the users are required to perform learning activities by using a game or a series of games designed for specific learning activity (Ghazvini et al., 2009; Kurkovsky, 2009; Shih et al., 2011). The digital games on mobiles can be effective in providing fidelity of simulations and problem solving tasks, which could enhance the learning activity and motivate the users. Understanding its scope, researchers have suggested that gamification can be a key concept for learning security awareness concepts in future (Shih et al., 2011). While few studies have identified the potential of gaming in learning, other studies have already identified the change in the implementation (Molnar and Frias-Martinez,

2011). Different studies have found the huge potential of implementing gaming technology in different areas. In a study conducted by Banerjee et al. (2007) with a focus on assessing gaming for learning, it was identified that learning process can be significantly be improved by mobile gaming education. Another study conducted by Tian et al. (2010) has found that gaming process can improve literacy levels among children.

Research studies have found that games are an effective education tool widely popular and effective in teaching, especially puzzle games. A study conducted by Costabile, et al. (2008) has explored how a mobile phone can be used to teach archaeology through game-based learning. The games-based learning method has several advantages. The obvious advantage is that games-based learning method provides an interactive approach to train or educate the users about a specific program. It enables the players to acquire skills and to enable thought processes in a fun and interactive way. The adaptability and flexibility of gaming approaches enables to design the game that suits almost all training subject possible (Boyle, 2011). For example, a puzzle game can increase the computational skills, and creative thinking. Similarly, a quiz game can increase the awareness levels on a subject or topic; and also useful in evaluating the players knowledge levels. Games are used in both cases whose purpose and the concepts are different, which reflects its adaptability and flexibility to be used in various aspects. One of the strengths of the gaming applications as analysed by various authors is that it can promote learning using its various enhanced approaches such as interactivity, adaptability, flexibility, usability; and also understanding of various concepts.

A well designed game enables the user to enter a virtual environment that is similar to the real environment and would enable the player to draw connection between the learning in the virtual environment to the real world. The games-based approach would motivate the player to move towards the goal with required actions and also see the consequences without facing penalties in the real life. Further, when compared to the traditional method of training, games-based methods are more engaging, relatively cost effective, easily transferrable to a large number of trainees, customized to each player, etc. (Trybus, 2014). GBL as discussed in various studies can be an effective way to enhance the learning process thereby creating awareness. Another important

strengths of gamification is that real time scenarios can be created in virtual environments, where the users can interact in similar to the real world interaction and minimise failures which may not have any effect as it is a virtual environment. This reduces the impact of failures and motivates the players interest and increases skills and competencies.

4.3. A Systematic Review of Cyber security Studies using Gaming technologies

The number of mobile and computer games has been on the rise in the past few years. With a rapid increase in the smartphone usage across the world, there has been a rise in the number of various mobile gaming applications. As the games are effectively engaging the users, the possibility of using them for cyber security awareness is being considered as one of the major areas of research. As the growth of these applications is observed to be at a rapid pace, the design and developments are going on in both academic and commercial settings. Therefore, it is necessary to consider both existing applications used for cyber security awareness and also the studies associated with them.

To assess the GBL application in creating cyber security awareness, a systematic review of previous studies focusing on the same concept was conducted. This review process would help in assessing the amount of research that has been conducted for cyber security awareness using Gamification and the suitability of gaming technology for this purpose.

4.3.1. Methodology

The systematic review was carried out in November and December 2016, which included studies and papers published in various journals and conferences. The literature search was conducted using IEEE, SDL, and Google Scholar, which is one of the popular search engines for academic releases and has various options for filtering the results. The following keywords and their combinations are used for literature search.

- Gamification
- Mobile Game
- Computer game

- Serious Games
- Cyber Security
- Online Security
- Safety Gamification
- Cyber Security Awareness

The search was initially focused on considering the studies with an outcome using some measurement techniques. However, as there were only few studies found that were focusing on cyber security awareness and training using gaming applications, the search was expanded to include any academic paper describing a cyber security game. The literature search yielded 68 results, which were inspected and 12 papers were selected that were focusing on the aim of this study (cyber security awareness through gaming applications). These studies were grouped by the games they describe, type, methods used, and the results (whether significant or not?). As the search shows large number of results only the first 15 results for each keyword or their combination are considered for inspection.

4.3.2. Review and Analysis

12 papers have been identified, which were focusing on cyber security awareness and training through games. These papers are presented in Table 4.1. Out of these only 6 studies were conducted in 2010 or before, and remaining 6 papers post 2010, which reflects the area of study as relatively new. These studies focus on analysing different games for creating cyber security awareness and training using technologies that include 3D virtual world or simulation, 2D framework, mobile applications and web based application technologies. Most of the games focused on general cyber security awareness, network security, and phishing and end-user PC protection.

As the number of studies in the area of cyber security training has been increasing, most of these studies were focusing on the general public. Very few studies are found to be focusing on training professionals in the aspects of internal threats. Any study has to evaluate the application to identify the suitability and the usability of such applications. Out of the reviewed papers only few studies have evaluated the applications which include Anti Phishing Phil, NGSEC, and Control-Alt-Hack. All these

studies have indicated positive feedback on utilizing games for creating cyber security awareness.

The Anti-Phishing game developed by Arachchilage and Love (2013) used an effective graphical interface, where the players are required to identify the legitimate URL's, and harmful URL's. The game used storyboard mechanism using two main characters (player fish, and teacher fish). A total of 10 URL's which includes five good worms (associated with legitimate URL's), and five fake worms (associated with phishing URL's. e.g. numbers in the front of URL) were used in the study. The player fish is supposed to eat good worms, which would increase its size. However, the player fish should avoid eating fake worms. In case the player fish has any doubt regarding a worm, it can take help from teacher fish, which would provide suggestions to identify the fake worms. Every time the player fish requests help, the score will be reduced by certain amount (by 100 seconds). The player fish is supposed to eat the worms from legitimate URL's and avoid illegitimate URL's by clicking the avoid button. This way the score can be achieved. There is a negative scoring for wrong identification of URL's and wrong selection of worms. This game was found to be very effective improving the understanding of phishing and avoiding phishing attacks. However, the game lacks effective narration, and is only limited to learning about phishing attacks in a limited scope.

Ctrl Alt Hack game developed by Dasgupta et al. (2013) was an interesting real time experience game where the users are required to apply their hacking skills in order to hack in to a system of a company in the game. All the players are considered as the employees of a computer security company providing security audits. The players get paid for hacking the given company in various approaches. This game not only increased competition among players but also helped in identifying security loopholes, and increased the awareness of performing security tasks. Different gaming engines were used in the study. The unreal engine allows the users to figure out the PIN using discrete mathematics in order to advance to the next level. Different set of permutations can be entered to identify the correct PIN. Similarly, Ceaser Cipher, another 3D game is used for decoding the encryption and decryption. The users were given randon strings as hints for decoding the encryption and decryption, using which the user rotates the wheel (locker) to correct the character. Once all the characters

are correctly decoded, the user wins the game. This game promotes thinking process among the users by providing various challenges, which not only educates the users, but also helps in identifying the security loopholes. In addition, the interactive process helps the users in engaging with the storyline or the problem. However, this game was evaluated only using a small sample population, and it needs to be evaluated with the larger set of population to generalise its results.

Similarly, 'Internet Hero' game developed by Kayali et al. (2014) was very successful in increasing the awareness among the children. The players were virtually transported in to the fictional world of internet, where the technical and social basics of using internet are conveyed to the players using a gaming approach. Email and malicious software were the two aspects focused in this game. *Ping,* an entity which acts as a tutor and guide to the players is very useful in the game which helps in identifying and avoiding various security issues. In the first level, the player has to help *Ping* in identifying the spam emails by sorting 20 different mails. The legitimate mails have to be forwarded to the recipients, while the spam mails have to be destroyed by throwing them to the trash bin on the left side of the screen. The player has to read the incoming mails and identify any suspicious contents such as attachments or links or advertising, and decide whether it is spam or legitimate email. The next level of the game focuses on identifying three different types of spam-ware, by using three types of defence towers including firewalls (stops viruses, trojans, and worms from getting to CPU), scanners (identifies malwares), and shooters (destroys the malware identified by scanners). Ten waves of attacks have to be faced by the player to win the game, and if any malware reaches CPU, the game is lost. The results of this study have found an increased awareness of using internet ethically among the players. However, few improvements were suggested in the story pattern and support to be received by the player.

These studies reflect the strengths and weaknesses of the gaming applications in increasing the awareness among the various participants.

Table 4.1 Major studies focusing on gamification for cyber security awareness

Authors	Game	Type	Methods	Results
Arachchilage and Love (2013)	Anti-Phishing Phil	Mobile gaming application: Training for links (URL) safety	Usability questionnaire	Improved learning and susceptibility of phishing
Arachchilage and Love (2014)	Anti-Phishing	Mobile gaming application: Training for links (URL) safety	Review	Improved learning
Nyeste and Mayhorn (2010)	Anti-Phishing	Mobile gaming application: Training for links (URL) safety	RCT, pre and post experimental study	Improved learning and susceptibility of phishing
Ariyapperuma and Minhas (2005)	Next generation security - NGSEC	Web based gaming application	Review of tasks and performance	Significant improvements identified among users in performing security tasks
Gondree et al. (2013)	-	Mobile Board game	Multi-player assessment (group study)	Positive feedback, need for more evaluation

Dasgupta et al. (2013)	Control Alt Hack	Mobile Puzzle game	Assessment based on Puzzles	Effective in creating awareness
Denning et al. (2013)	-	Review	Survey of teachers	Effective game for model dissemination
Geers (2010)	Baltic Cyber Shield- BCS	Training exercise with virtual attackers and defenders	Review	Recommendations for improving IT infrastructure
Kayali et al. (2014)	Internet Hero	Puzzle game	Experiment study	Improved awareness
Irvine and Thompson (2003)	Internet	-	Review	Positive impacts of games with recommendations
Pastor et al. (2010)	-	Multiple games	Review	Recommended developing and using more tools in games
Schweitzer and Brown (2009)	-	Visual presentation	Presentation (Education) case study	Positive experience of users in using interactive visualization

However few studies including (Gondree et al., 2013; Geers, 2010; Irvine and Thompson, 2003; Pastor et al., 2010) have suggested some improvements and recommendations, while all other studies have stated positive results.

Studies including Anti Phishing Phil and Security games by Next Generation Security (NGSEC) have shown significant improvements in using games for learning purpose, but the sample sizes used in these studies were quite small. Other games have resulted in positive feedback from users but did not evaluate the impact and effects on learning outcomes; while other remaining studies either did not study effects on learning outcomes, or the results were not quite conclusive, but the authors were convinced they gave a positive "early indication".

A review of these studies has indicated that the cyber security awareness approach through gaming is relatively quite new and needs extensive research studies and evaluation approaches for analysing various security issues and the related gaming techniques. As the cyber security is a large area were the threats may appear in various forms, some streamlined gaming techniques are necessary for generating awareness according to the types of threats.

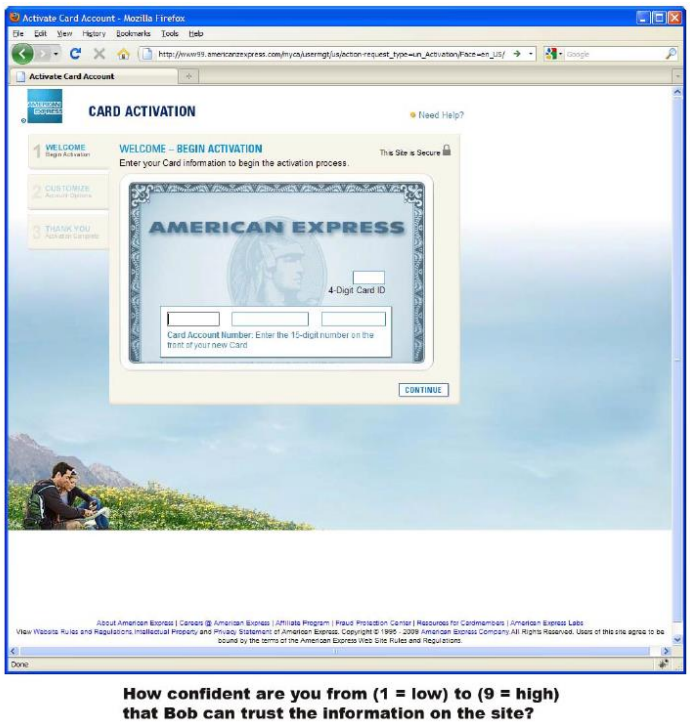


Figure 4.1 Anti-Phishing game prototype Nyeste and Mayhorn (2010)

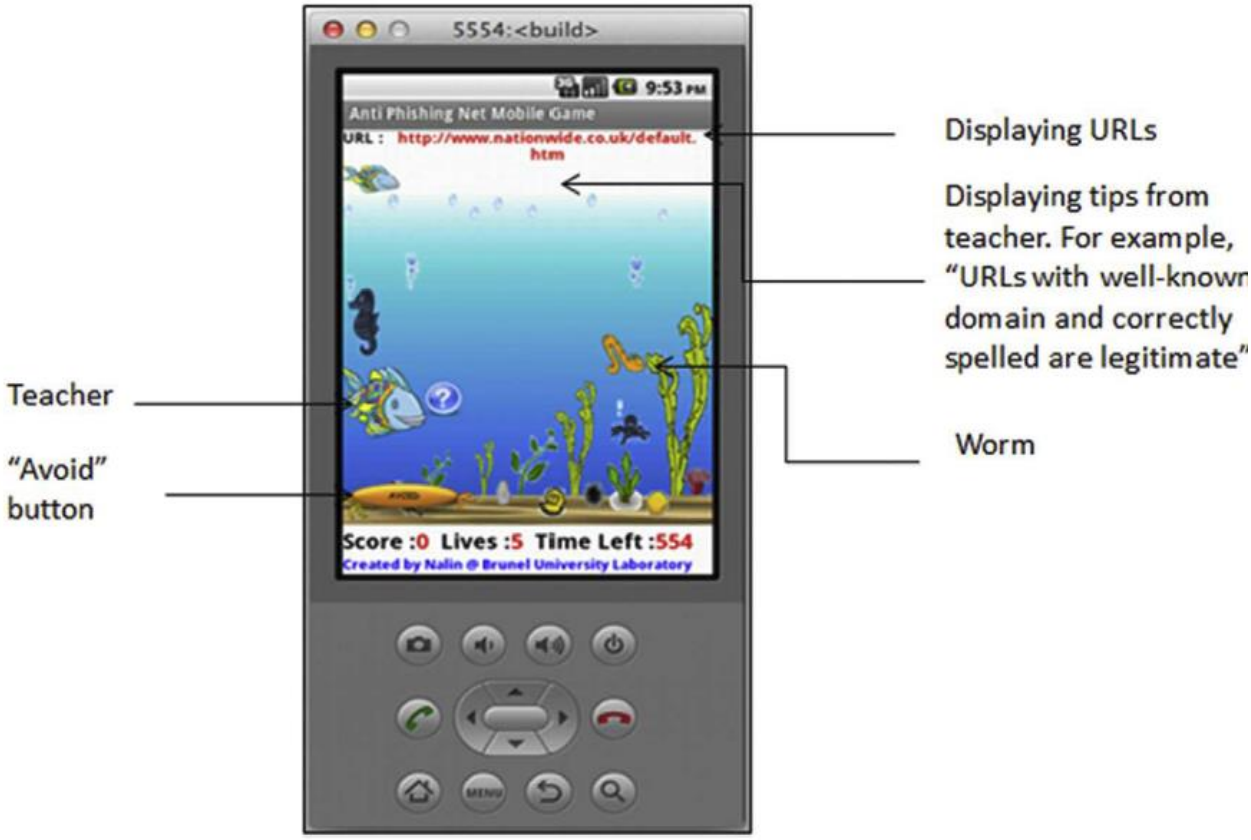


Figure 4.2 The mobile game prototype (Arachchilage and Love, 2014)

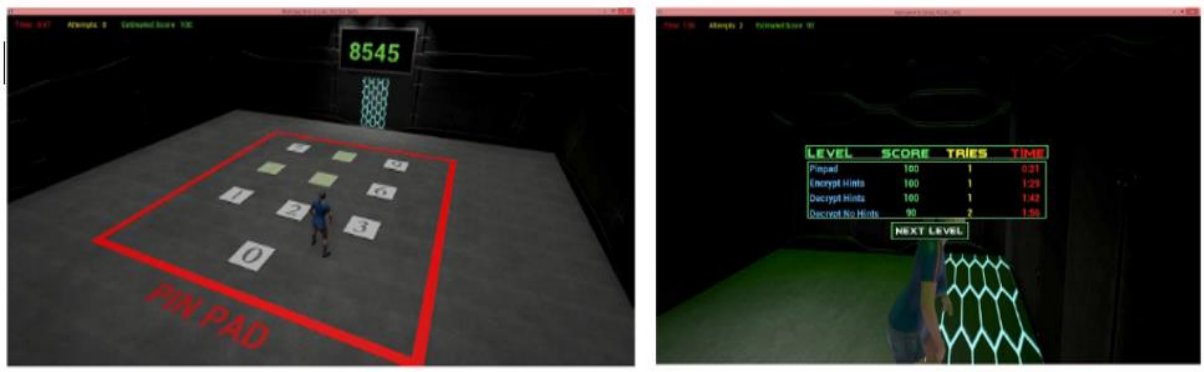


Figure 4. 3 Mobile puzzle game prototype (Dasgupta et al., 2013)

While the previous section focused on reviewing the games-based studies for cyber security awareness, this section would focus on reviewing the popular gaming applications developed for the purpose of learning various aspects relating to cyber security and threats.

4.4.1. Methodology

The application/ product search was carried out in November and December 2016 and updated in January 2017. The search was conducted using Google Play store, Google Search (UK), Bing, Apple App Store, and other popular gaming websites (www.gamespot.com; http://serious.gameclassification.com/). Only those gaming application focusing on cyber security were considered, and included for inspection if the information was freely available to assess their relevance (awareness; education) to the study. The search yielded 19 games, out of which 10 games were considered for review according to their relevance.

4.4.2. Review and Analysis

Various games have been identified which are related to specific aspect of cyber security or threat. Out of these 10 popular games- based on the ratings and review were selected and listed in Table 4.2, along with type, intended learning, and target audience.

Table 4.2 Popular Cyber security games

Authors	Game	Type	Audience	Intended Learning
(Department of Health and Human Services, 2017)	Cyber security contingency planning	2D –Click and turn based	Health Decision Makers	Data loss prevention
(Federal Trade Commission, 2017)	OnGuard	2D –Click and turn based	Teenagers	Online Security. Protection from viruses and malware
(Australian Department of Broadband Communications and the Digital Economy, 2017)	Buddie	2D –Click and turn based	Children	Online Security while browsing and social networking. Protection from viruses and malware.

(National Center for Missing and Exploited Children, 2017)	NSteens	Mini 2 D games – Click and turn based	Teenagers	Online Security while browsing and social networking. Protection from viruses and malware.
(cyber security challenge UK, 2017)	The Cyber security Challenge	National Competition (Physical role)	Students	Various topics including Online Security, prevention techniques, threats etc. Protection from viruses and malware
(Global CyberLympics, 2017)	High School Cyber Security Game - global cyberlympics	Global Competition	Students	Forensics, network security, threats prevention
(Information Assurane Support Environment, 2017)	CyberProtect	2D graphic game	Students and Professionals	Cyber security and information management

(McGoogan, 2015)	Cyphinx	Puzzles in virtual environment	Students and Adults	Forensics, network security, threats prevention, Cyber security and information management
(Federal Bureau of Investigation, 2017)	FBI Cyber Game	Puzzle	Children	Online safety management
(NOVA Labs, 2017)	PBS Cyber security Lab	2 D puzzle games with narrative scenes	Children	Scams identification and defending against various cyber attacks

Majority of the games are available for free and are mainly focused on teenagers, students and children. Corporate training games designed for professionals with more detailed threats awareness programs were found in ‘Cyber security Contingency Planning’ and ‘CyberProtect’ were awareness regarding data loss prevention, information management etc. was provided. However, no information was found regarding the effectiveness of any of these games in creating cyber security awareness.

Four games including OnGuard, Buddie, NSteens, The Cyber security Challenge were focusing on training related to safety from viruses and malwares, which are considered to be some of the major threats faced by the general Internet users. However, it is to be noted that only one game Cyphinx was developed for adults and the rest were for children and students. Therefore there is a need to develop games for general public who can use gaming as a means to enhance their cyber security awareness. The review has found that there are various games developed for specific issues relating to cyber security which are intended for children, teenagers and professionals.

4.5. Discussion

Cyber security is a wide area involving various aspects from software, hardware, human resources, operational processes, and psychology. Similar is the scope of security threats, which can be in various forms causing damages at different levels. Therefore, awareness and training is an effective approach in dealing with the threats of cyber security. Games, as discussed in the previous sections can be an effective tool in achieving this target. However, the concept of gamification for cyber security is relatively new and developing field. Threats can take various forms; however, the user need to be alert and aware of various precautions necessary in order to prevent any event of security attack. Usually the user side awareness includes recognizing web-based attacks, phishing and spam emails etc.

Various studies have been reviewed, out of which most of the studies have indicated positive results in using gaming technologies as a tool for creating awareness and training. However, few studies did not evaluate the games and few of them used small sample population in the studies. From the review it is evident that there is a need for in-depth and robust evaluations to conclude the effectiveness of serious games for cyber security, and also the need for using large sample population in these studies.

Few popular games available for raising cyber security awareness were also reviewed in this chapter. Most of these games are developed by governmental organisations or charitable intuitions. Most of these games were targeted at children or teenagers, and two of them for professionals. It was found that there are relatively few games focused particularly among the adult population in general. In addition, most of the games were focusing on general cyber security aspects, and issue specific games were not found. Therefore, there is a need for streamlining the game development according to the requirements and the types of security threats that are occurring frequently. In addition, there is a need for continuous monitoring and games updating necessary as there are new threats emerging every day.

From these reviews it was identified that though there are various studies supporting the positive impact of gaming in creating cyber security awareness, there is a need for regress study involving large sample populations to evaluate the impact and there is also a need for considering issue specific gaming applications to evaluate effectively which can help in concluding the impact of gaming technologies in cyber security awareness and training, as most of the studies reviewed focused mainly on general cyber security issues.

4.6. Summary

Understanding the concept of gamification and its effectiveness in raising cyber security awareness is the main objective of this chapter. It is evident from the systematic review that Gamification offers a potential option in raising cyber security awareness, and therefore there is a need to investigate how it can be used for creating issue specific cyber security awareness. For this purpose, the next chapter presents a design of 12 mobile games that can be used for raising issue specific cyber security awareness.

Chapter Five

Designing Issue-Focused Mobile Games

5. Designing Issue-Focused Mobile Games

5.1. Introduction

In the previous chapter from the systematic reviews, it was understood that the gamification can be used as an effective approach for learning thereby creating awareness about cyber security. It is important that the users are trained to be cyber security aware. An effective approach to achieve this is employing serious games that are designed to achieve a purpose along with entertaining the players. Serious games are considered to be effective in achieving impactful training and behavioural change among users. However, there is a need to understand the security aspects or threats and accordingly develop the awareness games. There are various types of cyber security threats. It is not possible to include all aspects in one game, and therefore issue specific games are needed for achieving better results and awareness relating to a particular type of security threat. Accordingly, the aim and objectives for this chapter include the following.

The main aim of the study discussed in this chapter is to investigate the use of gaming for creating awareness relating to a particular issue or cyber threat. In achieving this aim the following objectives are outlined.

- Understand the concept of GBL.
- Analyse the use of GBL in developing games relating specifically to a cyber security threat or an issue.
- Design 12 gaming concepts relating to different cyber security issues.
- A well-designed game enables the user to enter a virtual environment that is similar to the real environment and would enable the player to draw connection between the learning in the virtual environment to the real world.
- Identify the two most important and common issues that are faced by the public and select them for development and implementation.

The following figure 5.0. explains the process of study and how the games are selected for the study.

The Literature review has identified public security threats are one of the major cyber security threats prevailed across the globe. To address such threats, the role of users is an important approach, where they are educated with the cyber security practices to ensure safety. There are various approaches such as video based learning, training and education, game based learning etc. are identified for educating and creating awareness among the public.

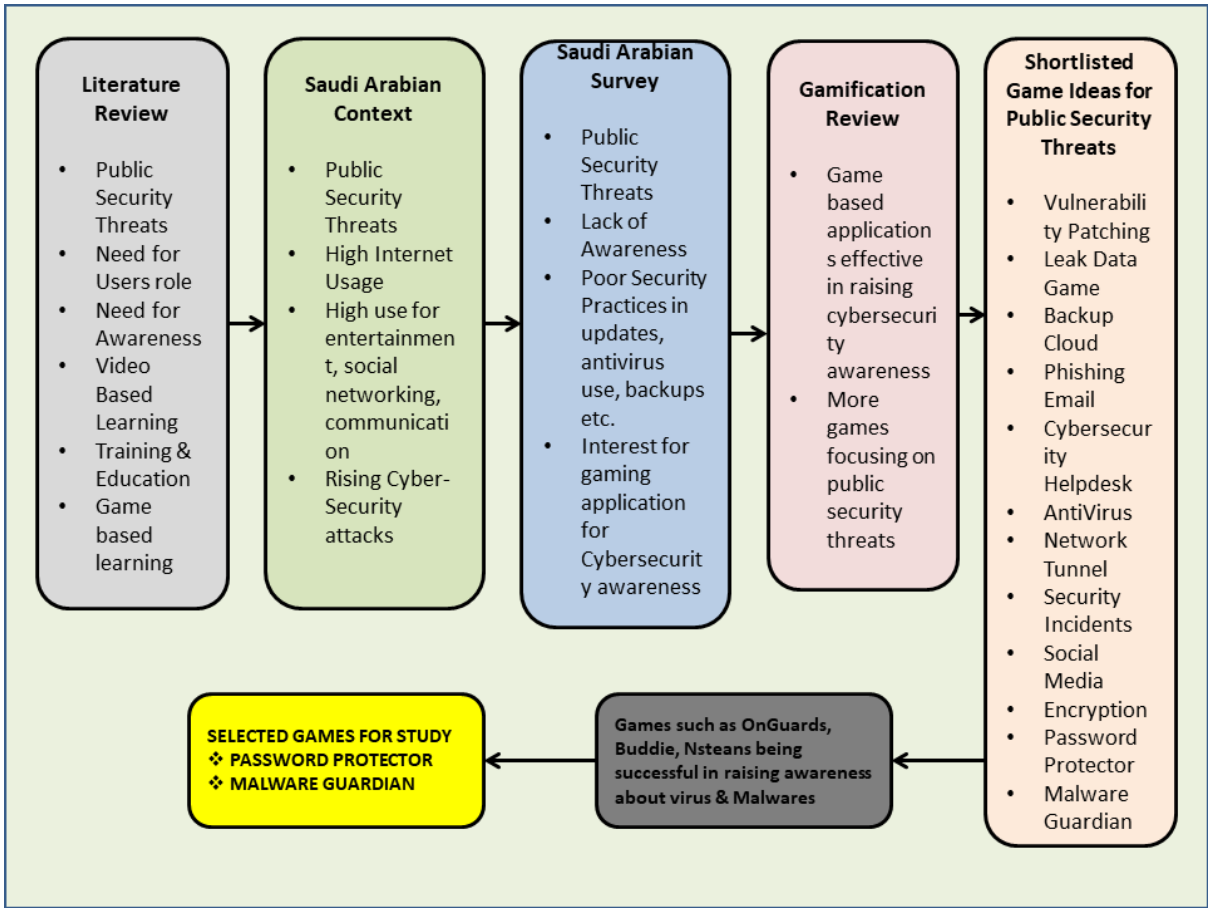


Fig 5.0. Approach for shortlisting games for creating awareness

Similarly, the review of Saudi Arabian case has identified that there is an increase in the cyber-attacks on various organizations and public users in the recent years. Public security threats were found to be increasing along with a rapid increase in the use of internet, especially for communication, social networking, entertainment

etc., which are highly associated with the risk of cyber-attacks. Accordingly, the survey results among the Saudi Arabian population have identified that public security threats as one of the major security concerns. Lack of cyber security awareness, poor security practices were identified as the major drawbacks among the Saudi Arabian participants. In addition, there is a high interest among the participants for using game based application for increasing cyber security awareness among them.

Focusing on this aspect, the review of gamification studies has identified that gamification can significantly improve the awareness creation and learning process; and also most of the studies focused on the public security threats such as phishing, vulnerability, security practices etc. Based on these findings, 12 gaming ideas for various public security threats were shortlisted. The literature review has also found that simple security aspects such as password protection, malware attacks as the major public security threats which are affecting the public to a greater extent. Accordingly, gamification review has found that few security games focusing on raising awareness about viruses and malwares were proved to be effective in other regions. Based on these points, two games including Password Protector and Malware Guardian were selected for the design and development in the study.

5.2. GBL

The approach of using games for training is referred to as games-based learning approach. These games are popularly used in school education. More recently, they are also adopted for healthcare, advertising, behavioural change, and cyber security training (Hendrix et al., 2016).

A key feature of games-based learning method is that it provides an interactive approach to train and educate users regarding the chosen topic. The games can impart or enhance the target skills of the players via a fun, engaging manner. The design of the games is flexible and can be adapted to meet the requirements of virtually every topic of interest for training (Boyle, 2011). Good games take the

player into a virtual world and simulate real world scenarios to connect the players to situations that might arise in the real world and its consequences. The player witnesses the consequences and would also be given tools in the games that they can engage to avert the consequences in the games. The player is rewarded for right actions and penalised for the wrong ones. This process encourages the player to use the correct tools and thereby empowers them with right knowledge that can be extended to the real world. The games-based learning method is not only engaging but also cost effective, scalable to cater to large number of users, and customizable (Trybus, 2014).

The games-based learning method has several advantages. The obvious advantage is that games-based learning method provides an interactive approach to train or educate the users about a specific program. It enables the players to acquire skills and to enable thought processes in a fun and interactive way. The adaptability and flexibility of games approaches enables to design the game to suit almost every training subject possible (Boyle, 2011). A well-designed game enables the user to enter a virtual environment that is similar to the real environment and would enable the player to draw connection between the learning in the virtual environment to the real world. The games-based approach would motivate the player to move towards the goal with required actions and also see the consequences without facing penalties in the real life. Further, when compared to the traditional method of training, games-based methods are more engaging, relatively cost effective, easily transferrable to a large number of trainees, customized to each player, etc. (Trybus, 2014).

GBL is a process which uses exercises (competitive/scoring) to motivate users in learning according to specific learning objectives (Teed, 2017). Usually the games involve an interesting and interactive narrative specifically designed to meet the learning objectives. Scoring is one of the major aspects of the game which is essential for developing the interest among the users. Another important aspect is GBL environment, which must be effective and encourage the users to learn and adapt (Oblinger, 2006). Many research studies were conducted and still being

conducted to analyse the impact of gaming in creating awareness about various activities in various fields. It was suggested that though GBL do not result in better performance in some instances, they do not generally result in worse performance, and may have additional benefit of a more positive attitude toward the subject of GBL. The performance in GBL can be attributed to various aspects including its environment, visual appeal, interactivity etc. (Ke, 2008). It was found that using immersive environments in the game, where all the said aspects were effectively designed would result in significant improvements in the learning aspect of the users (Virvou et al., 2005).

5.3. Concepts designed for cyber security awareness through GBL

A few research studies have shown that games can be used to impact security awareness (Denning et al., 2013; Gondree et al., 2013; Nyeste et al., 2010). This study approaches the games-based learning in a manner similar to brain-training apps. The games in this study are designed to engage the players in short activities frequently, eventually leading to enhanced cyber security awareness. To develop the games for training, 12 potential game concepts were shortlisted at the conceptual stage. These games were based on the security aspects that the end-users would likely encounter, and the concepts which they need to be familiar with. An overview of these games is presented in this section. The process involved outlining the security learning/awareness objective, key elements of the gameplay, and a storyboard level design of the game.

5.3.1. Vulnerability Patching

The main aim of this puzzle game is to educate the players about fixing vulnerabilities. In this game, different vulnerabilities are presented on the screen as cracks, which will spread over a period of time. Player needs to stop it from spreading by taking appropriate security solution steps, which involves in applying appropriate patch to fix it. Various cracks keep on appearing on the screen and the player needs to act quickly because the more time he takes to fix one patch new ones will start to appear even more rapidly. As the time progresses the difficulty

increase in terms of more complicated vulnerabilities will start to appear on the screen, which takes more time to solve. A prototype of the game is shown in Figure 5.1.

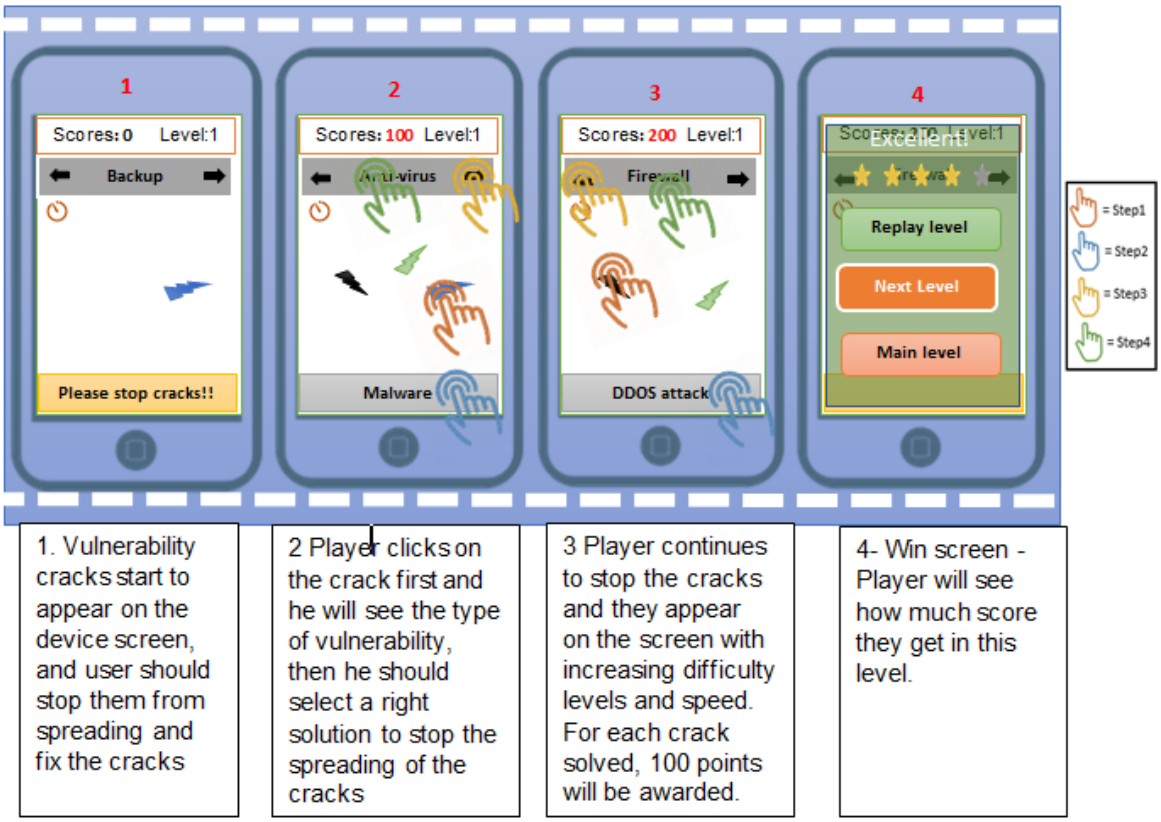


Figure 5.1 Prototype Model of Vulnerability Patching Game

The goal for the player here is to fix the crack in shortest period of time by following the correct procedure to apply the patch. Throughout the game the player will acquire new techniques (patches), which will help him to fix the vulnerability more quickly.

5.3.2. Leak Data Game

This is an action and tactic based game outlined with an objective of training the users about the importance of data privacy and security and intends to train them about being aware of leak data and type of data being collected from their devices. A prototype model of the game is shown in Figure 5.2. The aim of this game is to

rising awareness among the users that need to be aware about the importance of data privacy and the type of information being collected from their devices from Internet. The idea behind the game is to represent the data transfer between the user device and Internet in the form of network packets.

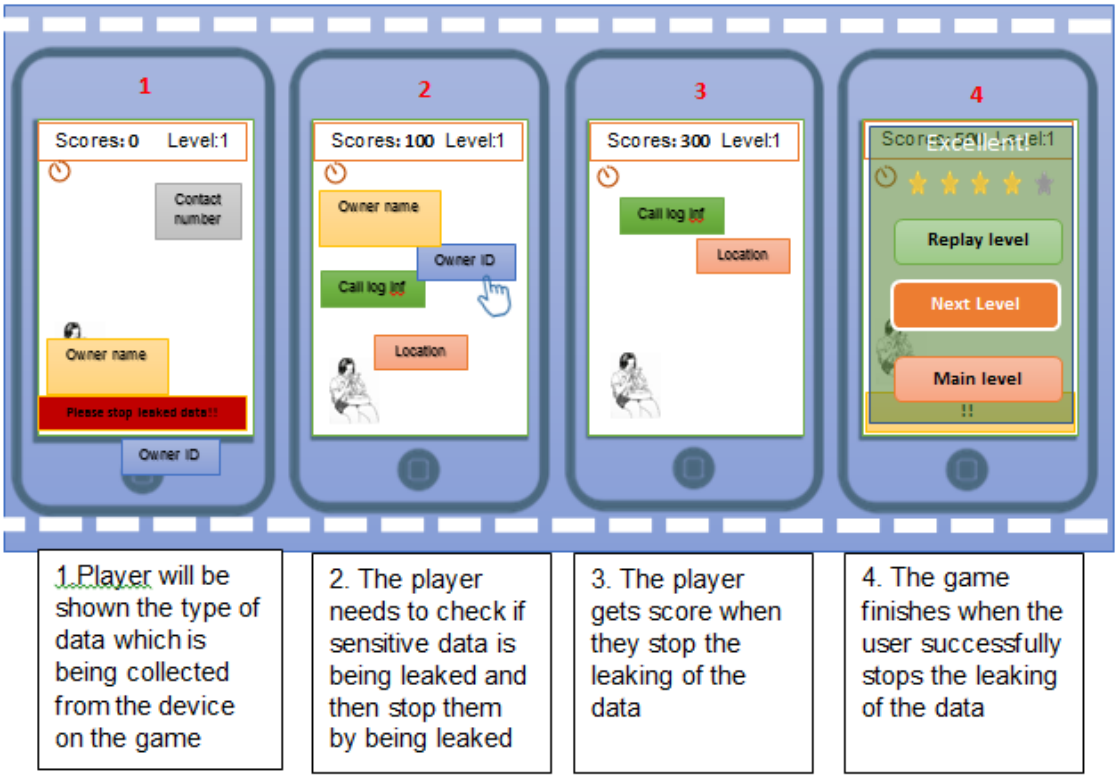


Figure 5.2 Prototype Model of Leak Data Game

The type of data being transferred in the network packet will be illustrated to the user. For instance, the data being carried from the network packet maybe something like user location, banking details, user`s personal information, pictures, etc. The user needs to decide which popping network packets need to be allowed to Internet and which popping network packets should stop leaked onto Internet.

5.3.3. Backup Cloud

This is a puzzle game outlined with an objective of creating awareness among players about the importance of taking backup of their files. The focus of this game is to train the players about the importance of data backup. In the game, the user

will be provided various scenarios in which they are required to store the given files according to the file type into their appropriate folders in the cloud. As the game proceeds the difficulty level of the game will be increased. In the next level, the number of file types will be increased to sixteen types but the number of folders in the cloud will be same, i.e. eight folders in the cloud. The prototype model of the game is shown in Figure 5.3.

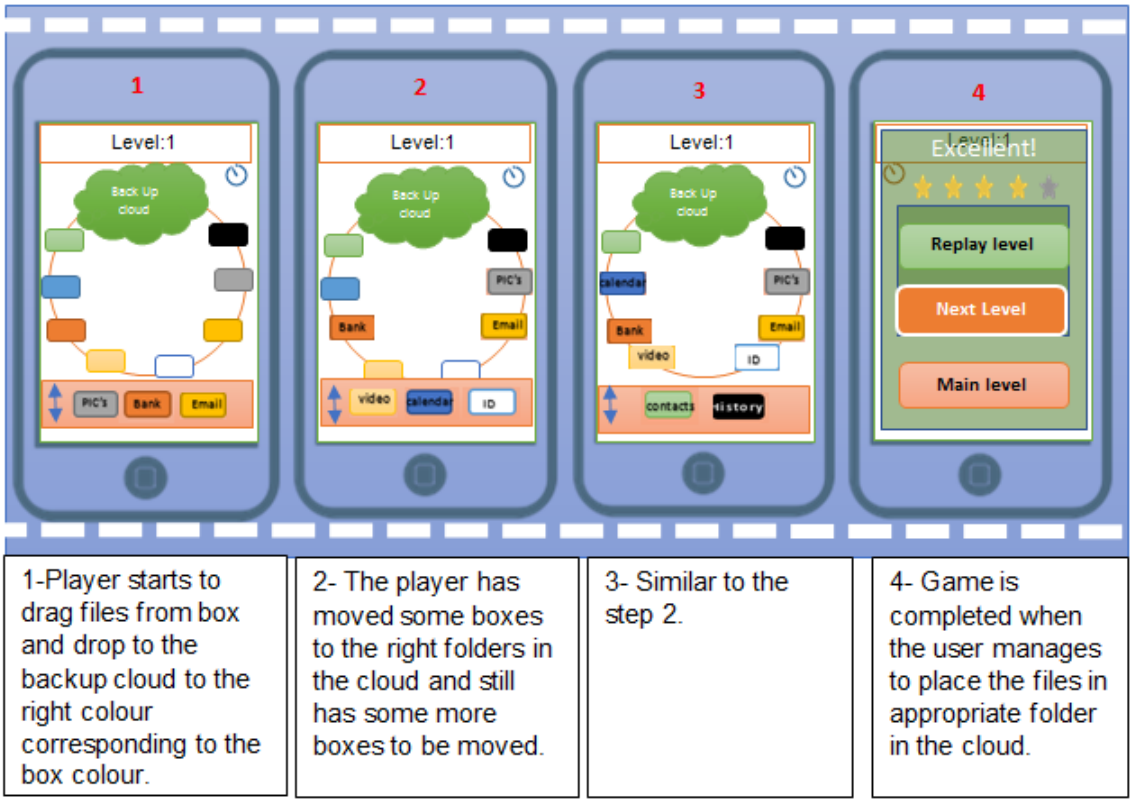


Figure 5.3 Prototype Model of Backup Cloud Game

This game enables the players to be aware about the concept of taking backup of important files. The game focuses on training the players to better manage their cloud system that are generally limited in space. It trains them to save more space for important files when there is a shortage of space. It is a tricky puzzle game, which trains the users on prioritizing the files for backup based on their importance, and challenges player`s decision making abilities.

5.3.4. Phishing Email

This game aims at enabling the users to identify phishing emails from legitimate emails and take appropriate action such as deleting the phishing emails. This is an interactive action type game where the user is posed with a list of emails on the screen with different types of email contents. The email list scrolls on the screen with different content types. The user identifies if it is a phishing email and drags it to the left to bin it and drags it to the right if it is a safe email. A prototype of the game is shown in Figure 5.4. This game addresses one of the most common types of cybercrime carried out via emails. The game trains the users and enhances their awareness about identifying the safe emails from phishing emails.

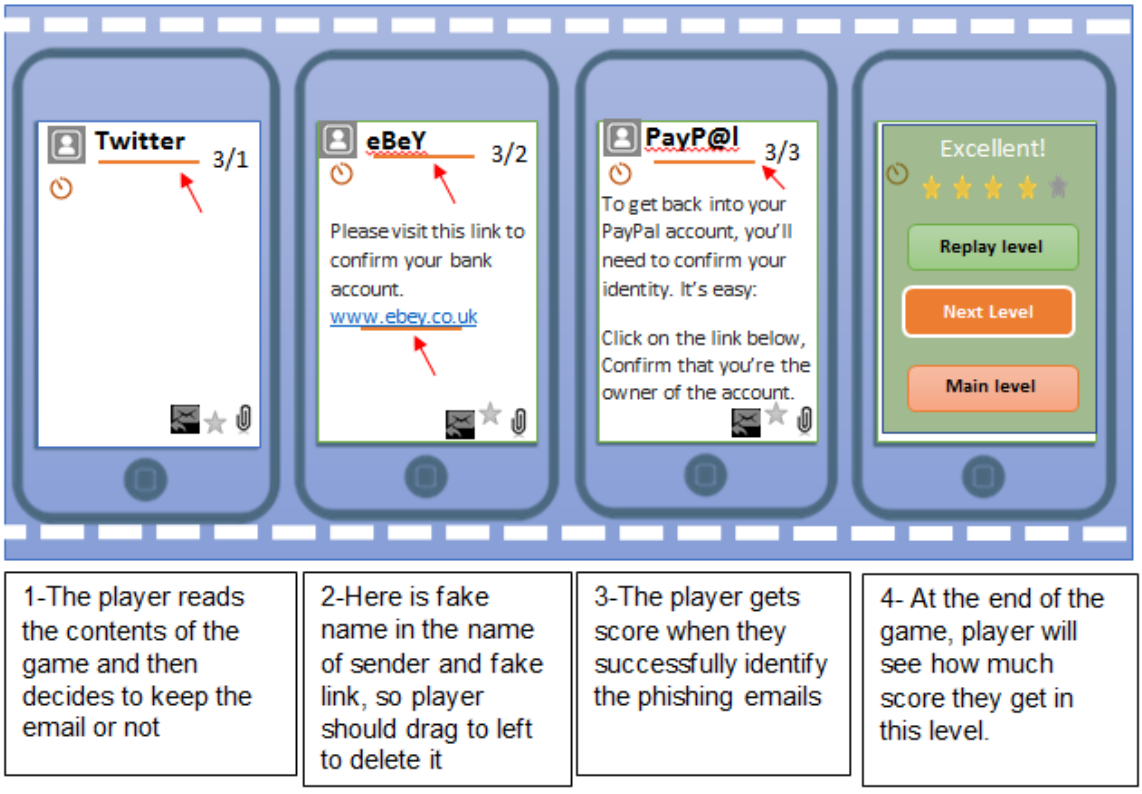


Figure 5.4 Prototype Model of Phishing Email Game

It would give a general idea about how not to trust phishing emails and avoid sending personal information by responding to such emails. This is a puzzle game which involves analysing contents in detail. The user is trained to decide whether

an email is secure or not, using an interactive interface where emails are swiped right or left.

5.3.5. Cyber security Helpdesk

This is a puzzle game, where the player would be enacting the role of a cyber security support worker. On the game interface, there is a computer network with different types of computing devices connected to the cyber space. The computing devices might be facing a cyber security issue and is indicated on the screen by the presence of a “happy” or “sad” emoticon on the computing device. The user needs to identify the “sad” device and investigate the cyber security issue the device is facing. In the game interface, first there will be a network with computers and the player identifies the computer with an issue and selects it. After this step, the issue faced by the device will be shown on the screen. The user needs to select the right solution for the issue. As the game progress, the number of devices and issues would be increasing. The player would gain points for selecting the right solution and would lose points if he selects wrong solution or does not select any solution in the given time. A prototype of the game is shown in Figure 5.5.

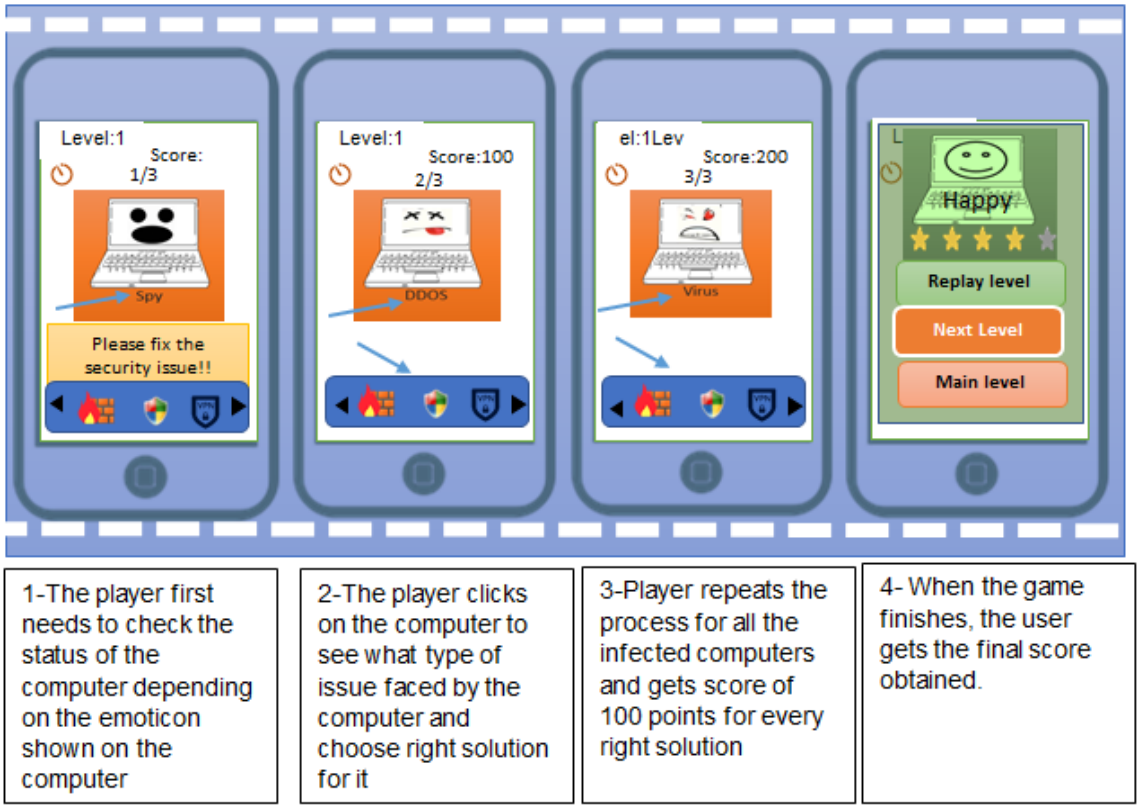


Figure 5.5 Prototype Model of the Cyber security Helpdesk game

This game is expected to train the users about choosing right cyber security solutions for a given issue. It is expected that the user will learn the ability of making correct decisions in a swift manner and also realize the risks and importance of addressing cyber security issue. It is a fast paced, puzzle game that will challenge the user`s decision making speed and familiarizes the user with different cyber security solutions.

5.3.6. Anti-virus

This is an action game with complex graphics in which malware attacks are posed to the player that needs to be stopped by the users using anti-virus update as ammunition. This is an action game where the player will encounter malware attacks. The setup will be of the user travelling on the screen in different directions where he will encounter malware during the journey that occurs in the cyber space. The user will be posed with malwares and viruses which the user needs to destroy to reach their destination. The user will be provided with ammunition which they

have to use to kill the malware or the viruses. The game will be a multi-level where the difficulty in each level increases with respect to time and the number of attacks. A prototype of the game is shown in Figure 5.6.

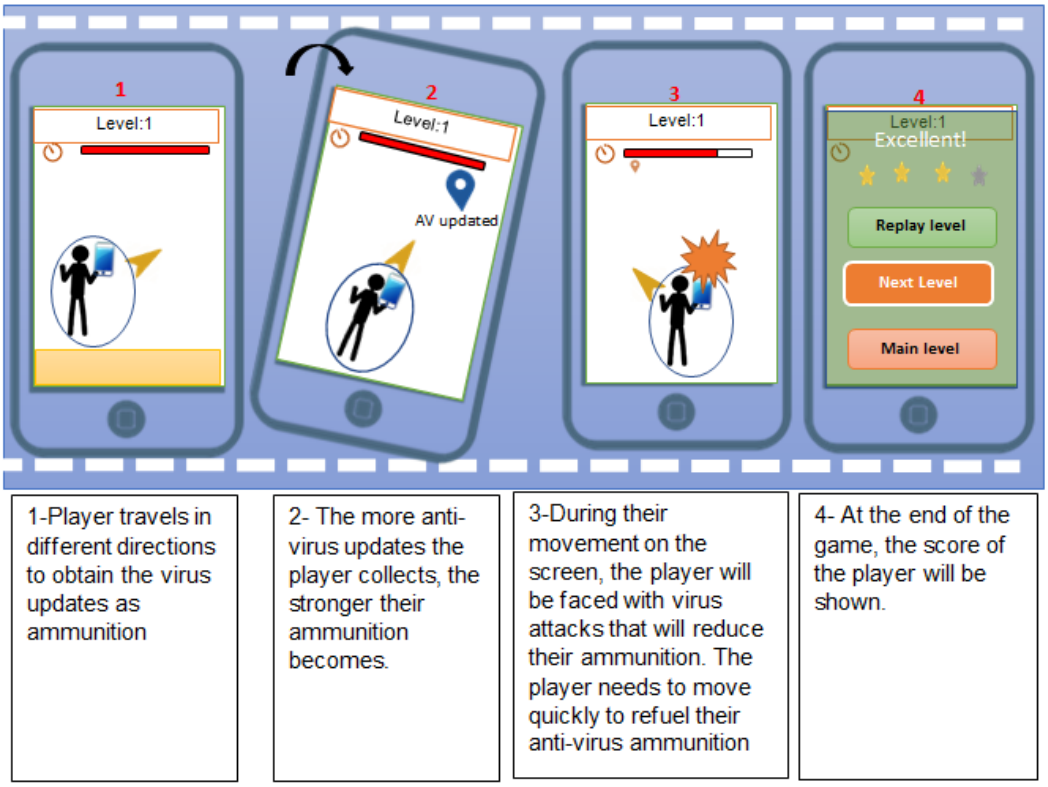


Figure 5.6 Prototype Model of the Anti-Virus game

The game will be fun because the attackers would be dynamic and be able to avoid the shooting of the player. Hence, the user needs to be careful while choosing the target and destroying them. The game maybe made complicated by having non-threatening objects such as files or required software which the user should not shoot. If the user shoots such file he will lose points as well as part of their ammunition.

The game will familiarise the user with the viruses and malware concepts and also train them about using anti-virus and anti-malware solutions in a fun, action filled way. It will also help them understand the importance of identifying the threats from the non-threats. It is a fun-filled action game, that will include attractive and thrilling

graphics, and it will be more attractive due to the shootings and action provided. It would familiarise the user with the anti-virus concept and actions required.

5.3.7. Network Tunnel

This is an action game where the user, with his devices, travels through a simulated computer network connection and encounters threats along the way in the network.

Figure 5.7 Prototype Model of the Network Tunnel game

The user will be an animated person and the player will be able to control the movement of the animated person through the up, left, right, and down arrow keys on the keyboard. In the simulated network there will be security issues which will be faced by the player such as virus or malware issue and the user then needs to choose right solutions to fix the issue using solutions such as anti-virus, firewall, etc. A particular situation the user will encounter while travelling through the network is getting connected to different Wi-Fi networks. When the user is connected to a public Wi-Fi, then the user is required to choose right solutions such as VPN and firewalls to increase their security against cyber threats. A prototype of the game is shown in Figure 5.7. The game intends to familiarise the users with different types of threats and vulnerabilities in public and private networks. The game uses interactive graphics to make the game more engaging. A familiarity with the malware would create more awareness amongst the users about different types of threats that exists and inform them how protection measures can be taken against those threats. This in turn would enable the user to identify the different type of threats that they may encounter in the real world and hence be prepared for it. It is an action filled fun game with attackers being different types of malware, which includes complex animations and interactive graphics. The user is familiarised with different types of malware.

5.3.8. Security Incidents

This game is about training and raising awareness amongst the users about incident reporting practices by challenging the user to take right measures when faced with a cyber security incident. This is a puzzle based game that aims at educating players about cyber security incident reporting practices. In the game the user will be posed with a cyber security incident on the game screen to which the user needs to determine the appropriate incident reporting practice. For a given incident shown on the screen, the user will be given four choices of incident reporting measure. The user needs to gauge the incident shown and choose an appropriate option to report the cyber security incident. There will be a time

restriction on the game of 30 seconds within which the user needs to decide the right option. A prototype of the game is shown in Figure 5.8.

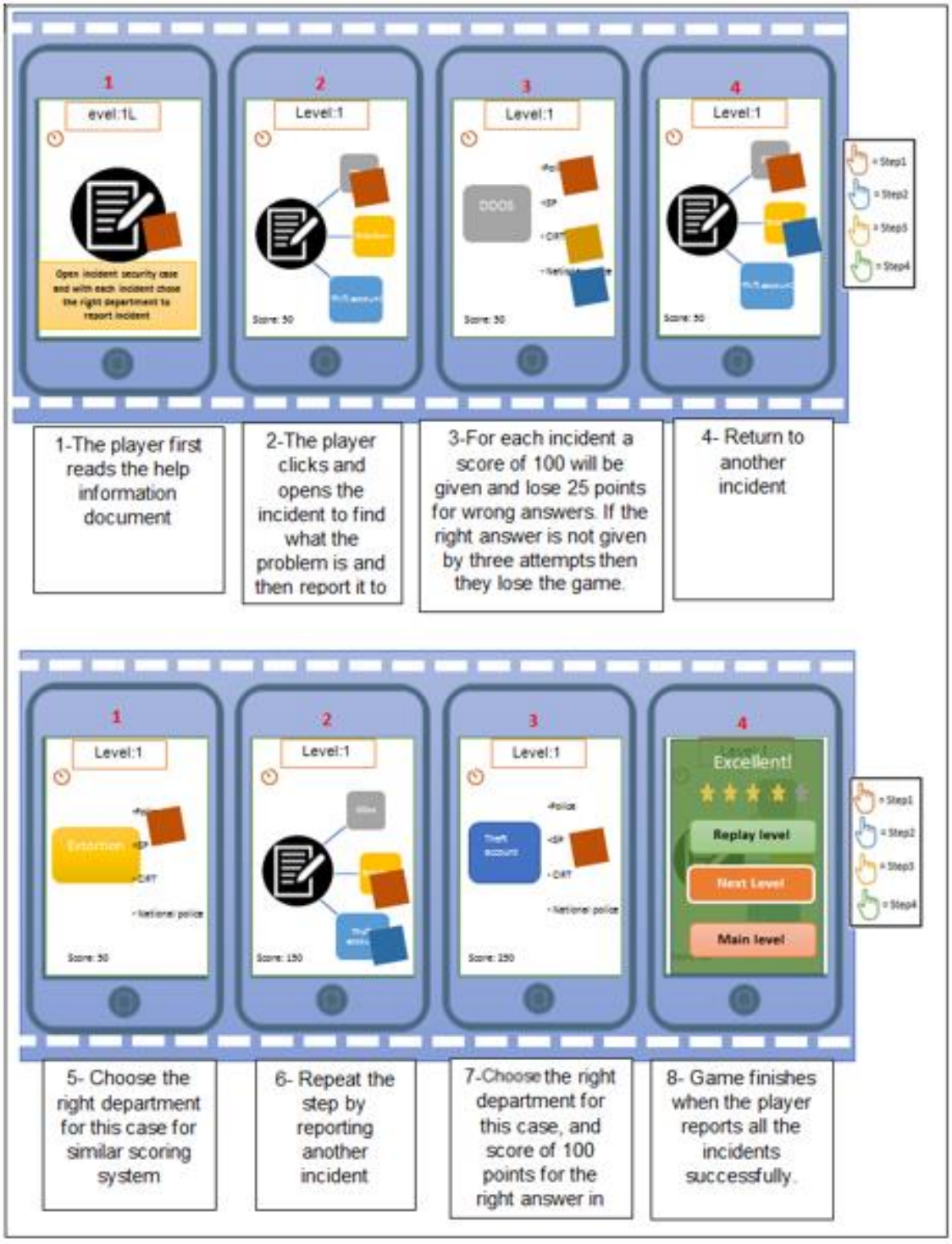


Figure 5.8 Prototype model of Security Incidents

Through this game, the user will be able to identify best cyber security incident practices and be more aware of various options available when faced with an incident. Another learning aspect would be making the user familiar with various cyber security incidents and enable them to identify the types of incidents by including various types of incidents in the game. The fun factor of the game is maintained by using appropriate graphics, sounds and special effects for a friendly user visual interface and the player will use on screen buttons to take desired actions. It is a fun filled puzzle game that trains the users on incident reporting practices, and it challenges player`s decision making abilities.

5.3.9. Social Media

This game aims at enabling the users to decide what type of posts are appropriate to post on social media. This game would create awareness about the users to be cautious while using social media. Updating personal information on social media is very common these days and it is important that the users are cautious while posting such information. In this game, the users will be posed with different examples of social media posts and they are asked to decide if posting such posts is safe or not. As shown in the above Figure, on the player`s screen, an example social media post will be shown. The user needs to decide whether this post is appropriate to be posted on social media or not. The user swipes right to accept the example post or left to reject it. The prototype of the game is presented in Figure 5.9.

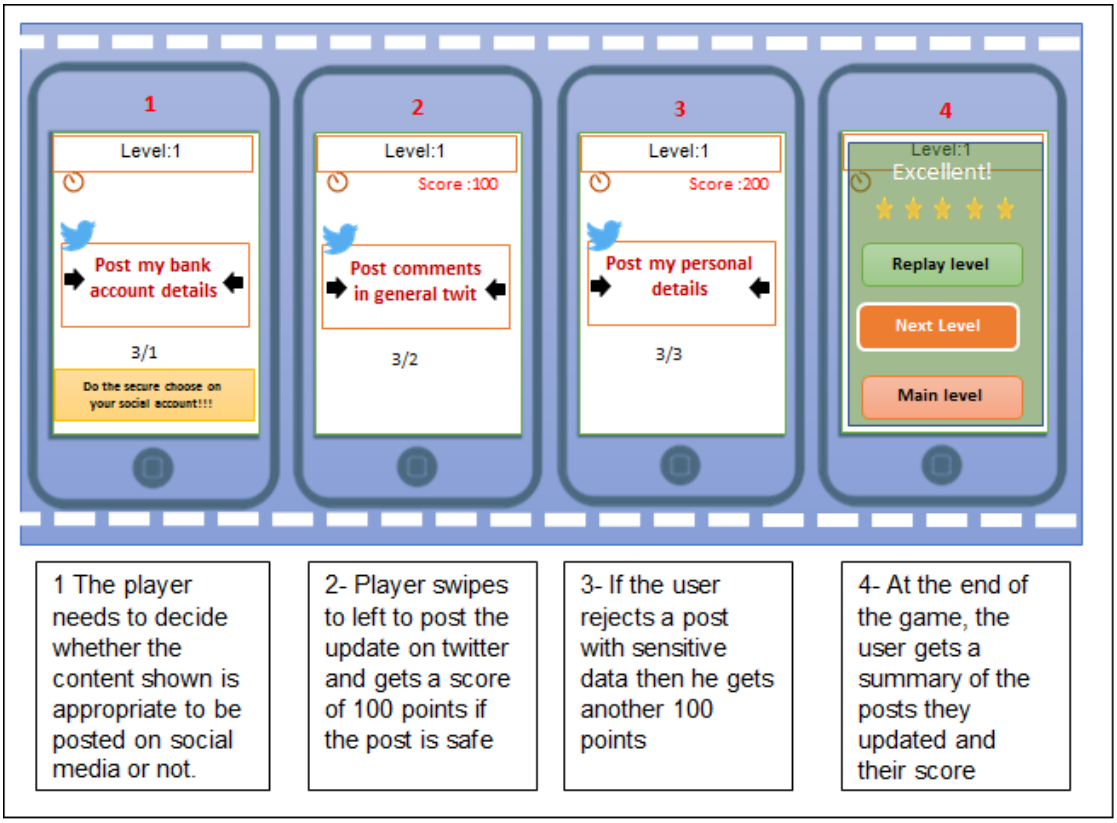


Figure 5.9 Prototype Model of the Social Media game

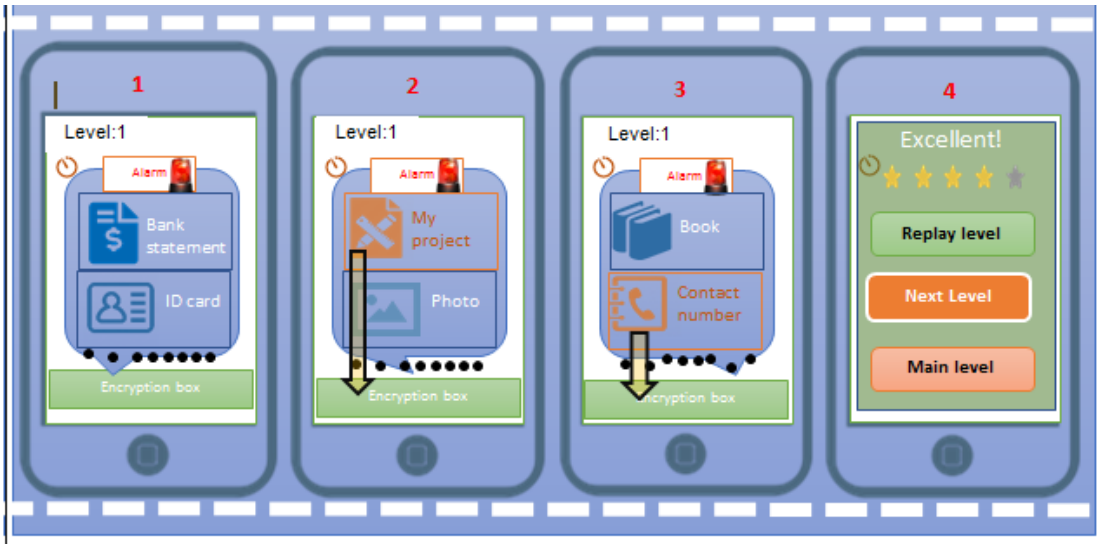
This game creates awareness amongst users about the importance of being cautious and thoughtful about the information shared on social media. It trains the user to be safe rather than risk sharing personal information that may potentially reach malicious people. It is a puzzle and tricky game that creates awareness amongst users about safe and unsafe social media posts and explains associated risks with certain social medial posts.

5.3.10. Encryption

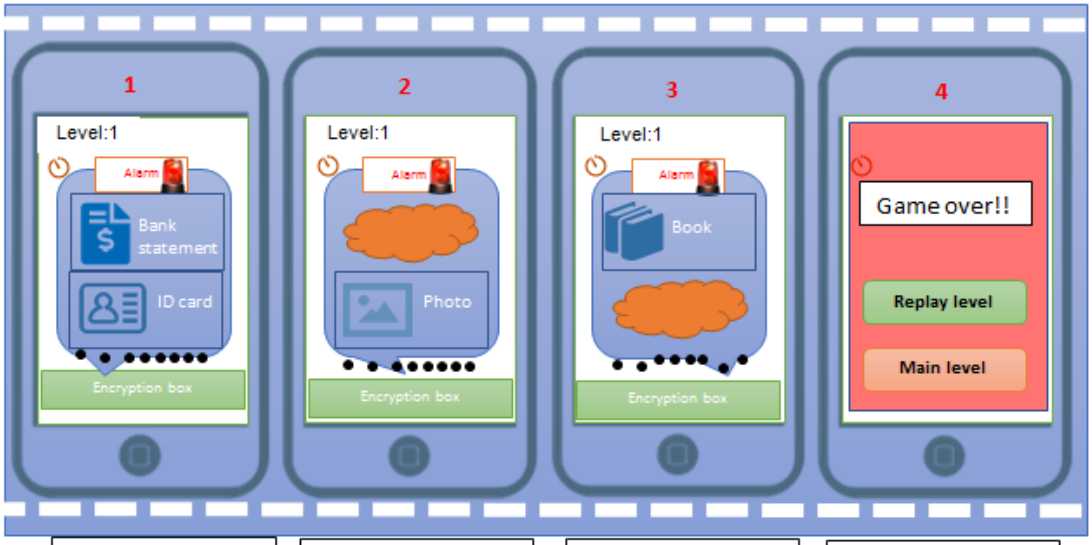
In this game, the user learns the importance of encrypting the files using different encryption methods. The game trains the user about encrypting files which is an important security practice against cyber threats. This is a puzzle and action type of game. On the user screen, there will be a set of different files from which the user identifies the files that are flagged with an alarm notification that needs encryption. There will be an alarm icon on the screen that indicates that there is a

file on the screen that needs encryption. The user needs to find the important file and drop it in the encryption box. An alarm will flash on the top of the screen when there is an important file in the page. The user then needs to find the important file and drop it into the encryption box. Once all the files are encrypted, the screen will move on to next page and then beep an alarm if there is a file that needs to be encrypted. For instance, files such as bank statements or company reports needs to be encrypted. The user needs to identify the important files within a given time constraint. A prototype of the game is presented in Figure 5.10.

This game would create awareness about the importance of encryption among users. Encryption is an effective measure against cyber security attacks and hence is essential that the users are aware of this approach. This game would also train them on identifying files that can be vulnerable to cyber-attacks and hence encrypt them. It is a puzzle game designed to identify important files, create awareness and to train the user about the importance of encryption using an interactive, drag and drop features.



1- The alarm icon indicates to the player that he should start to find file on pages and drop it on encryption box	2- On this screen, the player finds file with red colour and needs to drop it before it disappears from the page.	3- Similar illustration as the previous step	4- When the game is completed, the player will be able to see the score they got



11- The alarm icon indicates to the player that he should start to find file on pages and drop it on encryption box	2- The difficulty level increases with time constraints. The file slowly fades out with time and disappears if the user does not encrypt on time.	3- Increased time constraints	4-The game ends if the user does not manage to encrypt the files within the given time constraints.

Figure 5.10 Prototype Model of the Encryption game

5.3.11. Password Protector

This game is designed with an aim to train the players to hone their password creation skills by training them on the aspects of what constitutes a strong password. A prototype of the game is presented in Figure 5.11. The game allows the players to practice strong password creation in a competitive context. The players are provided with a random limited set of characters from which the players are required to create best possible strong, memorable passwords. The standard password strength principles of long passwords with diverse set of characters are used as guidelines to define the strength of the password. The game is timed and the passwords created are rated via a password meter. The game has a threshold score for the password to be acceptable. Further, the created password should not just be strong but also memorable to the players. The players are required to repeat the password, to test the repeatability of the passwords they created. Additionally, the game is time constrained. The players have to create the password in a limited time for game rewards.

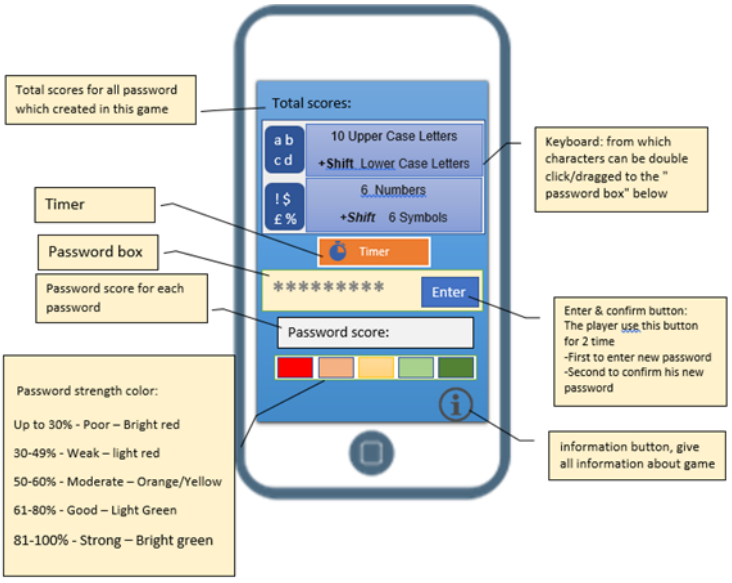


Figure 5.11 Prototype Model of Password Protector game

After creating the password, in the next screen, the user has to enter the password that was created. In order to get a high score, the user has to remember the

password. Additionally, a timer is provided in the game. There are currently four levels proposed for the game, where the difficulty level increases as the game progresses to the next levels.

5.3.12. Malware Guardian

The malware game will be designed and developed with an aim of educating the players about various types of malwares, the harm they would cause, and the necessary techniques of destroying them before they attack the system. A narrative approach is adopted in the game, with action sequences to make it attractive and to create interest among the players. The concept of game is based on destroying the various malwares that would try to attack the personal computer. The malwares are represented as bugs in the game. The malwares can move towards from multiple directions towards the computer on the screen. The player has to select the right method to kill different malwares. The methods describe the techniques to be used to destroy different types of malwares in reality. Therefore, every malware can have a different or a common method that can be used to destroy them. The prototype model of the game is shown in Figure 5.12.

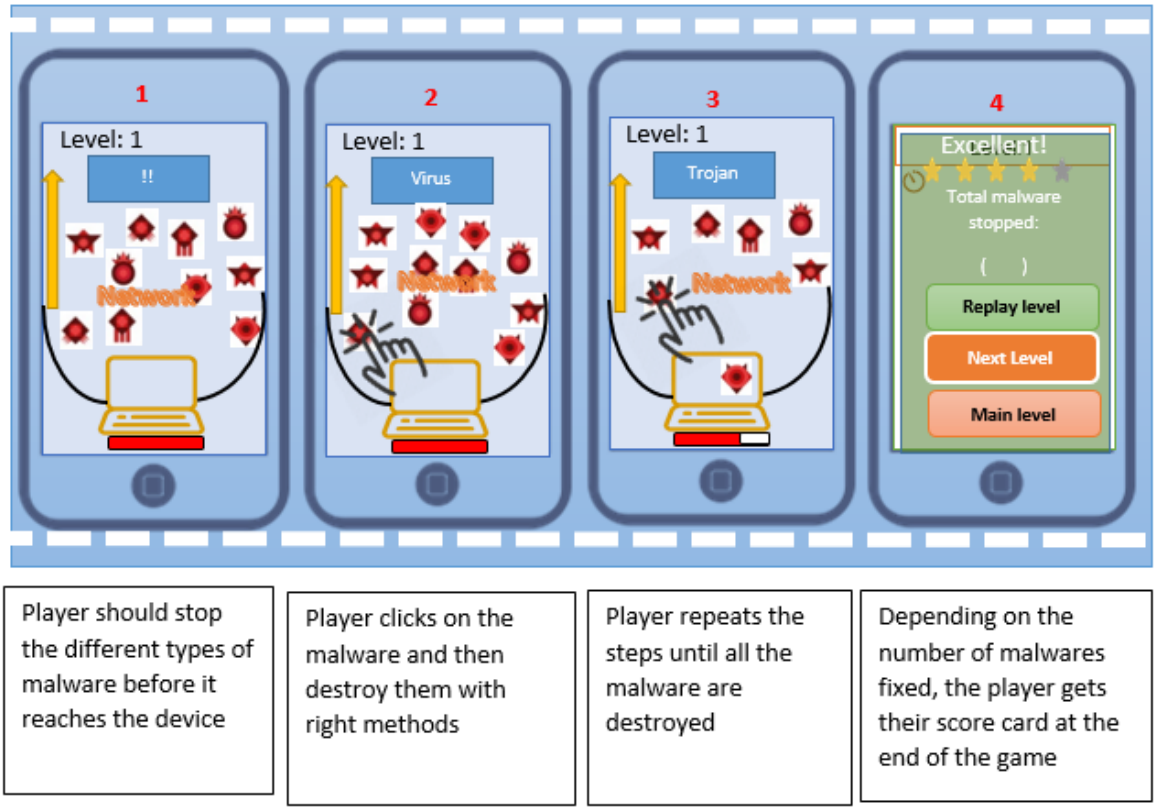


Figure 5.12 Prototype Model of Malware Guardian game

The directions in which the malwares attack represent the various ways in which an attack can take place. The player can kill the malwares by selecting the right method and clicking on the bug before it reaches the computer. The score is calculated depending on the number of bugs killed by the players. However, the time can be fixed to create more sporting spirit among the players, and there is also an option to deselect the fixed time for smooth play for the starters. The game is a multi-level game, where the complexity and the toughness increase as the game progress to next levels. Depending on the number of malwares fixed, the player gets the score, and ends the game.

5.4. Justification for selection of two games for development

For the final stage of the study, two mobile games are shortlisted. They are: The Password game and the Malware game. These two mobile games were chosen

because these games allow in raising awareness about two very relevant cyber security issues.

The password mobile game aims to train the adults to create more secure passwords. A survey in United States shows that around 43% of smartphone users use 4-6 apps on a daily basis (Statista, 2015). With the increased use of various applications, today`s Internet users is expected to use multiple passwords and is always recommended to use strong, complex, and unique passwords for each account. However, it is common among people to underestimate the importance of passwords and it is highly common for people to use single, simple passwords for multiple accounts. The one password approach for all accounts is very risky because an intruder can get access to multiple accounts if they manage to crack one password. Thus, it is very important that awareness about creating strong passwords is increased and the users are trained or learn to create a strong password.

The anti-malware mobile game aims to train the computer literate adult on identifying different types of the malwares that may possibly infect computers. This game was chosen over other games for the final study because, in survey results explained in chapter 3, it was observed that malware attacks were one of the most commonly occurring threats faced by users and as much as 45% of the survey participants informed that they were victims of cybercrime via malware attacks in Saudi Arabia. In a survey conducted by Paullet and Pinchot (2014) it was observed that 88% of participants experienced malware issues, however over 50% of them admitted that they were not concerned about malware and chose to ignore malware threats. They also employed poor cyber security practices that made their devices more vulnerable to malwares. Thus, to address this issue, the malware game can be an excellent tool for cyber security awareness training because the users would be introduced to different types of malware which gives them ability to identify different types of malwares. In the following sections, more details about these two games are outlined.

5.4.1. Password Protector Game

The password mobile game focuses on creating awareness about best practices for creating passwords. Creating secure passwords is possibly the simplest and sufficiently effective method of protection against cyber security. People are generally aware that creating secure passwords is important yet the attitude towards it is not very favourable. For instance, a survey presented in (Shay et al., 2010), over 400 participants agreed that creating complex passwords would make the account much safer and yet found the act of creating password very annoying. Thus, it can be seen that the attitudes of people towards creating secure passwords is not very favourable. The Password Protector game aims at training the players towards developing better attitudes for secure passwords.

There are several guidelines to create strong, secure passwords. An online search would provide several blog posts and articles from cyber security experts, companies, and governmental organizations on advising on best practices for creating strong passwords. However, there are no games found that specifically aims at creating awareness about strong passwords among users. Thus, the Password Protector game that will be designed in the study would be a novel attempt at creating awareness about the practices for secure password creation through a fun and interactive game.

5.4.2. Malware Guardian game

The Malware Guardian game focuses on training the users on the ability to identify different types of malware and then use specific Malware Guardian solution to destroy the malware. In the cyber space, different types of malware exist and often a single solution may not suit all types of malware. Thus, it is necessary that the users are trained about the different types of malwares that exists so that they can use appropriate solutions. Malware attacks are widely rampant in the cyber space. A report by the UK government indicates that 84% of the large organizations in the UK have faced malware attacks in 2015 (PricewaterhouseCoopers, 2015). Another report from Australia indicates that only around 65% of the users are

aware and understand the concept of malware (Parliament of Australia, 2010). Thus, there is not enough awareness and understanding of the malware among users. Further, a concern with the malwares is that malwares have the ability to stay hidden in the user`s devices and makes it detection or presence known difficult (Nazri et al., 2015). Hence, training the users about the malwares and its detection is important for enhancing the cyber security awareness.

There are few works that have created games to create awareness about malwares. For instance, a game named Malware Man was presented (Sercombe and Papadaki, 2012). This game includes an animated man and a series of questions to the user about the malware detection. If the user provides wrong answers then the animated man is burnt indicating the user lost the game. The contents of the questions or the focus area of the questions are not clearly available. However, the results showed that the game was able to increase awareness among users about malwares and phishing attacks. Another game, Cyphinx is designed for cyber security specialists where the game trains the specialists to find malware using knowledge of various security measures such as cryptography to find the malwares in the scenario (Metzger, 2015). This game is an advanced game and is specifically for cyber security experts. Further, (Arachchilage and Asanka, 2012) present a framework to design games to increase cyber security awareness. However, their game mainly focused on avoiding phishing attacks. There are several other games that have focused on providing malware training to users such as (OnGuard, Buddie, NSteens, The Cyber security Challenge) discussed in previous chapter, however, the target audience for these games have been children and teenagers.

From the literature reviewed, it was found that there were no works that are designed to train the users on the different types of malware. Thus, the Malware Guardian game that will be designed in the study would be a novel attempt at creating awareness about the different types of malware and the practices for malware protection through a fun and interactive game.

5.5. Summary

The chapter discussed various ideas of issue specific cyber security games focused on creating awareness. There are 12 different game designs that are discussed in this chapter, out of which the Password Protector and Malware Guardian game were shortlisted for the development and evaluation. Considering the most commonly occurring cyber security threats and the risks associated with the users, both Password Protector and Malware Guardian games are shortlisted. The next chapter would explain the design and development of these two games.

Chapter Six

Design and Development

6. Design and Development

6.1. Introduction

Previous chapter detailed the consideration of 12 major game ideas focusing on the cyber security issues, and the details of justification for selecting the two games including Password Protector and Malware Guardian. This chapter explains the design and development of both the games in detail. The design methodology explains the stages and development process. In addition, the design aspects are explained in detail using the use case and interaction diagrams, concluding the chapter with the explanation on the technologies used in the development of the games.

6.2. Development Methodology

Games development are similar to software development but with a slight difference in some stages. The game development in this study used the method prescribed by Jain (2017) and Jaggo (2016), and the development process is explained accordingly, which are shown in Figure 6.1.

Idea and Story: This stage focuses on the development of idea based on which the story would be developed. The story has to be effective and engaging in order to attract the more users. Especially in awareness generating games there is need to focus on enjoyability, usability and learning aspects. These features would form the main essence of the story development.

Conceptualise and Design: This section is used to explain the game concepts, levels design, user interface, player features etc. These aspects would reflect both high-level and low-level design features of both the games.

Technical analysis: This stage focuses on the technology infra structure (hardware and software) required for the development of the games. The programming languages, tools and techniques, game engine etc. are identified in this stage.

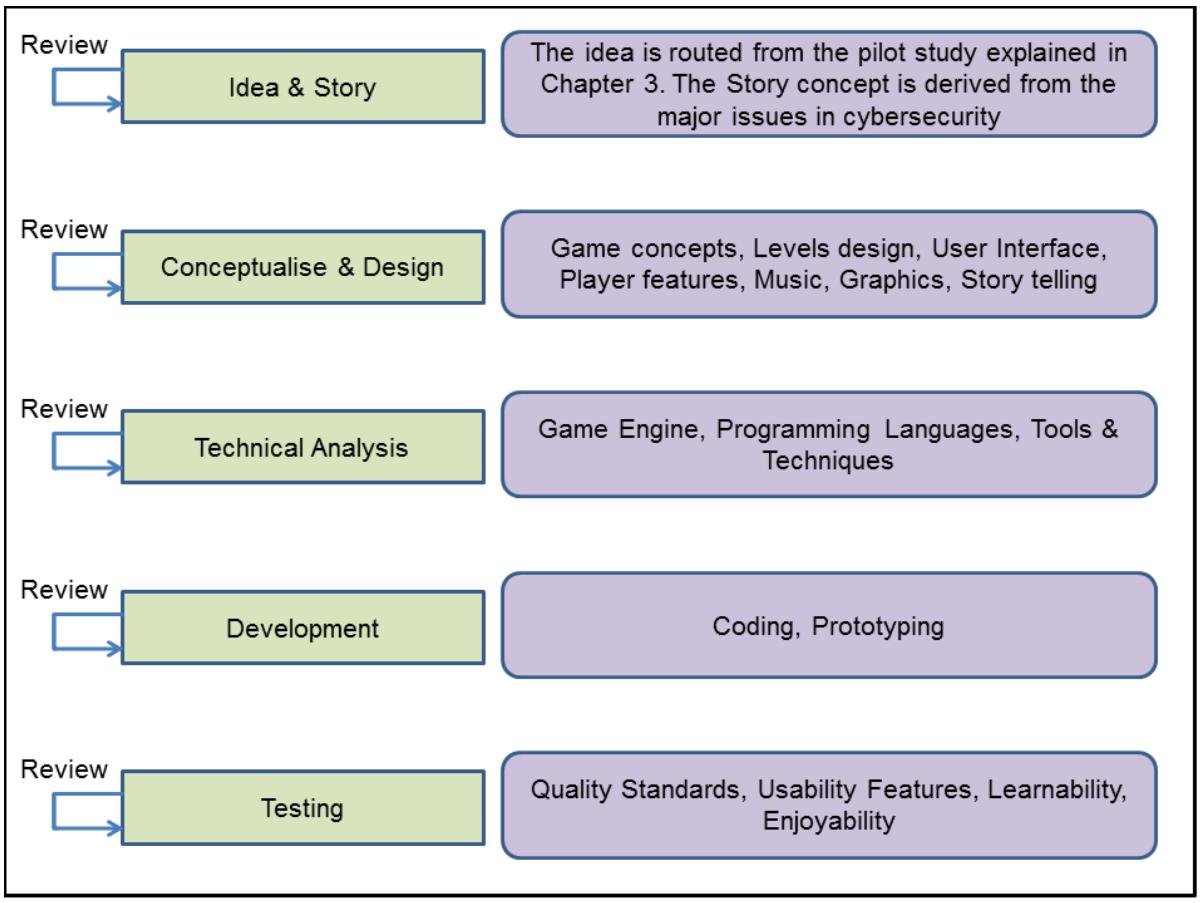


Figure 6.1 Stages of Game Development

Development: At this stage, the actual development of the game starts. A prototype model is built first, which is reviewed, and then the actual model is developed based by improving the design aspects and issues identified from the review.

Testing: The game is tested by the developers and testers, before it is actually released to users. Both unit testing and integration testing would take place. A beta testing process with actual users is conducted for both games as the part of study.

Evaluation: An online survey is conducted with the participants who used the games, and they are evaluated using heuristic evaluation techniques including the usability, enjoyability and learning aspects.

A review method is adopted at every stage to ensure the quality development at each stage and minimise the risk of errors and issues creeping in to the later stages of development. The development approaches individually for both games are explained in the next sections.

6.3. Password Protector Game Design and Development

Password Protector is an action game, which is focused on creating awareness about the password security in an interactive and enjoyable approach. The game aims at training the users to create complex, strong passwords. An important and a basic measure for cyber security is having safe and secure passwords. This game trains the user to create complex as well as memorable passwords. It will be an important learning aspect for the user and might be able to use this game training to implement in real life. The design and development of the Password Protector game is explained in the following sections.

6.3.1. Idea and Story

The idea for developing the game is routed from the pilot study conducted in Saudi Arabia, where majority of the participants preferred application type approach for creating cyber security awareness. However, there are various aspects of cyber security issues which are to be included in the awareness programs, out of which major issues and the games ideas relating to these issues are discussed in previous chapter. Among which two major issues including passwords and malwares are selected as the themes for story development. An overview of the game is presented in Figure 6.2.

The scenario of the game that is presented to the user is that they are required to create complex passwords that will be harder for an intruder to decrypt. The more complex password they create, the higher their score will be. The user will be presented with an interface where they select the letters into the box to create a password.

The scoring is based on the complexity of the password created. The trick for the users is to create a complex password but also be able to remember the password. Once the user creates a complex password, in the next moment, a blank box is displayed on the screen on which the user needs to re-enter the password. Hence, the user needs to remember the password they created.

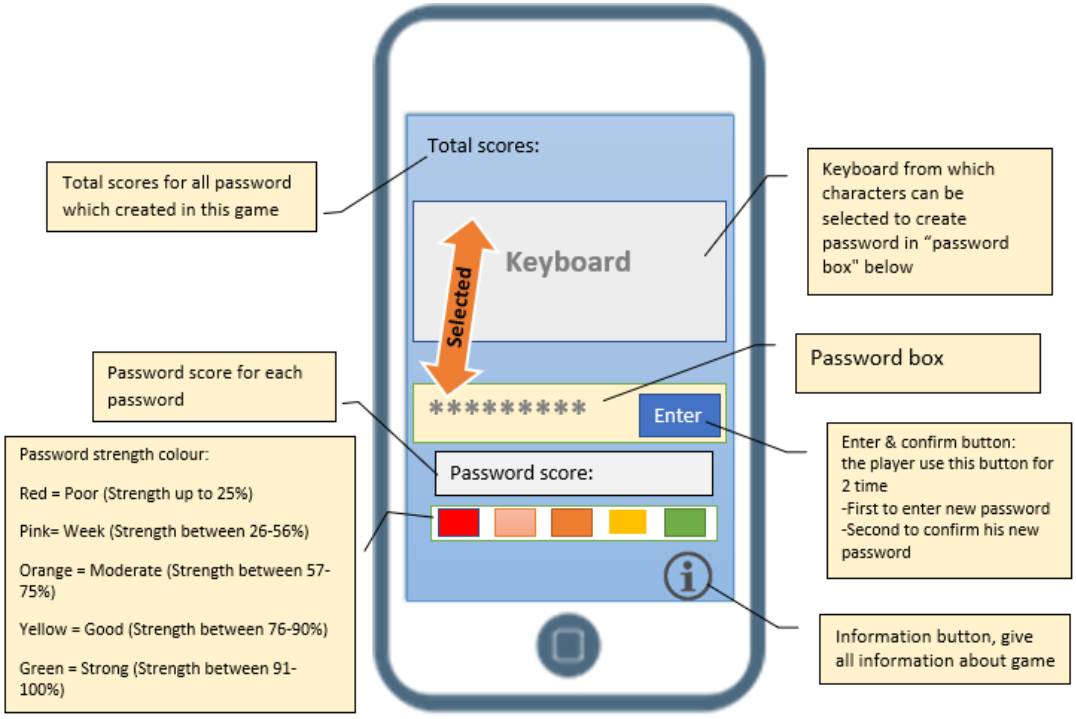


Figure 6.2 An overview of Password Protector Game

Further, in order to get a high score, the player will be compelled to create a stronger password. A timer will also be provided with different levels.

Additionally, Password strength colour function is designed to indicate the strength of the password to the users through the use of colour codes. Based on the same IBM guidelines that applies to define the complexity of the password, the colour code to indicate the strength of the password is defined based on the password complexity calculated. The purpose of the password strength colour function is to provide a technique where the password strength is indicated to the user as visual cues. Based on the combination of the different types of characters, numbers and

non alphanumeric characters, the password strength is determined. Further based on the determined password strength, the colour codes are used to indicate the password strength on the game interface. The game functions would make the game more exciting and thus more engaging to the user.

The first thing when the player starts the game is that he receives messages. The messages are informative and are aimed at educating the player about the importance of the password. This message/advice will be retrieved from the data bank of the bank where messages similar to the one showed in the above Figure are stored. At each level of the game and at different times when the player logs into the game, different messages will be randomly retrieved from the data bank of the game and displayed to the player.

Also, the message tells the player to not to use the previous password that they created previously as there will be a penalty in the game for repeating the password from any of the previous game. This message and penalty procedure aims at training the players to not to use similar passwords for multiple accounts. As using similar passwords to multiple accounts is a common practice, this approach in the game creates awareness among the players. This creates an enhanced awareness about the importance of password to the players. The informative message is shown in Figure 6.3.

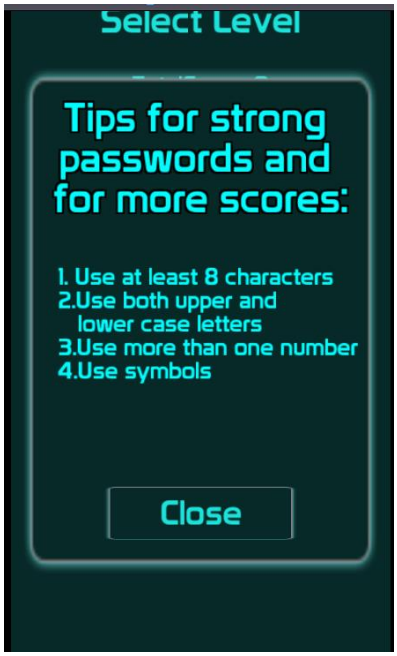


Figure 6.3 Password Protector Game Informative Message

The major aspect of the game is creating a strong password. The design concepts of the game for this purpose are explained in the following sections.

Password Creation: when the game actually begins and the player is asked to create the password. In each time, the creation of the password will be done in two steps. In the first step, the user will select the letters or characters and creates a password. In the second step, the user will be asked to re-create the password. This is done to check if the player is able to remember the password. When the player enters the correct password both times, the player will be provided a score based on the complexity of the score.

Scoring Technique: In order to get a high score, the user has to remember the password. Additionally, a timer option is provided in the game. There are currently four levels proposed for the game, where the difficulty level increases as the game progresses to the next levels. The available time decreases as the game proceeds to next levels. Level 1 (90 seconds), Level 2 (70 seconds), Level 3 (50 seconds), Level 4 (40 seconds). The scoring technique is based on the complexity of the password created. The password strength factors are calculated as per the

guidelines of Centre for Security, Communications and Network Research (CSCAN, 2016). The complexity of the password is based on the password complexity rules that are set out in the game. In the game, the password complexity rules are inspired from password guidelines provided by IBM knowledge centre and are defined based on the usage of characters from four characters, which includes the following

- Uppercase letters [A-Z]
- Lowercase letters [a-z]
- Number [0-9]
- Non alphanumeric characters (~!@#$%^and *_-+=`|\(){}[]:;'"<>,.?/)

The interface of the game is designed using vibrant colours and effective display of characters in order to effectively engage the players in the game.

Game Process: After closing the informative screen the following screen appears in the game as shown in Figure 6.4.

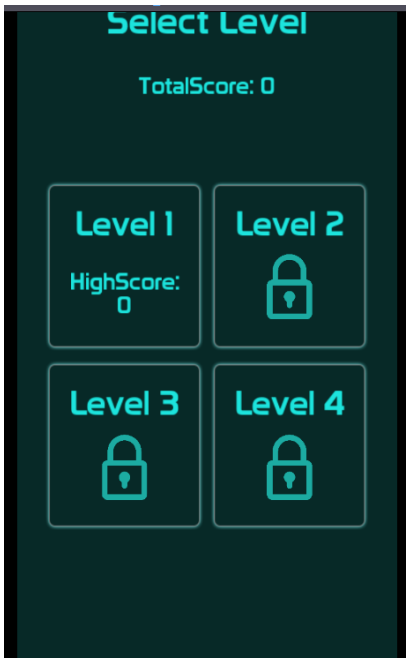


Figure 6.4 Home Screen of the Password Protector Game

The game process is depicted in Figure 6.5.

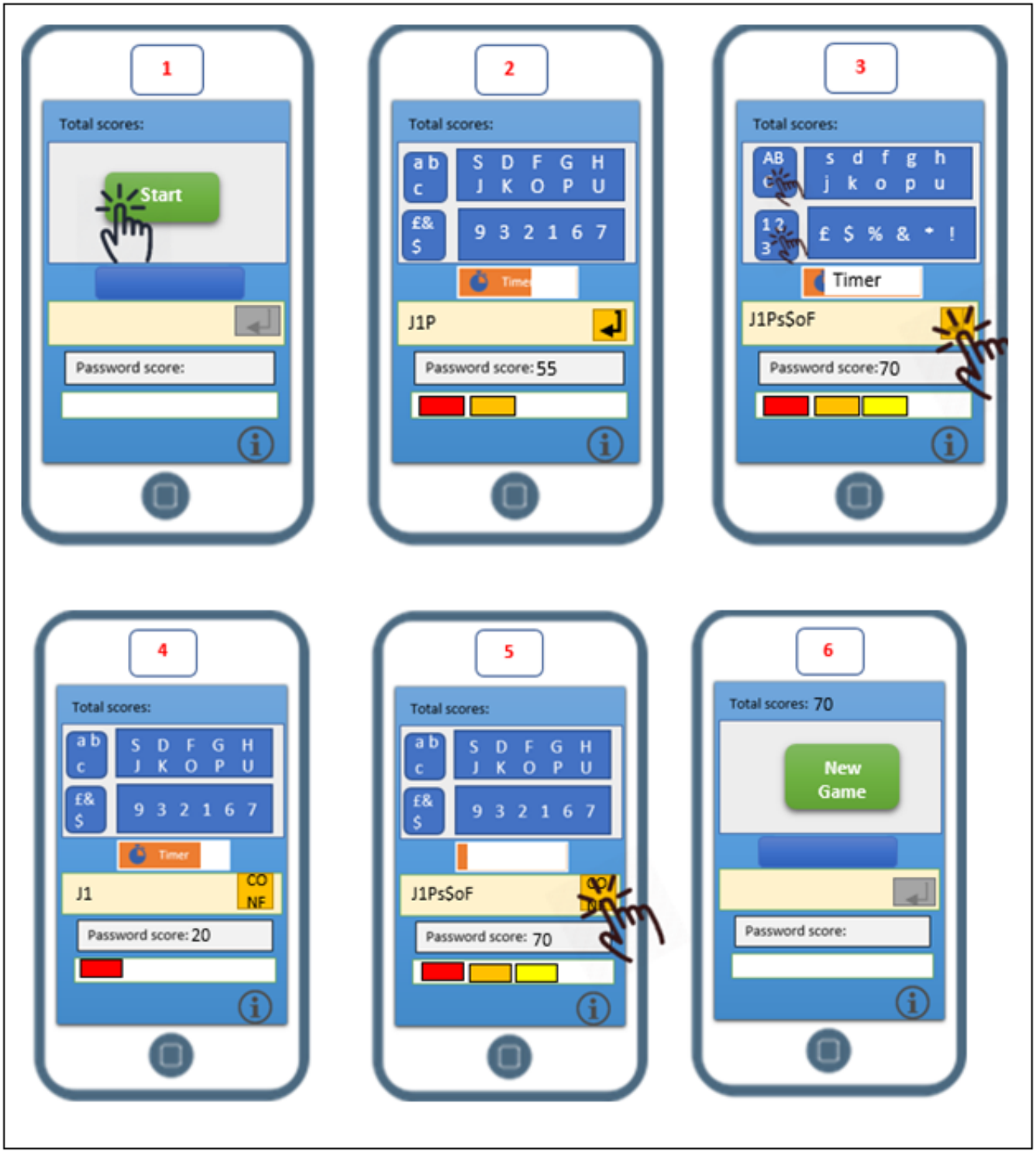


Figure 6.5 Password Protector Game Process

1. To begin, press start.
2. The timer will start. Player has 10 random letters and 6 random numbers and random symbols in separate boxes to select from. The user should select characters from either of the boxes and the same are appeared in the password box.
3. The player can select the Upper or lower case letters, numbers or symbols by pressing the buttons on the left. The user should press enter before the time runs out.
4. After pressing enter following the previous steps, the user should start with the same limit time and confirm his previous password.
5. The player should confirm his second password before the time runs out.
6. If the last step is correct then the scores will be totalled and the player can move on with next game.
7. ***Miscellaneous Situations:*** Such unexpected situations are presented in Figure 6.6., and explained below.

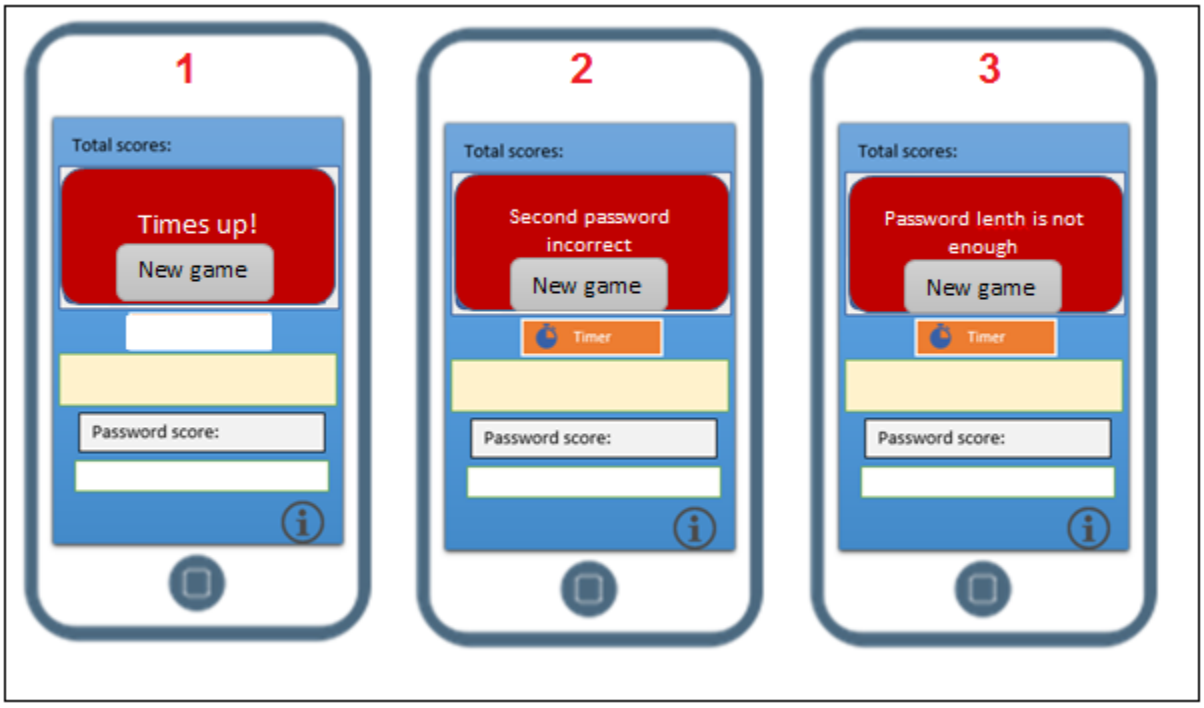


Figure 6.6 Miscellaneous Situations in Password Protector Game

1. Time Over: If the player does not enter both the first and second password, he will receive the message below.
2. Incorrect Password: This message will be received if the user types a second that does not match with the first one.
3. Password too short: This message will be received if a score of 50 or more is not achieved.

Game Levels: Each level has different set of conditions that are needed to be fulfilled in order to move to the next level. In each level, the number of characters to be used for creating the password is different from other levels. The complexity level remains same at all levels; however, the user need to create strong password based on different combinations to score more. The available time decreases as the game proceeds to next levels. Level 1 (90 seconds), Level 2 (70 seconds), Level 3 (50 seconds), Level 4 (40 seconds). Different combinations that users may use include numbers and letters; mixed case letters; letters, numbers and Symbols mixed case letters, numbers and Symbols. Based on the combination and the length of the password, the score is determined in each level.

User Interface: The game uses Graphical User Interface which is intended to be eye-catching and visually appealing, with attractive graphics, music, and touch sounds. The user interface of the game is shown in Figure 6.7.

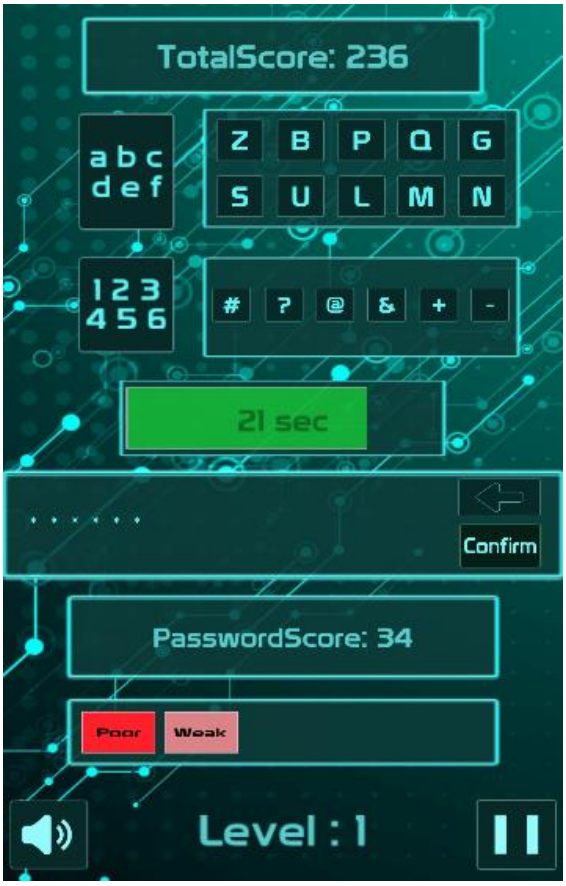


Figure 6.7 Password Protector Game User Interface

6.3.3. Technologies used for Password Protector

The following technologies are used for the development of the Password Protector game.

C# Language – The C-sharp language is used for the development of the game. The programming language is an object oriented programming that is used for making object functionalities in the game. Data structure techniques of programming is used for handing and manipulating data.

Unity3D – This platform is used for the development of the game. It is developed by Unity Technologies and is widely used for development of both 2D and 2D games. It supports the development of the game using C# language with support

for APIs for graphics. It facilitates easy deployment of games across different platforms including iOS and Android.

Adobe Photoshop and Illustrator – For the front-end graphical design and art, technologies such as Adobe Photoshop and illustrator is used. These tools facilitate art and design of the skin and look of the game along with other assets such as icons, animations, images.

6.3.4. Testing and Evaluation

Two types of testing are conducted in the study. A review approach at each stage of development is adopted to ensure the quality in the development and to mitigate risks and errors. The second stage of testing includes beta testing. In this process the game is played by the actual users from Saudi Arabia, and various aspects were tested including the awareness (increase in the knowledge about password security), and the aspects related to the game through heuristics evaluation including the various features like usability, learnability, and enjoyability. The analysis and evaluation process are explained in the next chapter.

6.4. Malware Guardian Game Design and Development

The intention of the game is to familiarise the user with different types of malware present in the context of the cyber security. This would create more awareness amongst the users about different types of malware that exists and inform them that such malware can be treated. This in turn would enable the user to identify the different type of malware that they may encounter in the real world and hence be prepared for it. The design and development of the Malware Guardian game is explained in the following sections.

6.4.1. Idea and Story

The Malware Guardian game is an interactive game-based on a scenario where a computer is a character and the computer`s assistant named Malware Guardian keeps the computer safe when it is communicating with the cyber space. The

scenario in the game is that the computer receives file from cyberspace and the player needs to scan the files with the Malware Guardian to deduce whether the file is safe/unsafe. An overview of the game is presented in Figure 6.8.

In the game, the player role plays as a computer protector by scanning each file with the Malware Guardian agent and verifies whether the file is a malware or not. If the file is a malware, then the player destroys the file and minimizes the threat to the computer. On the other hand, if the file is safe, then the player need not take any action after the scan.

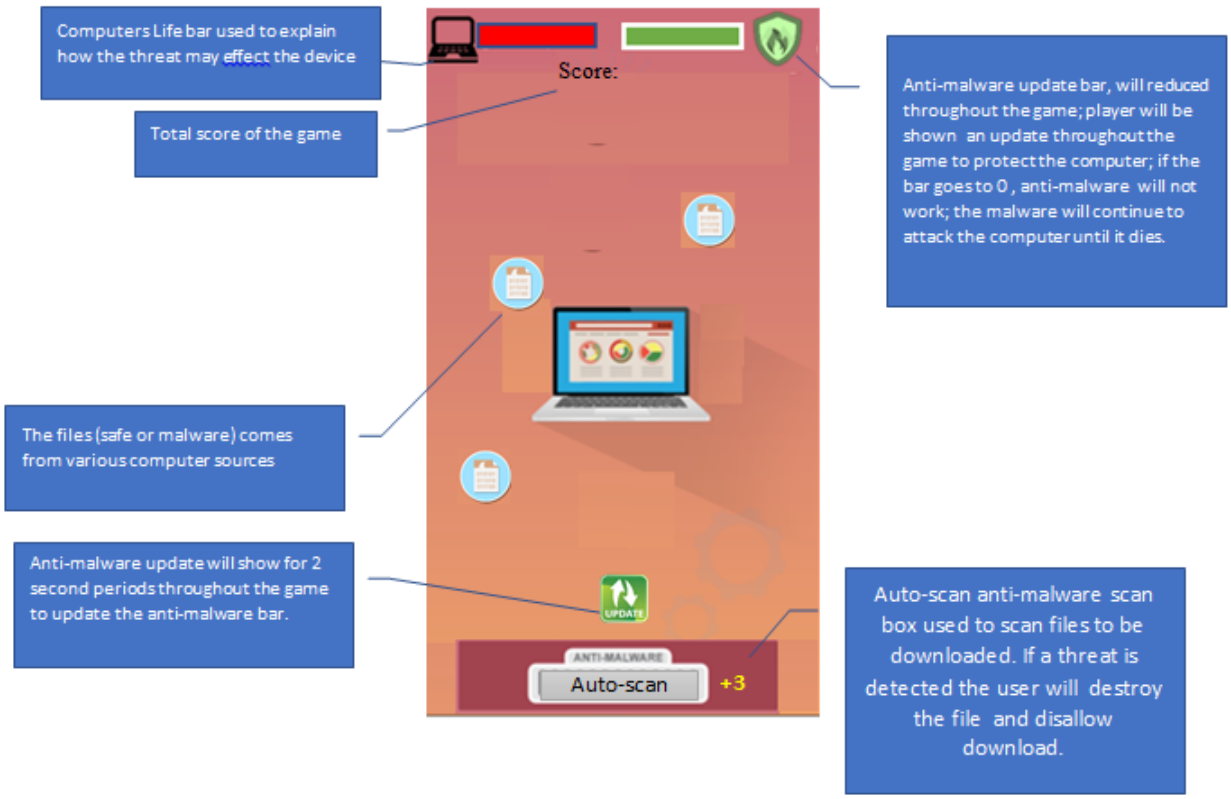


Figure 6.8 An overview of Malware Guardian Game

On the game screen, the computer character and Malware Guardian agent will be displayed. The computer will be surrounded by a number of files that are enacting as files that communicated to the computer through the cyberspace. Of these files, some of them are malware files and some are safe. The player role is to protect the computer from the malware files. There is anti-scan option also in the game.

The player should check a file manually before it reaches the computer and then scan it to check its safety credibility. The player taps on the file which is approaching the computer. If the file is a malware, then the player destroys the file. Unable to destroy such files will lead to a penalty on the player. This is done in order to create the threat perception of the real world.

In Figure 6.8, it can be noticed that under the computer there are two bars red and green colure. One bar is a life bar of the computer (red) and the other is the anti-malware bar (green). The life bar length is reduced each time the player fails in preventing an attack on the computer. When the failures cross a certain threshold, the life bar goes empty and the game ends. On the other hand, the anti-malware bar is an indication of the strength of the Malware Guardian agent. It is important that Malware Guardian tools are regularly updated in order for them to know about the new cyber-threats and combat them. The player then needs to click on the update button which will be flash from time to time so that the anti-malware agent is updated. If the player does not update within a few seconds, then the anti-malware life reduces (in this case, by 25%) and then may lead to disable the box which then results in the end of the game. This aspect of the game, trains the players about the importance of keeping the anti-malware software up-to-date.

6.4.2. Conceptualization and Design

The major objective of this game is to increase the awareness of the players. The design and concepts are built based on this objective. These design aspects are explained in the following sections.

Concept: The Malware Guardian game will be designed and developed with an aim of educating the players about various types of malwares, the harm they would cause, and the necessary techniques of destroying them before they attack the system. A narrative approach is adopted in the game, with action sequences to make it attractive and to create interest among the players. The concept of game is based on destroying the various malwares that would try to attack the personal computer. The malwares are represented as bugs in the game. The malwares can

move towards from multiple directions towards the computer on the screen. The player has to select the right method to destroyed different malwares. The methods describe the techniques to be used to destroy different types of malwares in reality. Therefore, every malware can have a different or a common method that can be used to destroy them. Additionally, there is backup option for users in game, which they need to select in the event of an attack. An update bar on the screen, which notifies fully update or update available. The player needs to regularly update the anti-malware software to destroy the new threats.

Scoring Technique: The score is calculated depending on the number of bugs destroyed by the players. For example, if the player destroys all the five bugs, score would be 50, if the user destroys 4, score would be 40, and so on. However, the time is fixed in each level to create more sporting spirit among the players. The game is a multi-level game, where the complexity (increase in malware) and the toughness (reduce in time to finish the level) increase as the game progress to next levels. Depending on the number of malwares fixed, the player gets the score, and ends the game.

Types of Malware: Different types of malware are used in the game, which are commonly found over the Internet are included in the study. These are shown in Table 6.1.

Table 6.1 Types of Malwares used in the Malware Guardian Game

Malware type	Explanation	Messages from pop up in the top screen
Adware	Adware (short for advertising-supported software) is a type of malware that automatically delivers advertisements.	A message indicating that the adware malware is destroyed and another message indicating the harm this type could cause to the system.
Bot	Software program to automatically perform specific operations.	A message indicating that the bot malware is destroyed and another message indicating the harm this type could cause to the system.

Bug	A fault that creates undesired outcome	A message indicating that the bug is debugged and another message indicating the harm this type could cause to the system.
Ransomware	It holds the computer on hold until an action dictated by it is not performed	A message indicating that the ransomware is destroyed and another message indicating the harm this type could cause to the system.
Rootkit	A software used by intruders to remotely control the computer without the realization of the actual user	A message indicating that the rootkit malware is destroyed and another message indicating the harm this type could cause to the system.
Spyware	It is a malware that monitors the user data on their device	A message indicating that the spyware is destroyed and another message indicating the harm this type could cause to the system.
Trojan Horse	Trojan is a common type of malware that disguises itself as a genuine software and infects the device	A message indicating that the Trojan horse malware is destroyed and another message indicating the harm this type could cause to the system.
Virus	A virus is a bug that copies itself into multiple times in the system effecting its performance	A message indicating that the virus is destroyed A message indicating the harm this type could cause to the system.
Worm	This type of malware exploits the vulnerabilities of the computer`s operating system	A message indicating that the worm is removed from the device and another message indicating the harm this type could cause to the system.

Game Process: The game starts with a message asking the player to backup to prevent data loss from any malware attack. Once the player backup the system, the next screen appears with a message that a copy of backup is made and it has to be used if the computer is attacked by malware. Then the player can start the game from level 1. This process is depicted in Figure 6.9.

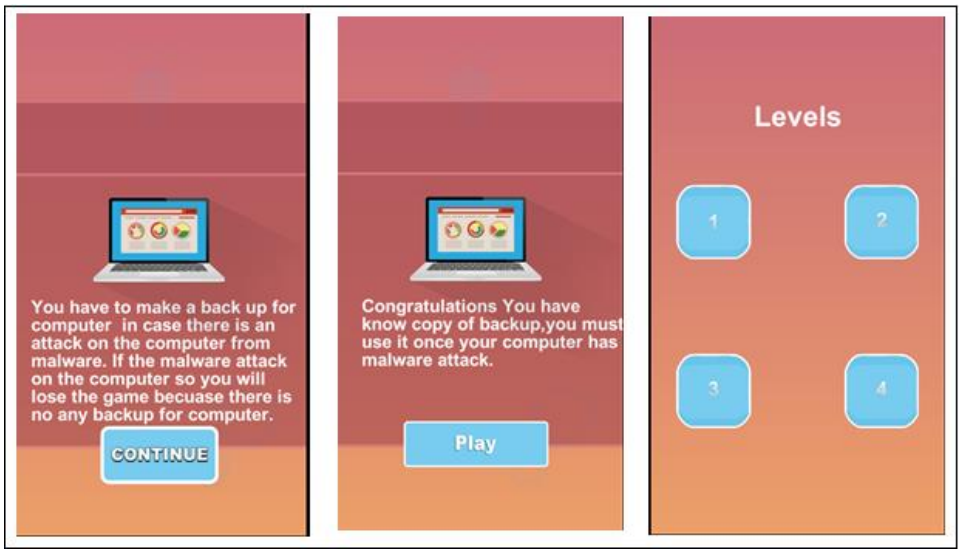


Figure 6.9 Initial setup of Malware Guardian Game

The game starts with level 1. As the game starts the files start downloading (1). The user can use auto-scan option to scan the files and can stop malware files from being downloaded (2). If the anti-malware software is fully updated is fully updated, the player can destroy the malware and score 100 points (3). The game then continues. As it progresses, the anti-malware bar starts decreasing, and the player must find update icon appearing on the screen and press it to update (4). In the game there is only one option of auto-scan for the players. However, if the Malware Guardian program is not up-to-date, the player may not be able to destroy the malware and the destroy button will be disabled till the anti-malware program is updated (5). This process is depicted in Figure 6.10.

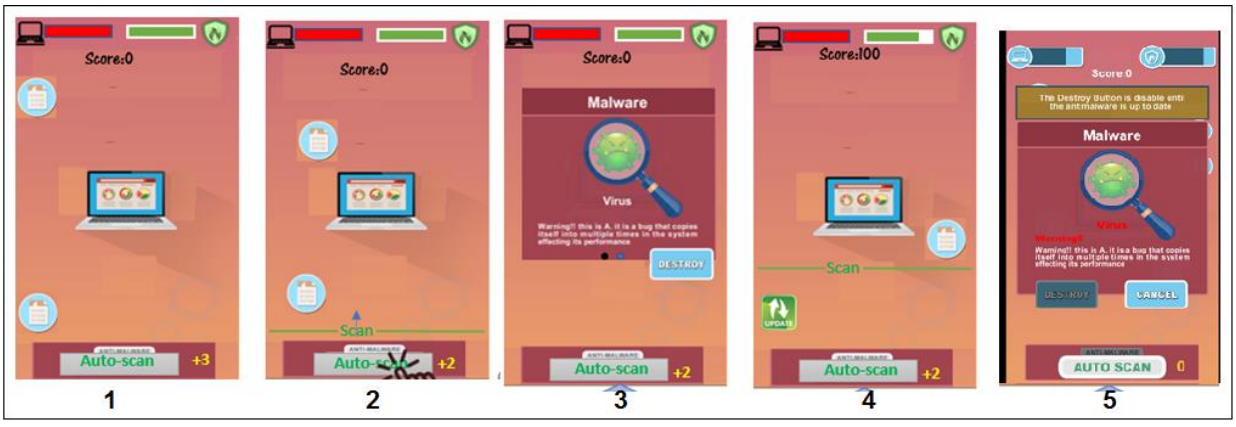


Figure 6.10 Auto-scan and Update options in Malware Guardian Game.

Different types of malware can affect the computers in different ways. For example, when an adware attacks, its description is presented on the screen (6). If the player could not destroy the adware, then warnings will pop up around the play area. All this serves to obscure parts of the play area and hamper the player's ability to scan other files, which continue to head towards the system. This screen will last for 5 seconds and then the game resumes (7). Here the anti-malware bar continues to decrease; the user should tap the update icon coming up. The player has one opportunity to attack the file manually by tapping on it. If the player ignores that then there is one further manual scan opportunity (8). If the player uses auto-scan, then '0' appears beside auto-scan which indicates there are no auto-scan options left to use (9). This process is depicted in Figure 6.11.

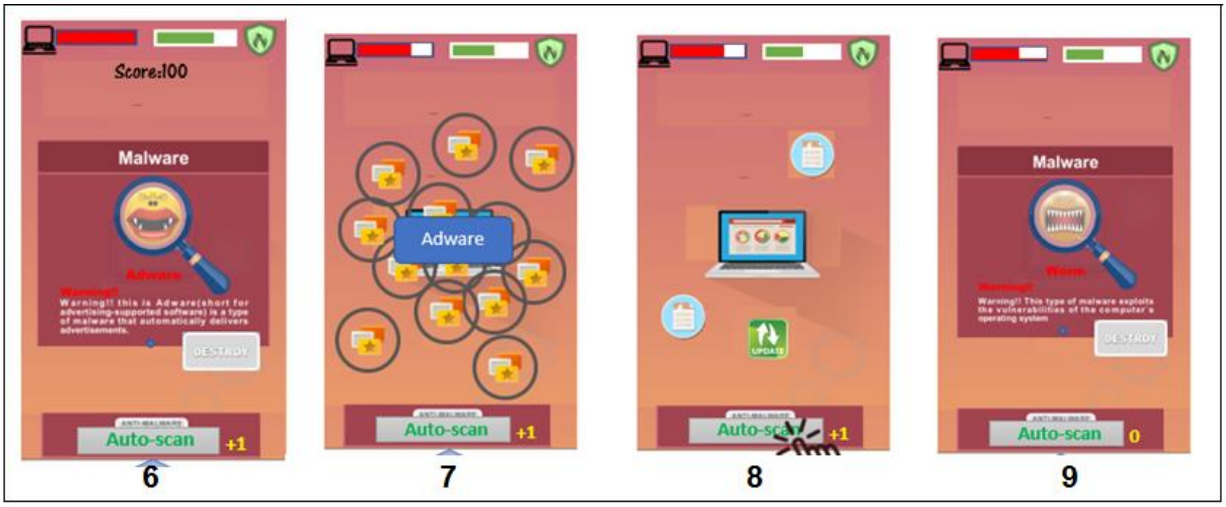


Figure 6.11 Malware Attacks and Auto-scan options in Malware Guardian Game

Different malwares are depicted with different icons. For example (6) in Figure 6.12 presents the files with worms, this will cause malware copies to spread from the computer. The user has to fully update the anti-malware in order to get an extra auto-scan option to use (11). The user can continue the game with fully updated anti-malware (12). This process is depicted in Figure 6.12.

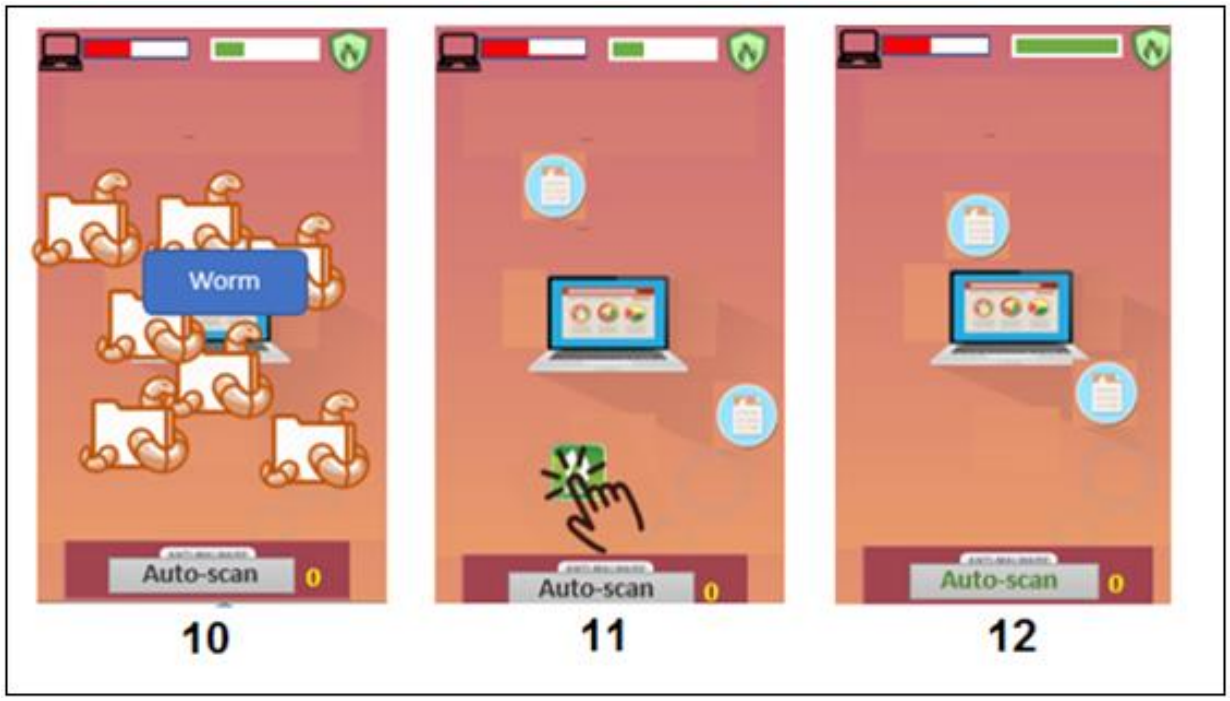


Figure 6.12 Worm and Update options in Malware Guard

This process continuous in the game as the levels increases. In addition to these a backup option would appear on the screen when the computer is attacked by a malware, which can be used by the player to get back the system of previous version.

Miscellaneous Situations: The players would end the game if the life bar is fully drained and start again from the beginning. However, a backup option can be used in such instance. Similarly, if the anti-malware program bar drains out completely, the players would either end game or update the anti-malware.

Game Levels: There are four levels in the game. Their description is presented in Table 6.2.

Table 6.2 Levels Description of Malware Guardian Game

Levels	Description	Final scores
First level	90 secound, 35 random Malware attack, 25 Safe gfile, Auto-scan each 5 secounds	1 Star: If total scores=> 150 2 Stars: If total scores=>250 Hihg scores: If total scores=>300
Secound level	70 secound, 40 random Malware attack, 20 Safe gfile, Auto-scan each 7 secounds	1 Star: If total scores=> 150 2 stars: If total scores=>250 Hihg scores: If total scores=>300
Third level	60 secound, 45 random Malware attack, 15 Safe gfile, Auto-scan each 10 secounds	1 Star: If total scores=> 200 2 Stars: If total scores=>300 Hihg scores: If total scores=>400
Fourth level	50 secound, 50 random Malware attack, 10 Safe gfile, Auto-scan each 15 secounds	1 Star: If total scores=> 250 2 Stars: If total scores=>350 Hihg scores: If total scores=>450

User Interface: The game uses Graphical User Interface which is intended to be eye-catching and visually appealing, with attractive graphics, music, and touch sounds. Interesting icons and effective graphics are used to represent various malwares and their attacks to make it more appealing to the users.

6.4.3. Technologies used for Malware Guardian Game

The technologies used for Malware Guardian game is similar to the technologies used in Password Protector Game, as described in Section 6.3.3.

6.4.4. Testing and Evaluation

Two types of testing are conducted in the study. A review approach at each stage of development is adopted to ensure the quality in the development and to mitigate risks and errors. The second stage of testing includes beta testing. In this process the game is played by the actual users from Saudi Arabia, and various aspects were tested including the awareness (increase in the knowledge about malware attacks), and the aspects related to the game through heuristics evaluation including the various features like usability, learnability, and enjoyability. The analysis and evaluation process are explained in the next chapter.

6.5. Summary

The objective of this chapter is to explain the design and development of the Password Protector and Malware Guardian games. The approach explained by (Jain, 2017; Jaggo, 2016) are used to explain the design and development process of both the games. It is explained and justified in the previous chapter about the selection of two games which addresses the most commonly found cyber security threats. The methodology adopted in evaluating the games is discussed and the results of pre and post study survey are explained in the next chapter. The survey results of the games are analysed in the next chapter.

Chapter Seven

Evaluation

7. Evaluation

7.1. Introduction

As explained in the previous chapter, the games Password Protector and Malware Guardian are evaluated using a pre and post study survey process and heuristic evaluation approach is used to evaluate usability, enjoyability, and learnability aspects of both the games. The results are explained and analysed separately for each game in the following sections.

7.2. Evaluation Methodology of Password Protector and Malware Guardian

The evaluation study is completed in phases. The first phase focuses on collecting the responses from the participants using pre-study survey questionnaire in order to assess their knowledge levels with respect to password security and malware attacks. A separate questionnaire was used for each game, tailored according to the topic focus. After conducting the pre-study survey, the participants would download and play games for two weeks. At the end of two weeks they took part in post-study information gathering. This used the same questionnaire as the pre-study survey in order to assess any change in responses. The next step of the study focuses on the usability, fun and learning aspects, which is conducted using Heuristics Evaluation strategy.

The heuristics evaluation strategy was originally designed to assess the usability of software programs. They assess the user opinion about a given user interface and assess the usability component of the interface. It tries to understand how easily and effectively the users of an application will be able to reach the application objectives. Several versions of heuristics evaluation methods exist and in the context of mGBL, there have been few works that have designed strategies for evaluating learning based games (Korhonen and Koivisto, 2006; Pinelle, et al., 2008; Zaibon and Shiratuddin, 2010). In the context of games, the focus of heuristics evaluation is not on the usability but on the playability aspect of the game. The playability aspect includes concepts such as the game usability, how

easily the players are able to play and navigate within the games, the mobility of the game and others. Further, for GBL, the heuristics evaluation strategy focus is not just on the playability of the game but also on the learning impacts the game provides. In this study the evaluation part focused on four aspects, which include awareness creation, usability, learning, and enjoyability.

7.2.1. Study Setting and Participants

The study was conducted using an online link for the survey, and the participants included the general Internet adult users from the Kingdom of Saudi Arabia (KSA). Online study was a convenient approach as it allows participation of variety of people in population which is often difficult to access by traditional methods such as face to face interviews. Further, participants from different locations and background can be easily requested to take part in the survey.

Two survey links are created separately for Password Protector game and Malware Guardian game. The study took place in online medium. The interested participants were asked to contact personally through email, WhatsApp, and other social media platforms. After the interested participants gave their consent to take part in the study, they were sent a message with the purpose of study and instructions, along with the survey links (Pre and Post) and download link for the using drop box for android, using social media platforms including email groups, WhatsApp, twitter, telegram etc. The download link in iTunes could not be created as the Apple team cited the reason that not all games can be uploaded. However, they provided an alternative way to send the copy to the participants using drop box for download link. Accordingly, the participants were requested to email in order to get a copy for their iPhone or iPad. The participants were allowed to use the game for two weeks after taking part in the pre-study survey. After using the game for two weeks, the participants were requested to take part in post study survey process.

7.2.2. Sampling

The survey links for both games along with the download links are sent to the different people using email groups and social media. The study was also promoted and sending invitation using social media platforms like Twitter and Telegram.etc. A total sample of 50 was achieved for the Malware Guardian Mobile game who undertook both pre and post study survey. For the Password Protector Mobile game, a total of 50 participants participated in both pre-study and post study survey. A total sample of 100 was achieved for the study.

7.2.3. Questionnaire Design

The questionnaires in both pre and post study includes multiple choice questions where the users can select the right option among the given choices. The pre-study survey of the Password Protector game includes 12 questions out of which three questions are designed for gathering demographic information, while the remaining questions focus on assessing the level of creating strong password. The post-study questionnaire for the Password Protector includes the same questions as in Pre-study questionnaire. Additionally, 14 questions are added as the part of evaluating the games using heuristic evaluation strategy focusing on the aspects of awareness (1), usability (5), learning content (4), and fun and enjoyment (4).

The pre-study survey of the Malware Guardian game includes 15 questions out of which three questions are designed for gathering demographic information, while the remaining questions focus on assessing the level of Malware awareness. The post-study questionnaire for the Malware mobile game includes the same questions as in Pre-study questionnaire. Additionally, 14 questions are added as the part of evaluating the games using heuristic evaluation strategy focusing on the aspects of awareness (1), usability (5), learning content (4), and fun and enjoyment (4). The questionnaires were translated to Arabic language for better understanding among the Saudi participants.

7.2.4 Validation

A pilot of this process has already been conducted with nine participants, in order to validate the surveys and ensure that the game apps were meaningful to a wider audience. While it is not statistically meaningful to analyse the survey results from this stage in any depth, they did at least serve to give an illustration that the games themselves were considered effective by the participants. The themes of usability, learning content and enjoyment were each investigated via 4-5 related questions, with each rated on a 5-point scale (where 1 is most negative and 5 is most positive). Given the low number of respondents, rather than looking at each question individually, Table 1 presents the averages across all questions in each category for each of the games. This gives a broad indication that the overall results in all cases was skewed towards the positive side. The notably lower 'enjoyment' score for the Password Protector game is perhaps to be expected, as it is a time-based memory game, whereas the apparently more enjoyable Malware Guardian is an action game and does not make the participants feel that they are being explicitly tested and rated in the same way.

Table 7.0 Averaged game feedback ratings from the pilot study

	Average ratings		
	Usability	*Learning content*	*Enjoyment*
Password Protector	3.8	3.9	2.9
Malware Guardian	3.6	3.8	3.7

As a more specific result, one of the activities in the pre- and post-study surveys for the Password Protector game is for users to create what they consider to be a strong password. In the pre-test surveys, this was yielding responses such as brief passwords and/or passwords composed of only one or two character types (e.g. alphabetic only, numeric only, etc), and scoring the passwords against the strength meter algorithm used in the app gave an average of just 45% across the participants. It was therefore encouraging to find that the average observed from

the same task in the post-test survey had risen to 78%, and it was notable that all passwords were now alphanumeric and included at least one punctuation symbol, whereas none of the pre-test choices had included these at all.

Accompanying text-based comments were also collected and gave some early indications of areas for development. One notable example was the desirability of playing the games against other players as a form of competition. This is a theme that the authors had already identified as a potential route for deployment of such apps in an organisational setting (e.g. as a means of engendering a sense of competition amongst staff within and between departments).

7.2.5. Overview of Statistical techniques used in the data analysis

Analysis of Variance (ANOVA) is one of the important statistical analysis tools for comparing the means of two or more groups by analysing their variance (Roberts & Russo, 2014). It assumes that the variance would differ only when the means are significantly different. Its sum of squares indicates the variance of each component. It has various advantages which include providing effective approach for multiple sample comparisons, applicability in the analysis of various designs and experiments, robustness against violations of its assumptions etc. There are two types of tests which include one-way ANOVA and two-way ANOVA tests. One-way ANOVA only considers a single factor or one categorical variable, and enables the researcher to compare the means of three or more samples (For example, analysing the password test scores based on gender or age). The password test score is a dependent variable, and only one independent variable either age or gender can be used. Two-way ANOVA examines the effect of two independent factors on a dependent variable (For example, analysing the password test scores based on gender or age) (Macfarland, 2011). The password test score is a dependent variable, and both independent variables including age and gender can be used.

There are two kinds of means that we use in ANOVA calculations, which are separate sample means (μ1, μ2, μ3….) and the grand mean (μ). The grand mean

is the mean of all observations combined. The sum of squares between the group is calculated by using the formula

$$SS_{between} = \sum n_j(\bar{X}_J - \bar{X})^2$$

Where, $\bar{X}_J$ denotes a group mean, $\overline{X}$ denotes overall mean or grand mean, n_j denotes the sample size per group, and for '*m*' groups *df between* = m-1. Similarly, sum of squares within the groups is calculated by using the formula

$$SS_{within} = \sum (X_i - \bar{X}_J)^2$$

Where, $\bar{X}_J$ denotes a group mean, and X_i denotes an individual observation. For '*n'* independent observations and '*m*' groups, *df within* = n – m.

To calculate the F-ratio, the sum of the squares between groups will be divided by the sum of the square within a group. It is usually represented by F(*df between, df within*). If the value of F is high, it is a strong evidence that our null hypothesis -all groups having equal mean scores is not true, which can be further supported by the value of *p (significance).* If the value of p is <0.05, then the result may be considered as significant (Turner & Thayer, 2001).

Similar to ANOVA, a t-test is a type of inferential statistic used to determine if there is a significant difference between the means of two groups, which may be related in certain features. It is used for the purpose of hypothesis testing where the hypothesis (μ1- μ2 = 0). That is the difference of the mean of first group and second group is considered to be null. The value of *t* is calculated by using the formula

$$t - value = \frac{\mu 1 - \mu 2}{\sqrt{(\frac{v1^2}{n1} + \frac{v2^2}{n2})}}$$

Where, V1 and V2 are the variance of each group, and n1 and n2 are the number of participants in each group (Welkowitz et al., 2006). If the calculated t-value is

greater than the table value at an alpha level of .05; and the p-value is less than the alpha level: p <.05, then the null hypothesis can be rejected stating that there is no difference between means. The t-tests would be used in this study for comparing the performance of the groups in pre and post studies of using password protector and malware games, and also for analysing various aspects by dividing the results by gender and age.

7.3. Survey Results and Heuristic Evaluation for Password Protector Game

This section explains the survey results for the Password Protector game in five sections including demographic information, concept based questions like Internet usage, game related questions, heuristics evaluation of the Password Protector game including the aspects of usability, learning and enjoyment, and the comments made by the participants' about the game.

7.3.1. Demographic Information

The total number of participants'' identified for both pre and post study surveys for Password Protector Game was 50. Among the 50 participants'', 34 were male and 16 were female.

A random sampling approach was adopted for collecting the sample population; as such no particular age group was targeted. The majority of participants'' (60%) in the study fall under the age group of 18-29, which potentially highlights that young people are more interested in games compared to the older ones and therefore more willing to volunteer. 28% of the total participants' come under the age group of 30-39, 10% under 40-49, and only 2% (i.e. one participant) aged above 50 years participated in the study.

The majority of participants were pursuing their school education and undergraduate programs. Only seven participants were in post-graduate courses.

More than 90% (47) of the participants' in the study were using Internet related services frequently throughout the day. The response highlights the level of Internet usage among the young people.

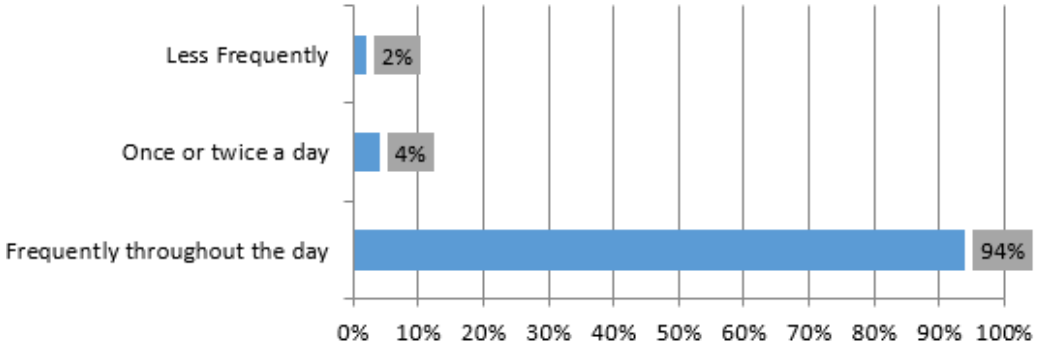


Figure 7.1 Participants' Internet Usage levels

Nearly 80% (20-beginner/21-intermediate) of the participants' considered themselves to belong to the categories of beginner/Intermediate skills when self-assessed for Internet and digital device knowledge, and nine participants rated themselves as experts in terms of Internet skills.

7.3.2. Password Protector Survey Analysis

The results are analysed for each question separately in this section.

Q1. I understand the concept of password strength.

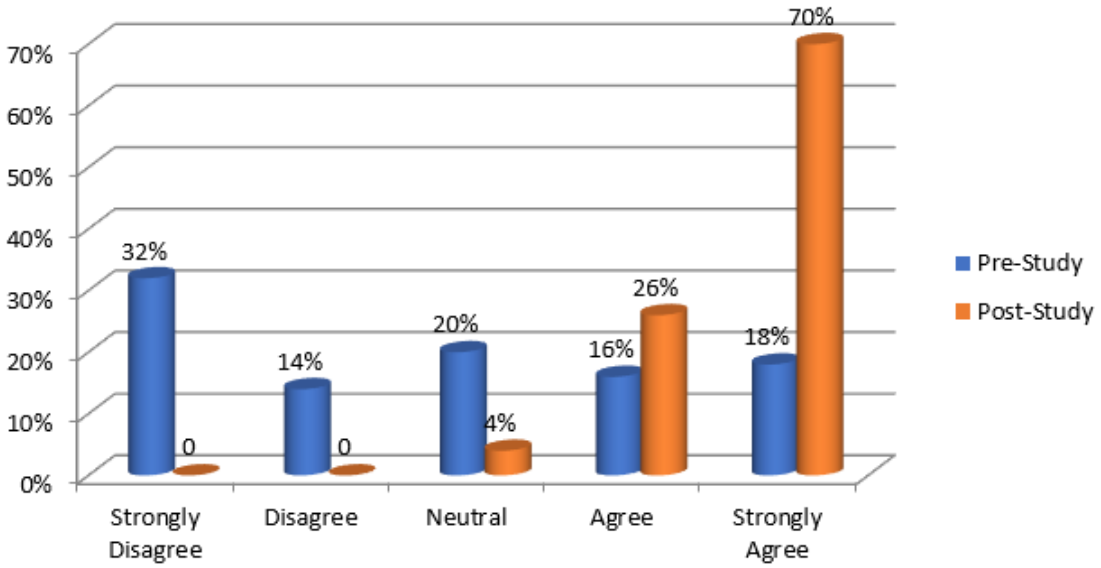


Figure 7.2 Participants' awareness levels of the concept of password strength

The shift in the awareness levels can be easily found as the results in the post study clearly presents the increased number of participants' understanding the concept of password strength.

Q2. Increasing the Password length increases the strength of the password

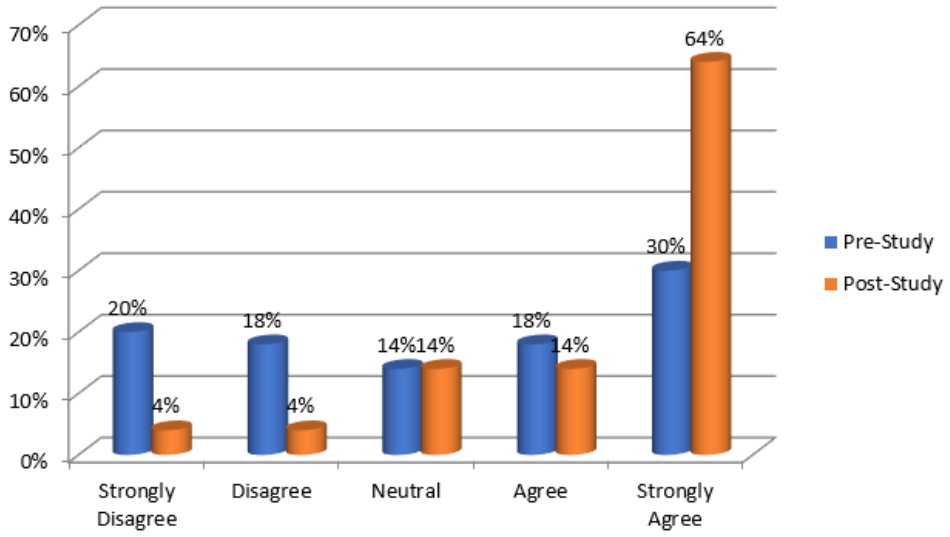


Figure 7.3 Participants' awareness levels of the concept of password strength (length)

The strength of a password can be based on different factors including length, the characters, numbers used along with the symbols. Length is one of the factors which determine the password strength, but not the only factor. The results from the study have shown that majority of the participants' understood that increasing the length of a password would increase the password strength.

Q3. Use of different character types (letters, numbers, etc) in my password increases its strength.

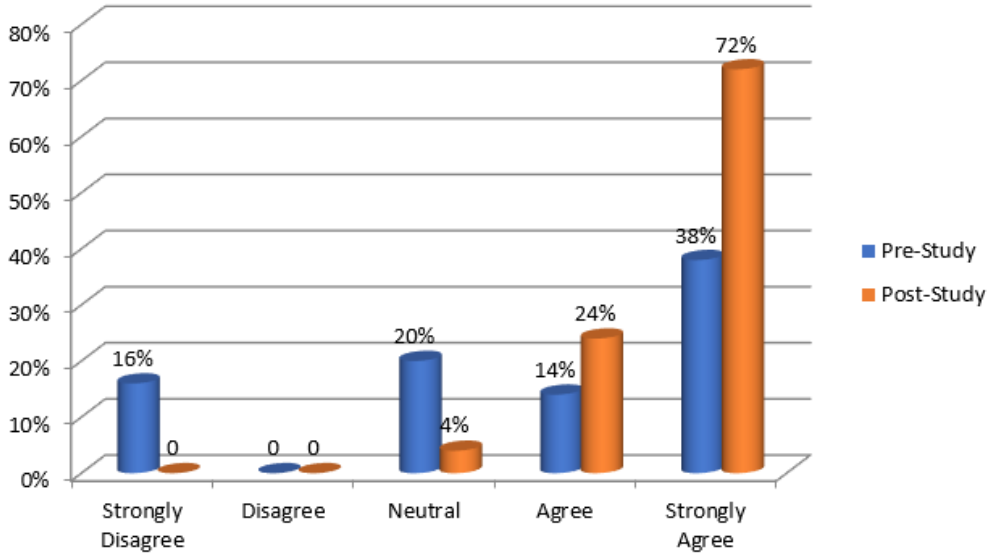


Figure 7.4 Participants' awareness levels of the concept of password strength (characters mix)

As explained in the previous question the password strength is determined by the combination of characters used. The Password Protector game promotes the use of different combinations of characters to increase score in each level. It is evident from the pre-study results that there is considerable number of participants' who were not aware that the combination of characters would increase the password strength. However, the results have shown that majority of the participants' understood this concept after playing the game.

Q4. I can remember passwords of more than 8 characters

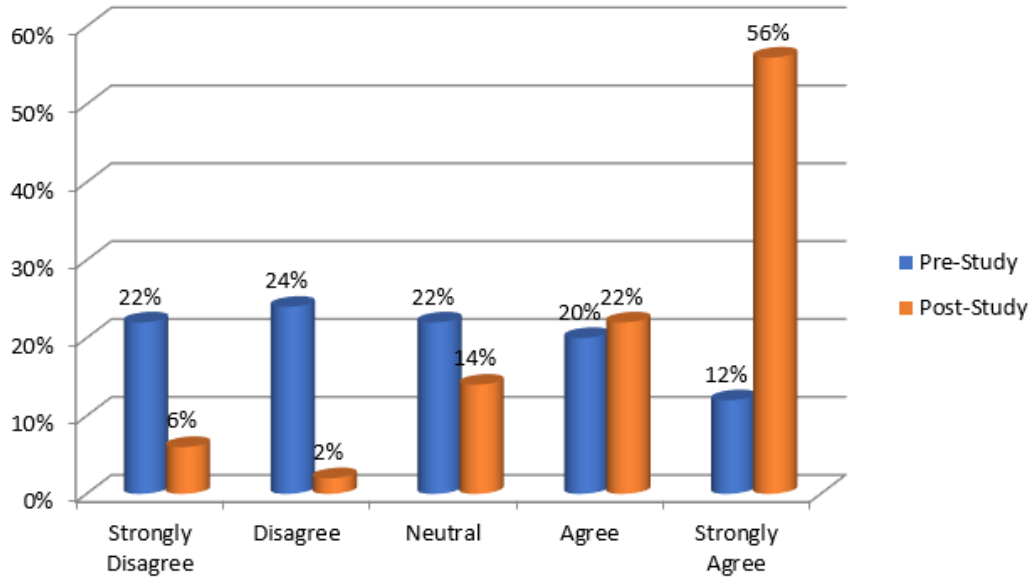


Figure 7.5 Participants' ability in remembering passwords

This question focuses on the participants' ability to remember long passwords. This question has got mixed responses. The pre-study results show that the participants were mostly not sure or unable to remember the long passwords. However, after the study there is a slight increase in the number of participants' who are able to remember the long passwords. The results have shown that a password with eight characters can be a benchmark for setting the complex passwords considering the ability of the users in remembering long passwords.

Q5. I find password meters useful in checking if my password is strong or not.

Password meters show the strength of the password at the time of password creation. The users can create strong passwords if the strength is low. This method would alert the users if they are creating weak passwords. While a considerable number of participants were neutral about the usefulness of password meters in the pre-study survey, most identified it as a useful method.

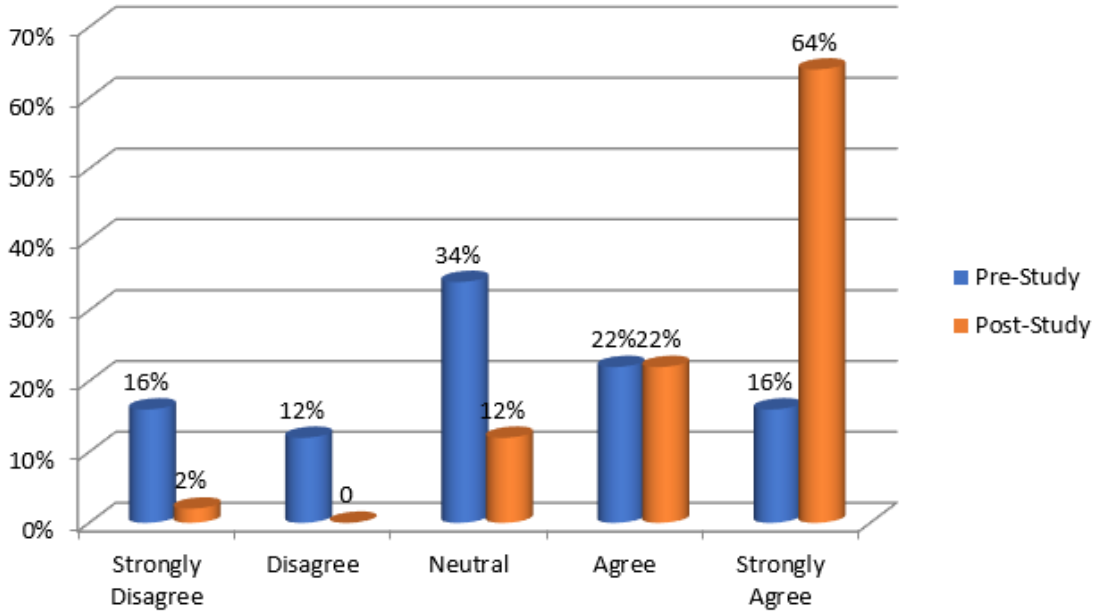


Figure 7.6 Participants' responses about Password Meter

Q6. Create a Strong Password

The participants' were asked to create a strong password in pre and post study surveys, and based on their input, the password strength was calculated. The Table below presents the means and standard deviations of the password strength before and after playing the games.

Table 7.1 Average password strength ratings from pre- and post-study attempts

	Pre-Study	**Post-Study**
Mean	59.1	80.2
SD	15.5	13.2

Few examples of passwords and their strengths before and after the study are presented in Table 7.2 below.

Table 7.2 Passwords from pre- and post-study attempts

Pre-study Password	Strength	Post-study Passwords	Strength
A435354	46%	(-_-)Aa01234554321	100%
Ddo900	52%	K@Dg431!Mo00oD	88%
1234554321k	50%	U77665544::	82%
ta1aaa1	28%	GHasiband 9795	78%
F0114897654	58%	%Www.be.aware.50.;	90%

7.3.3. Heuristics Evaluation

The heuristics evaluation in this study for the Password Protector game is conducted in three areas including usability, learning content, and enjoyment.

7.3.3.1. Usability Evaluation

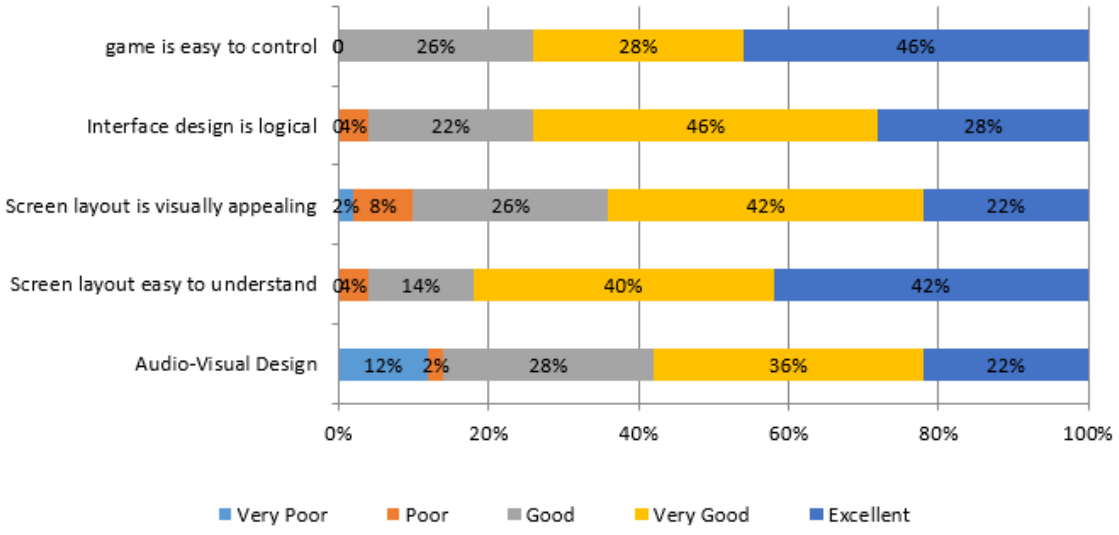


Figure 7.7 Usability Analysis of Password Protector Game

It is clearly visible from the chart that majority of the participants' rated above average for various aspects of usability. The audio-visual design aspect was rated to be very good and excellent by more than 58% of the participants. The easy to understand screen layout was rated very good and excellent by more than 80% of the participants. More than 64% of the participants' have rated that the screen layout visual appeal as very good and excellent. More than 73% of the participants' have rated that the interfaces design logic as very good and excellent and the same rating was given to the easiness to control feature of the game. The responses to the usability questions reveal that majority of the participants are satisfied with the usability aspects of the Password Protector game.

7.3.3.2. Learning Content

The learning content of the game has to be designed effectively so that the users can easily and quickly learn and engage with them. However, the game has to be fun and engaging in order to let the users play and gather their attention.

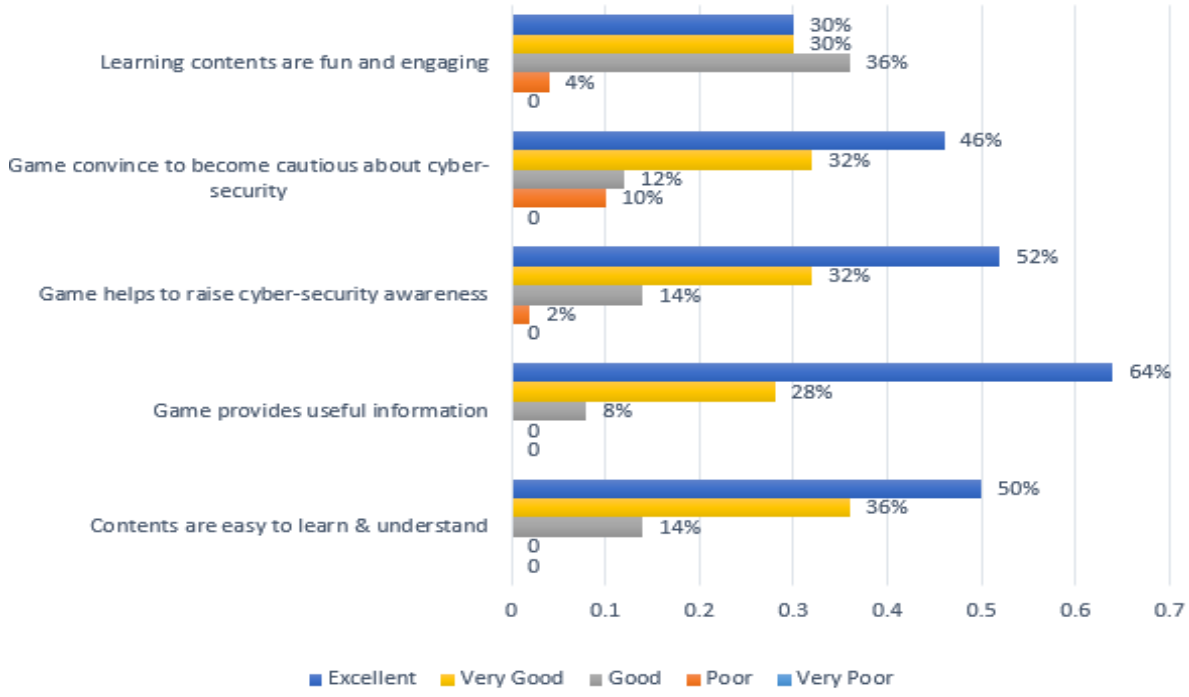


Figure 7.8 Analysis of Learnability in Password Protector Game

More than 80% of the participants' have rated very good and excellent for the learning and content features including easy to learn contents, information availability in the game, raising cyber security awareness, and convincing players to become cautious about cyber security. More than 60% of participants rated very good and excellent for the fun and engaging learning contents available in the game. The overall responses for the learning aspects of the Password Protector game reflects that majority of the participants are satisfied.

7.3.3.3. Fun and Enjoyment Aspects

One of the most important aspects of the game design is that the games must be fun and provide enjoyment to the players. These features engage the players in playing the game. Four aspects associated with Password Protector game which include learning about cyber security, fun, interest of the players in playing similar games, and the enjoyability in learning password creation through the game were assessed. The results have shown that majority of the participants were satisfied with all these aspects.

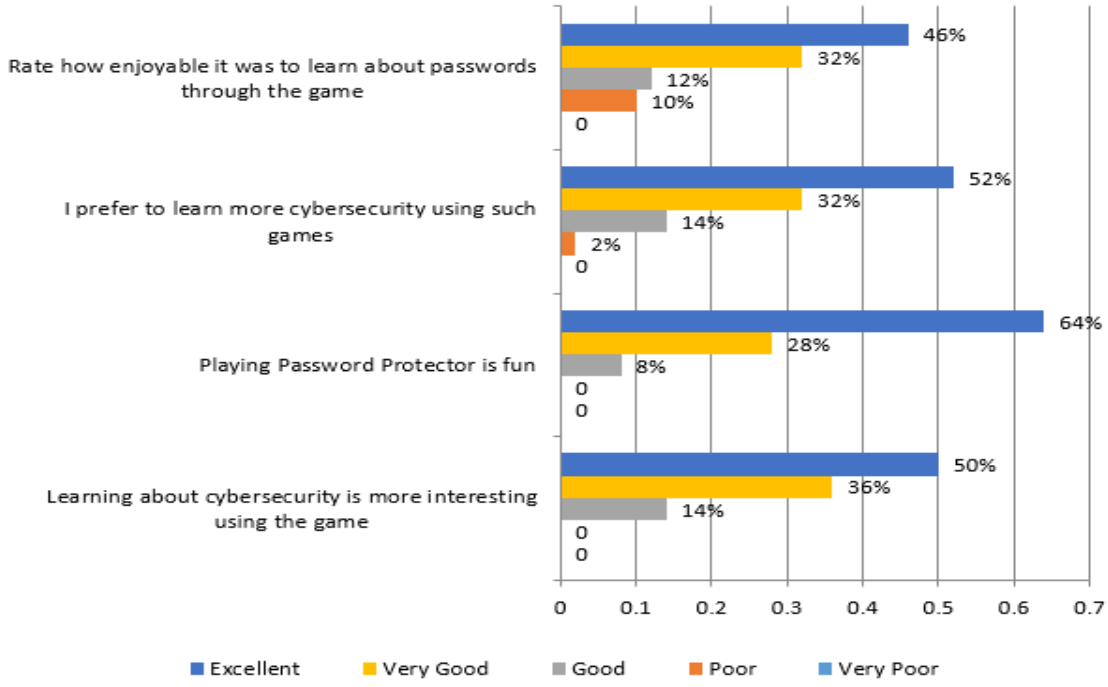


Figure 7.9 Enjoyability Analysis of Password Protector Game

More than 78% of the participants' rated very good and excellent for all the aspects about fun and enjoyability in the game.

7.3.4. Comments analysis

The pre-study survey did not receive many comments, other than a few (seven participants wishing, and one participant asking the game download link) of the participants' wishing good luck with the study. The post-study survey received many interesting comments. A few comments were regarding the design of the game, suggesting using a light-coloured interface (one participant), diversifying levels and increasing challenge (three participants), setting up alerts and reminders (one participant) for users to re-exercise, changing sounds, and increasing complexity/hardness as the level goes up (one participant). Meanwhile, other participants were interested in sharing the game with friends, suggesting deploying in office/organizations/schools (two participants). However, one of the interesting comments identified was that the game is suitable for younger generation, who are relatively new to Internet, and are more prone to security threats. The overall comments analysis reflects that majority of the participants were happy with the game, however few design aspects were suggested to be improved.

7.4. Survey Results and Heuristic Evaluation for Malware Guardian game

This section explains the survey results for the Malware Guardian game in five sections including demographic information, concept based questions like Internet usage, Malware awareness, game related questions, heuristics evaluation of the game including the aspects of usability, learning and enjoyment, and the comments made by the participants' about the game.

7.4.1. Demographic Information

The total number of participants identified for both pre and post study surveys for Malware Guardian game were 50. Among the 50 participants', 30 were Male and 20 were female. There is a slight difference in the gender gap, and the majority of

them were young having same level of education, therefore this difference has very little/no impact on the results.

Majority of the participants' (58%) in the study fall under the age group of 18-29, which highlights that young people are more interested in games compared to the older ones, though random sampling was employed in the study. About 34% of the total participants' come under the age group of 30-39, 8% under 40-49, and there were no over-50s in this study.

The majority (94%) of the participants' in the survey are in their school education and undergraduate programs. Only three participants were in post-graduate courses.

More than 90% (48) of the participants' in the study were using Internet related services frequently throughout the day. The response highlights the high levels of interest of Internet usage among the young people.

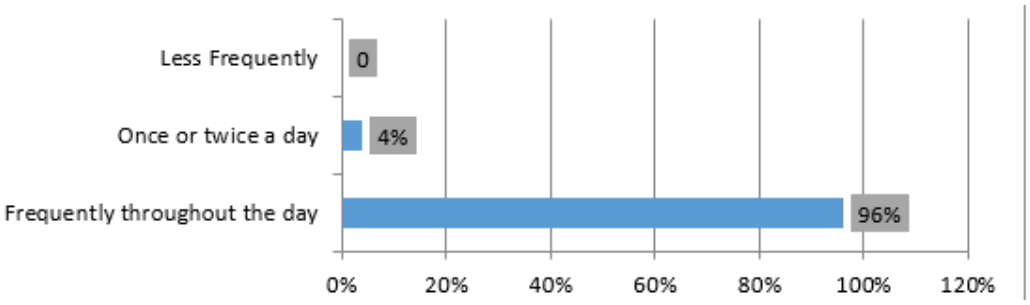


Figure 7.10 Participants' Internet Usage levels

96% (26-beginner/22-intermediate) of the participants belong to the categories of beginner/Intermediate skills when assessed for Internet and digital device knowledge, and only two participants' are experts in Internet skills. This is an added advantage as the study is about increasing the cyber security awareness among the young in KSA, and beginners are particularly prone to cyber security attacks as they are less aware of cyber threats.

7.4.2. Malware Guardian Survey Analysis

The results are analysed for each question separately in this section.

1. I have a good understanding of the concept of Malware

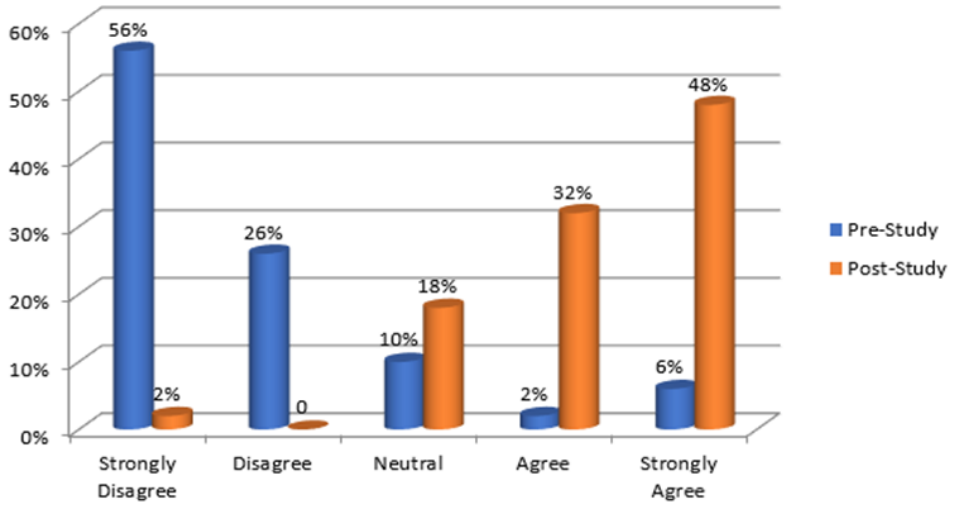


Figure 7.11 Participants' awareness levels of the concept of Malware

The majority of students were not aware of the malware concepts before playing the game, however, there is a steep learning curve identified among the students after playing the game, as more than 80% of the students agreed and strongly agreed that they are aware about the concepts of Malware in the post-study survey.

2. I am aware of the different types of malware that might attack my system.

This question focuses on identifying the various types of malware attacks that participants are aware of. More than 80% of the participants' in pre-study have responded that they are not aware of any types of malware attacks. However, after the study there is a mixed result. About 34% were neutral to the question, 26% agreed they are aware of the types of malware attacks, and 36% strongly agreed for the same. The complexity in understanding malware and how they attack might be completely new and a challenge for the beginners. It may be the reason for the considerable number of participants' opting neutral for the question.

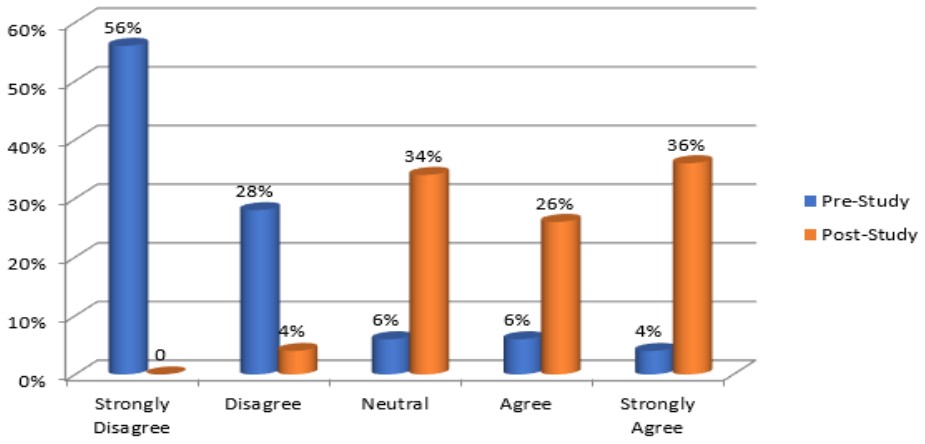


Figure 7.12 Participants' awareness levels about Malware types

3. Malware has the ability to take over my computer remotely.

Majority of the participants' (74%) were not aware if the malware has the ability to take over the computer remotely as they opted strongly disagree, disagree, and neutral. However, post the study majority of the participants' more than 80% of them agreed and strongly agreed to the same question. The pre and post study responses clearly indicate the increase in the level of awareness about malware attacks.

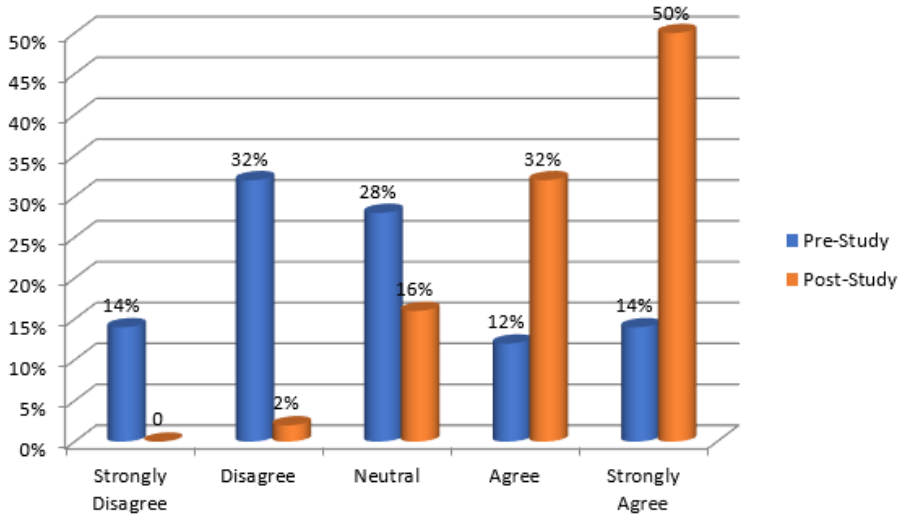


Figure 7.13 Participants' awareness levels about Malware attacks

4. I am aware of the different effects that malware can have upon my system.

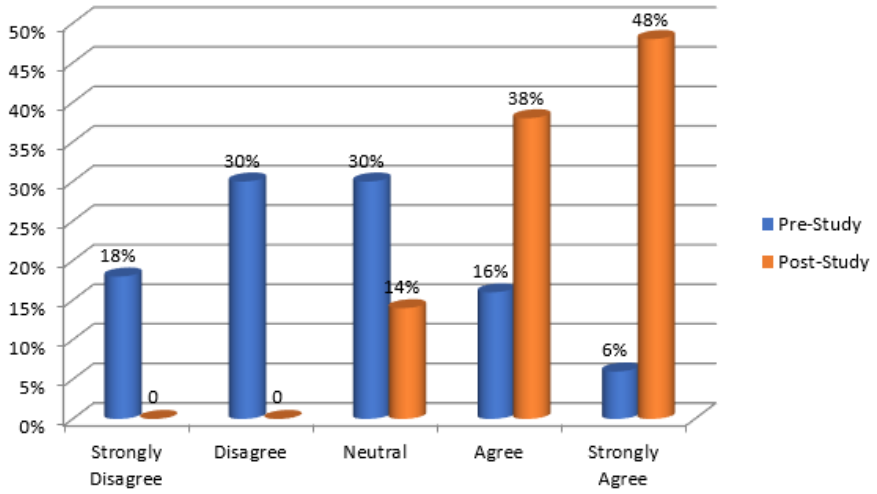


Figure 7.14 Participants' awareness levels about the impact of malware attack

The participants were not aware of the effects that a malware can have upon their system before participating in the study as 78% of the participants' responded to strongly disagree, disagree and neutral. However, post study nearly 86% of the participants' agreed and strongly agreed to the same. The responses reflect that the Malware Guardian game not only educates the users about the types of attacks but also the impact it would have on their computers.

5. I can understand why anti-malware software is so important.

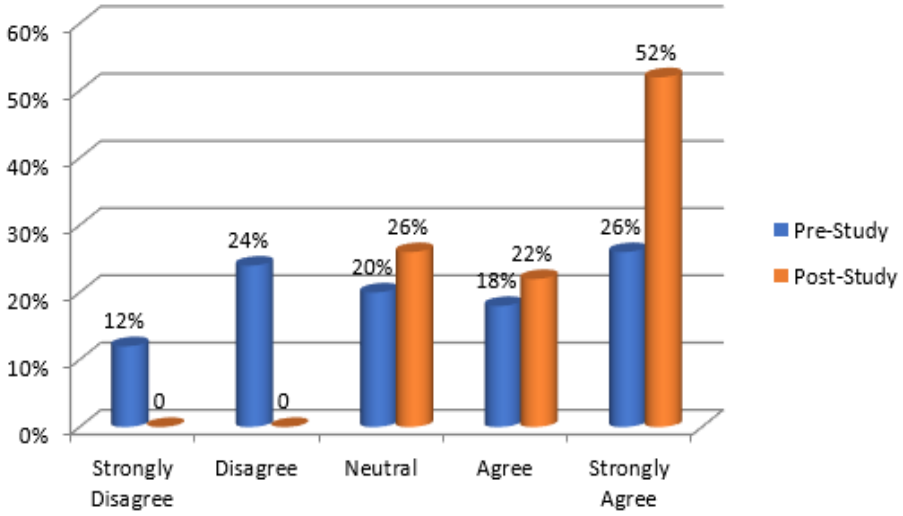


Figure 7.15 Participants' awareness levels Anti-Malware Software

This question was frame to check if the participants are aware of the importance of anti-malware software. The responses from the pre study show that 56% of them were not aware of its importance as they opted strongly disagree, disagree, and neutral. However, post the study about 74% of them opted agree and strongly agree to the question. There are considerable numbers of participants' who were neutral in both pre and post study, suggest that there is a gap in effectively promoting the importance of Anti-Malware software through the game.

6. It is important to keep anti-malware program up-to-date.

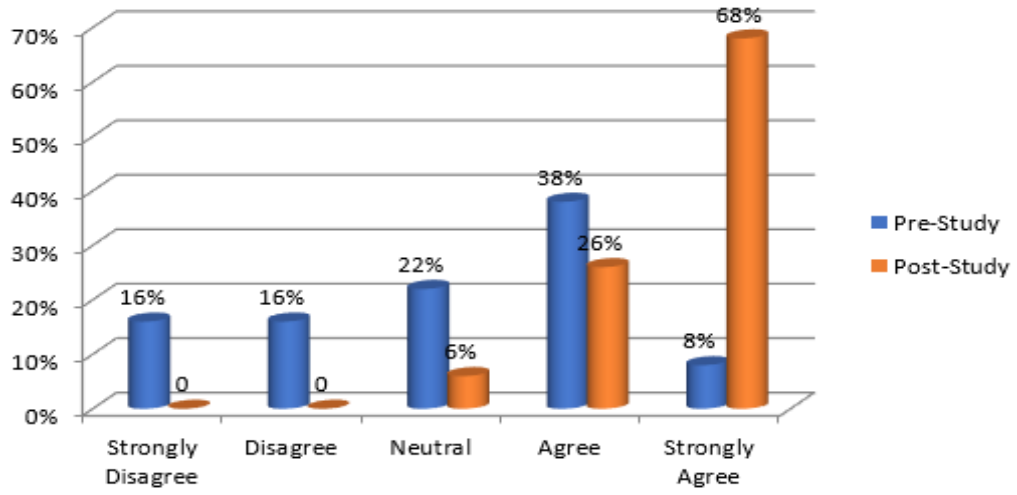


Figure 7.16 Participants' awareness levels about updating Anti-Malware software

It is very important to keep the anti-malware program up to date, as the new malwares keeps popping up in the cyber space, which may not be recognised by the programs if not updated. To assess if the participants were aware of this concept, this question was framed. The pre-study results reveal that more than 50% of the participants were not aware of this concept as they opted strongly disagree, disagree, and neutral. However, post the study, the awareness levels grew at larger pace as about 94% of the participants' opted agree and strongly agree for the same question.

7. I understand the difference between manual and automated malware scanning.

It is important for the users to be aware of the manual and automated scanning for effectively using the anti-malware programs. From the pre study responses it is clear that nearly 78% of the participants were not aware of the techniques as they selected strongly disagree and disagree options. However, post the study more than 66% of the participants' agreed and strongly agreed that they understand the difference between manual and automated malware scanning.

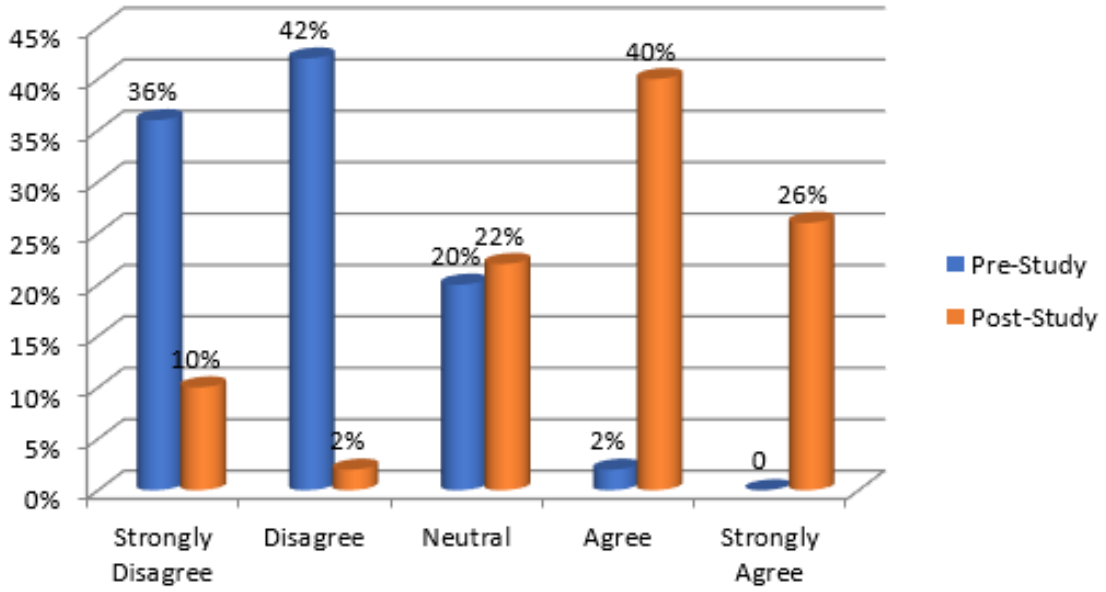


Figure 7.17 Participants' awareness levels of the concept of Malware Scanning

8. It is important to back up the files in my computer regularly.

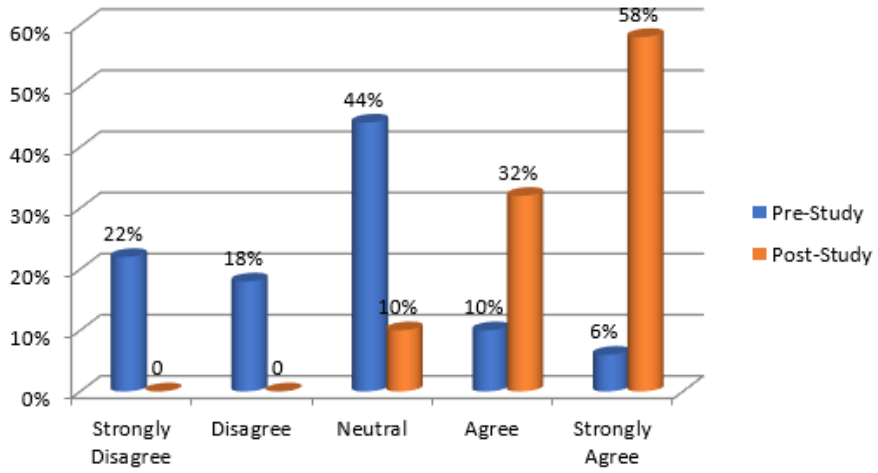


Figure 7.18 Participants' awareness levels of the concept of backup

Backup is one of the important routines which computer users must be aware of in order to prevent data loss in case of any cyber-attack or any other incident. It is evident from the pre study responses that majority, more than 80% were not aware of the importance of backup, as they opted strongly disagree, disagree, and neutral. However, post the study, there is a huge steep bend towards understanding the importance of the same as more than 90% of the participants' opted agree and strongly agree for the same question.

9. Backup are a useful safeguard to protect against malware

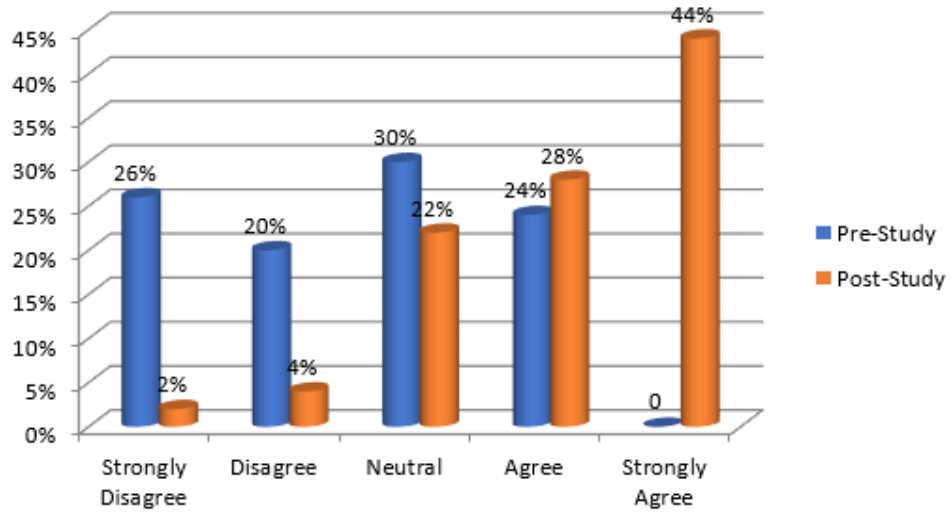


Figure 7.19 Participants' awareness levels about the use of backup

As mentioned in the previous section, backup is important activity to safeguard against any data loss due to malware attacks. The responses are similar to previous question. This question focuses particularly on malware attacks vs backup, and majority of the participants were not aware of this concept prior to the study amounting to 76%. However, post the study, more than 75% of the participants' responded that they are aware of this concept.

7.4.3. Heuristics Evaluation

The heuristics evaluation again considered the issues of usability, learning content, and enjoyment.

7.4.3.1. Usability Evaluation

The usability aspects of Malware Guardian game in assessing audio visual content, screen layout for controlling and understanding, logical interface design, and easiness in control, were evaluated using heuristics evaluation strategy. The results have shown common trends across all the usability aspects. Majority of the participants' more than 70% of them rated very good and excellent for all the usability features of the Malware Guardian game. The results have shown greater satisfaction levels of the participants' in relation to the usability features of the Malware Guardian game. The results are presented in the following chart.

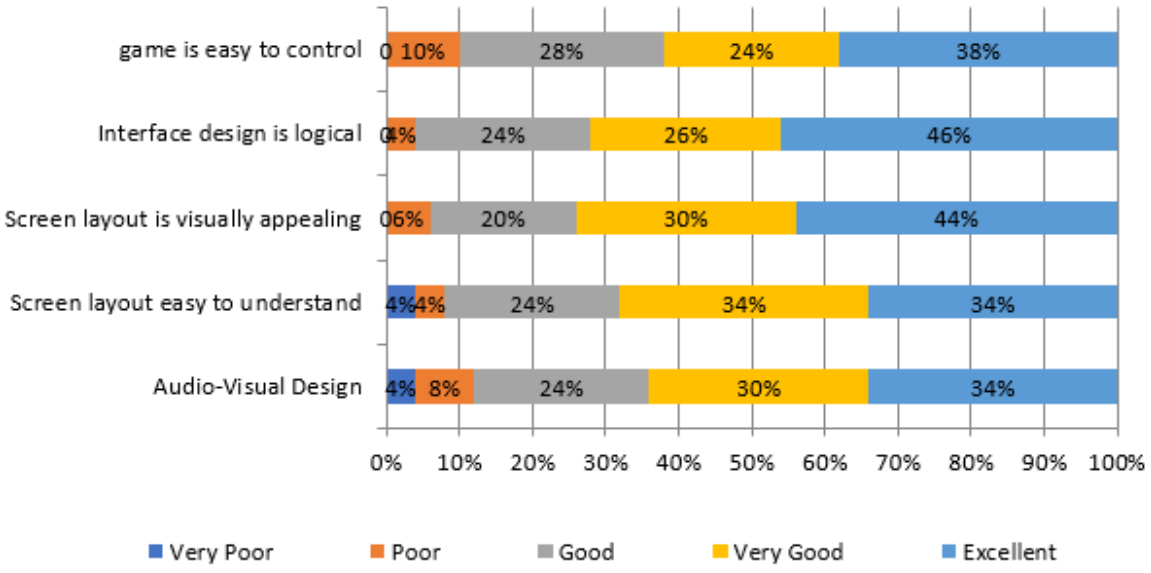


Figure 7.20 Usability Analysis of Malware Guardian game

7.4.3.2. Learning Content

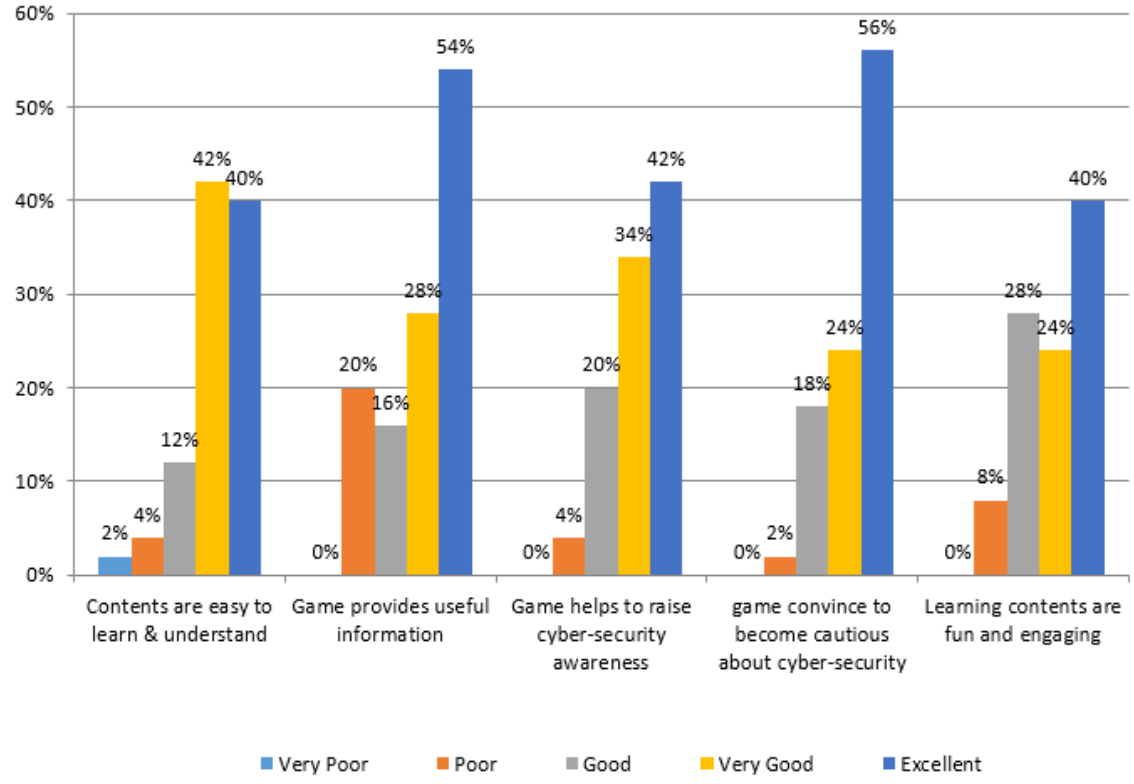


Figure 7.21 Learnability Analysis of Malware Guardian game

The learning content is important for any awareness related game as the main objective of developing the game is to educate the users through fun filled enjoyable environment through gaming interface. More than 80% of the participants' rated as very good and excellent concerning the learnability and understand ability through Malware Guardian game. Similar results were found for the learning aspects which include availability of useful information, raising cyber security awareness, enabling the users to become cautious about cyber security, and fun and engaging learning contents. The overall results of the learning content reflect higher satisfaction levels among the participants of the Malware Guardian game.

7.4.3.3. Fun and Enjoyment

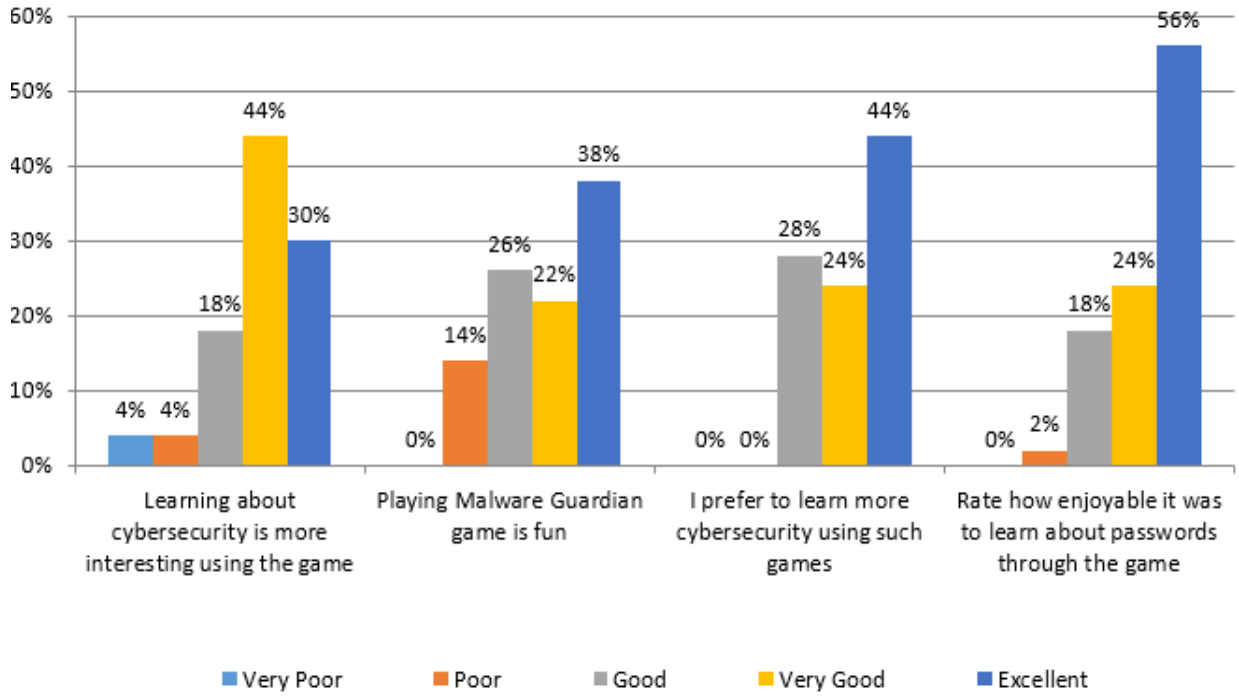


Figure 7.22 Enjoyability Analysis of Malware Guardian game

While there are very few responses for poor and very poor options concerning the fun and enjoyment features of the Malware Guardian game, the responses were distributed evenly across the good, very good and excellent options. The results

indicate that majority of the participants' are satisfied with the fun and enjoyment aspects of the Malware Guardian game, as more than 70% of the participants' opted for very good and excellent options for all the fun and enjoyment related aspect of the Malware Guardian game, which include learning about cyber security, fun playing the game, preference of learning more using similar games, and the enjoyability.

7.4.4. Comments analysis

The pre-study survey received only two comments, among which one comment suggests little awareness about malicious software (Malicious programs attack devices with important files of money and others) and other suggests lack of awareness (I just have a query if malicious software is the same as viruses). The post-study survey has identified some interesting comments. Most of them were related to the design aspects like introducing update of OS (one), which is equally important as updating anti-malware program, increasing time spent on each level (one), some design bugs (two), using 3D technology in the game (one), and using small font for instructions (one). Other comments suggested using the game in organizations to promote awareness, using media for raising cyber security awareness (one), suitable for small age groups/younger generation (one), and few comments wishing good luck (three). A detailed list of comments can be found in the appendix. From the analysis of comments, it can be said that majority of the participants were satisfied with the game, with few of them suggesting to include additional criterions like OS update, and 3D technology.

7.5. Inferential analysis using SPSS– justification for the tests

This section explains the inferential analysis of the survey results of both Password Protector and Malware Guardian games. SPSS Version 20.0 was used for carrying out the statistical analysis operations. This section explains the correlation between different variables and the results. This analysis would help in analysing the results from various perspectives that would help in in-depth analysis.

7.5.1. Password Protector Game

The inferential analysis for Password Protector game is conducted by comparing various attributes like creating complex passwords vs age; age vs awareness; education levels vs awareness; differences in pre and post study results etc. This analysis would help in investigating if the factors like age, education have any impact in creating complex passwords, learning, and achieving awareness. This analysis would help in developing the awareness applications by considering the influential factors such as age and education, in the process of creating storyline and other design aspects that would be more appealing to the target group.

7.4.1.1. Age vs Password complexity

One of the important awareness creation activities is to use different characters for the password and remembering them. T-tests are used for comparing two means and for assessing if they are different from each other. The t-score reflects the difference between the groups. The larger the t-score the larger is the difference between two groups. The t-test results indicated that there is a significant difference using different password characters and remembering them differed across the age groups (t = -24.75, *p* = 0.000).

Table 7.3 Password creation and age

		Mean	*SD*	*SE*	95% Confidence Interval of the Difference		*t*	*df*	*Sig.*
					Lower	Upper			
Pair 1	Age – Password Creation	-6.06	2.44	.245	-6.55	-5.58	-24.75	98	.000

As in the following graph respondents who aged above 30 had a better use of different characters for their password and ability and ability to remember them efficiently compared to their counterparts. Similar responses were identified in other studies (Pilar et al., 2012; Renaud & Ramsay, 2007; Golgowski, 2012; Truong, 2016). It is identified in these studies that the older people are more concerned about the privacy and security and consider every option to ensure safety, while the younger generation are more focussed in creating simple passwords that are easy to remember, without giving themselves any stress. Therefore, the results indicated that the older generation are more creative and serious about using strong passwords compared to younger population.

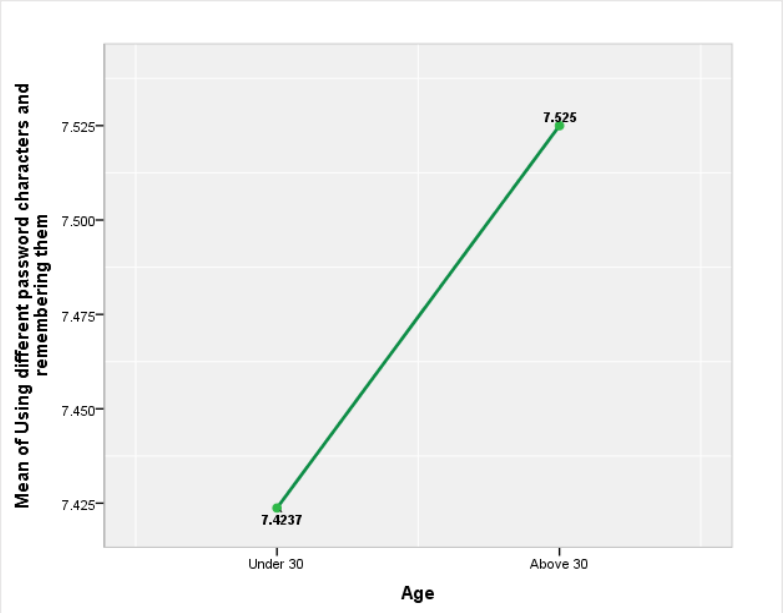


Figure 7.23 Using different characters for the passwords and remembering them

7.4.1.2. Age and awareness differences at the pre-test stage

To check whether there is a significant age wise difference in the awareness (at the pre-test stage) a paired sample t-test was carried out. As the following Table represents, the awareness was significantly differed ($t = -13.860$, $p < 0.05$) between age groups. Due to the means of the under 30 and above 30 age groups and the direction of the t-value, it can conclude that there was a statistically significant improvement in the awareness after the age from 1.40 ± 0.070 to 15.26 ± 0.830 ($p < 0.05$); an improvement of 13.860 ± 0.830.

Table 7.4 Age wise differences in awareness at the pre-test stage

		Mean	*SD*	*SE*	95% Confidence Interval of the Difference		*t*	*df*	*Sig.*
					Lower	Upper			
Pair 1	Age – Password Creation	-13.86	5.77	.82	-15.50	-12.22	-16.99	49	.000

As in the following Figure, the awareness increased in 2.9 points where under 30 respondents mean score was 14.10 ± 5.76 and above 30 respondents mean score was 17.00 ± 5.74. Awareness about cyber security and the knowledge was found to be high among the older people as they tend to self-monitor, clearly observe every sequence of action, and follow the guidelines for cyber security prescribed to them without any fail (Blackwood-Brown et al., 2019). Similarly, younger generation in UK were found to be lacking cyber security awareness, making it easy for hackers to target younger generation (BBC, 2018). While older generation may comer across the cyber security aspects during their lifetime, the younger generation need to be educated about these issues in schools and colleges. The younger generation may either find it new or complex in understanding and are more prone to using simple security mechanisms than a complex approach. Therefore, the older population may be more aware of cyber security issues as identified from the results.

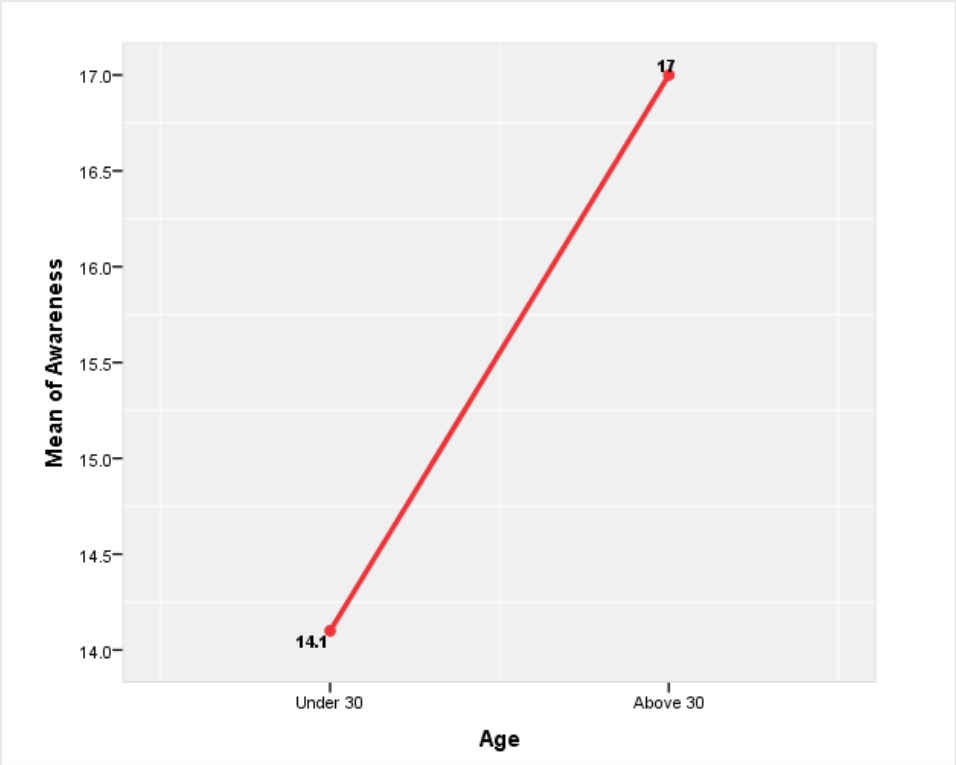


Figure 7.24 Mean plot of pre-test stage awareness differences

7.4.1.3. Education level wise awareness differences at pre-test stage

Though the awareness increased as the education level increases, that increase was not enough to observe a significant difference. Since there are three education levels, the statistical significance tests on the three groups can be carried out using the one-way ANOVA tests. This test is a popular statistical significance test to test for differences among three different groups. One-way ANOVA results indicated that mean awareness across the three education levels was not significant (F = 2.67, $p > 0.05$).

Table 7.5 Differences in awareness across various education levels

	Sum of Squares	*df*	Mean Square	*F*	*Sig.*
Between Groups	172.42	2	86.21	2.67	.079
Within Groups	1515.20	47	32.23		
Total	1687.62	49			

The following Figure shows the increase of awareness. At the school level awareness mean was 12.90 and at the postgraduate level, it was increased to 17.86. Though the increase was not significant, a slight increase reflects that education had minimal impact on the awareness creation process.

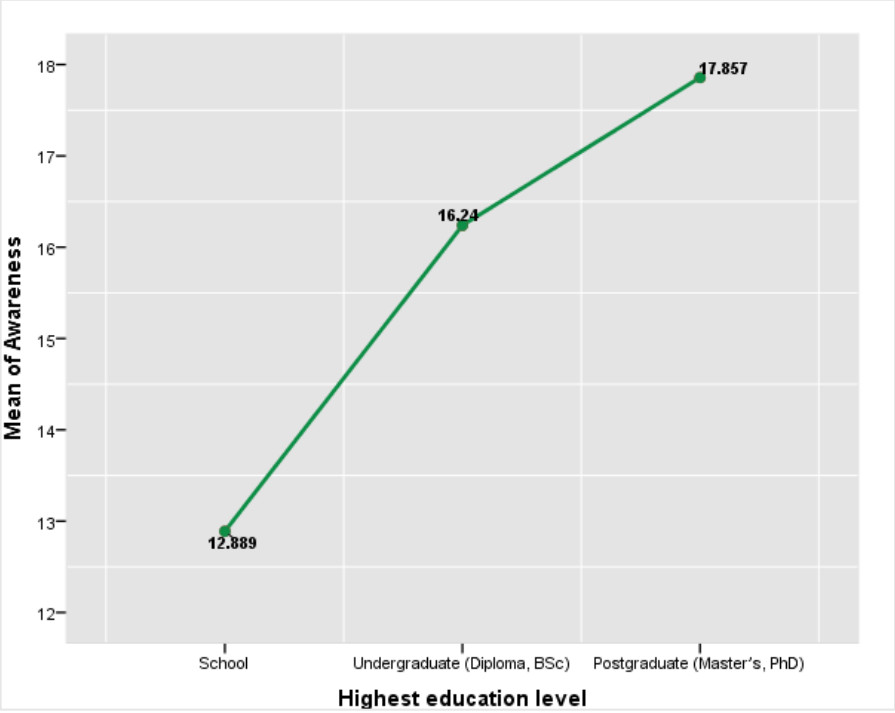


Figure 7.25 Education level wise differences in awareness

The study has found positive relationship between the level of awareness and the level of education. Similar observations were found in various studies (Wahyudiwan et al., 2017; Ogutcu et al., 2016; Aliyu et al., 2017). The more the respondents perceive threats, their behavior becomes more protective. The more the respondents perceive threats, their behavior becomes more protective. Their perception of threats is raised from the level of education and awareness of cyber security threats.

7.4.1.4. Pre-test and post-test difference in experience of creating a password

To check whether there is a significant difference in the pre-test and post-test experience of creating a password a paired sample t-test was employed. As the following Table represents, the experience of creating a password significantly differ (-30.71, $p < 0.05$) between pre-test and post-test. Due to the means of the pre-test and post-test experience and the direction of the t-value, it can conclude that there was a statistically significant improvement in the experience of password creation following the programme from 1.49 ± 0.05 to 18.60 ± 5.82 ($p < 0.05$); an improvement of 17.101 ± 5.54.

Table 7.6 t-test results of experience of creating a password

		Mean	***SD***	***SE***	**95% Confidence Interval of the Difference**		***t***	***df***	***Sig.***
					Lower	Upper			
Pair 1	Age – Password Creation	-17.10	5.54	.56	-18.20	-15.10	-30.70	98	.000

As identified earlier experience of creating a password differ in the pre-test and post-test results. Hence to identify whether this difference consistent across two age groups (above 30, under 30) two way ANOVA (a statistical technique wherein, the interaction between factors, influencing variable can be studied with two independent variables) was conducted. The two-way ANOVA test is an extension

of one-way ANOVA test to analyse the influence of two independent categories on a continuous dependent variable. Here, since the difference in pre-test and post-test results across two age groups is examined, the two-way ANOVA test is used. There was a statistically significant interaction between the age group and test on the experience of creating a password, F (1, 95) = 6.48, *p* = .012. And the effect size was medium ($\eta^2 = 0.064$). The experience of creating password was found to be more enjoyable by the participants under 30, compared to the participants aged above 30 years. The reason might be the attractiveness of gaming interface for younger population compared to the older. The younger participants were more involved in the gaming and were quick in adapting various awareness techniques integrated in to the gaming; whereas the older participants were slow in adapting the techniques but were found to be efficient in creating strong passwords, which is due to their awareness levels.

Table 7.7 Two-way ANOVA results of experience of creating a password

Source	Type III Sum of Squares	*df*	Mean Square	F	*Sig.*	Partial Eta Squared
Corrected Model	1269.830[a]	3	423.28	19.63	.000	0.38
Intercept	33289.61	1	33289.61	1544.19	.000	0.94
Test	937.51	1	937.51	43.49	.000	0.31
Age	5.46	1	5.46	.253	.616	0.003
Test * Age	139.77	1	139.77	6.48	.012	0.06
Error	2048.01	95	21.56			
Total	37553.00	99				
Corrected Total	3317.84	98				

At the pre-test stage, above 30 aged respondents had a better experience (17.00 ± 1.038) than the under 30 respondents (14.10 ± .85). However, that was changed at the post-test stage where under 30 respondents had a better experience level (22.79 ± .862) compared to above 30 (20.85 ± 1.038).

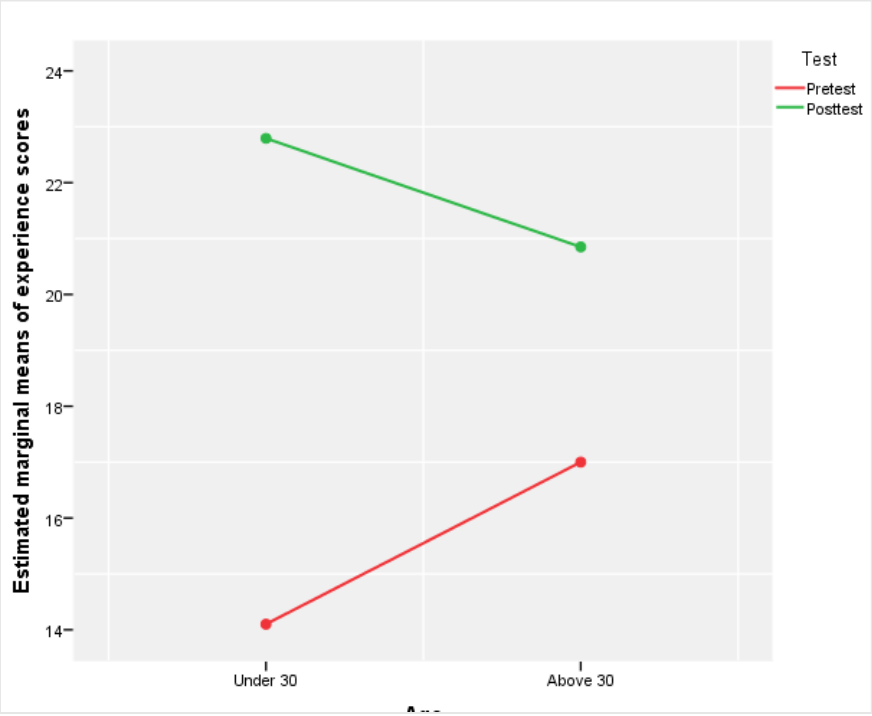


Figure 7.26 Mean plot of the experience change according to the test and age group

7.4.1.5. Heuristics evaluation of post-test results

Game usability (-30.87, $p < 0.05$), learning content (39.01, $p < 0.05$) and ability to enjoy (-28.86, $p < 0.05$) significantly differed between under 30 and above 30 respondents. Due to the means of the usability, learning content, enjoyability and the direction of the t-values, it can conclude that there is a statistically significant decrease in usability, learning content and enjoyability after age 30. As explained in the previous section, the learnability and enjoyability of the gaming application may decrease with the increasing age of the participants. Gaming applications are found to be more popular among the younger generations compared to the older generations (Huynh et al., 2017; Li & Kulkarni, 2016). It was also observed that gaming continuity is found to be more applicable among the younger group

population than the older group population (Cullinane et al., 2015). The findings related to the usability, learning and enjoyability presented in the table 7.8, justified the above observations.

Table 7.8 Usability, learning content and enjoyability across two age groups

		Mean	***SD***	***SE***	**95% Confidence Interval of the Difference**		***t***	***df***	***Sig.***
					Lower	Upper			
Pair 1	Age - Usability	-17.96	4.07	.58	-19.13	-16.79	-30.87	48	.000
Pair 2	Age - Learning Content	-19.57	3.51	.50	-20.58	-18.56	-39.01	48	.000
Pair 3	Age - Enjoyability	-14.02	3.40	.49	-14.10	-13.04	-28.86	48	.000

Usability, learning content and enjoyability was decreased after age 30. Usability was decreased in -3.16 ± 1.031, $p < 0.05$, learning content was decreased in -3.77 ± .762, $p < .05$ and enjoyability in -4.02 ±.679, $p < .05$.

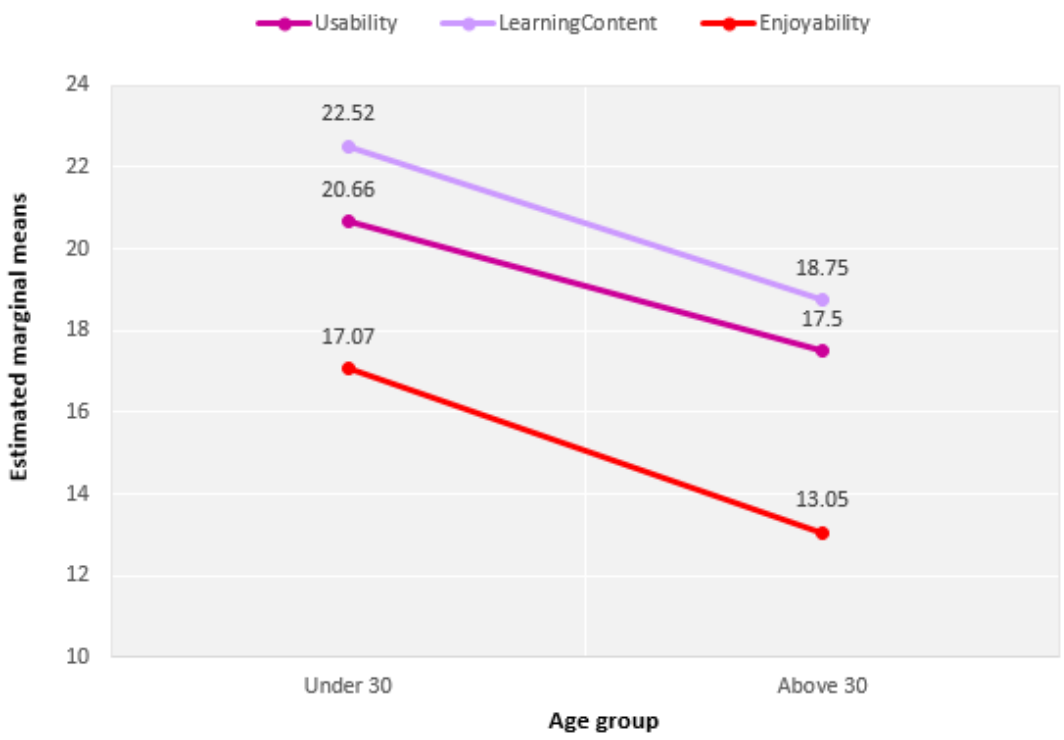


Figure 7.27 Mean plot of game usability, learning content and enjoyability

7.5.2. Malware Guardian Game

The inferential analysis for Malware Guardian game is conducted by comparing various attributes like age vs awareness; education levels vs awareness; differences in pre and post study results etc. This analysis would help in investigating if the factors like age, education have any impact in creating understanding malware concepts, learning, and achieving awareness. The game is developed with an objective to create awareness about IT threats such as malware, which may not be easy to understand by the non-IT or people with less qualification. But the game uses a story scheme, which would be easy to understand by both no-technical and less qualified people. So, there is a need to investigate and analyse how the influential factors such as age and education impact the process of creating awareness through games. This analysis would help in developing the awareness applications by considering the influential factors

such as age and education, in the process of creating storyline and other design aspects that would be more appealing to the target group.

7.4.2.1. Age and the malware awareness differences at the pre-test stage

At the pre-test stage only significant difference in awareness was observed in the backup ($F = 5.77$, $p < 0.05$). Understanding malware ($F = 2.18$, $p > 0.05$) and anti-malware program ($F = .21$, $p > 0.05$) were not significantly differed across the two age groups.

Table 7.9 Age and the malware awareness differences

		Sum of Squares	*df*	Mean Square	*F*	*Sig.*
Understanding Malware	Between Groups	21.71	1	21.71	2.18	.15
	Within Groups	479.11	48	9.98		
	Total	500.82	49			
Anti-Malware program	Between Groups	10.34	1	10.33	1.59	.21
	Within Groups	313.04	48	6.52		
	Total	323.38	49			
Backup	Between Groups	19.67	1	19.67	5.77	.02
	Within Groups	163.61	48	3.41		
	Total	183.28	49			

Tough only the awareness in backup significantly differed between age groups, malware understanding, anti-malware program and backup experienced an increase in awareness after the age 30 (see below Figure).

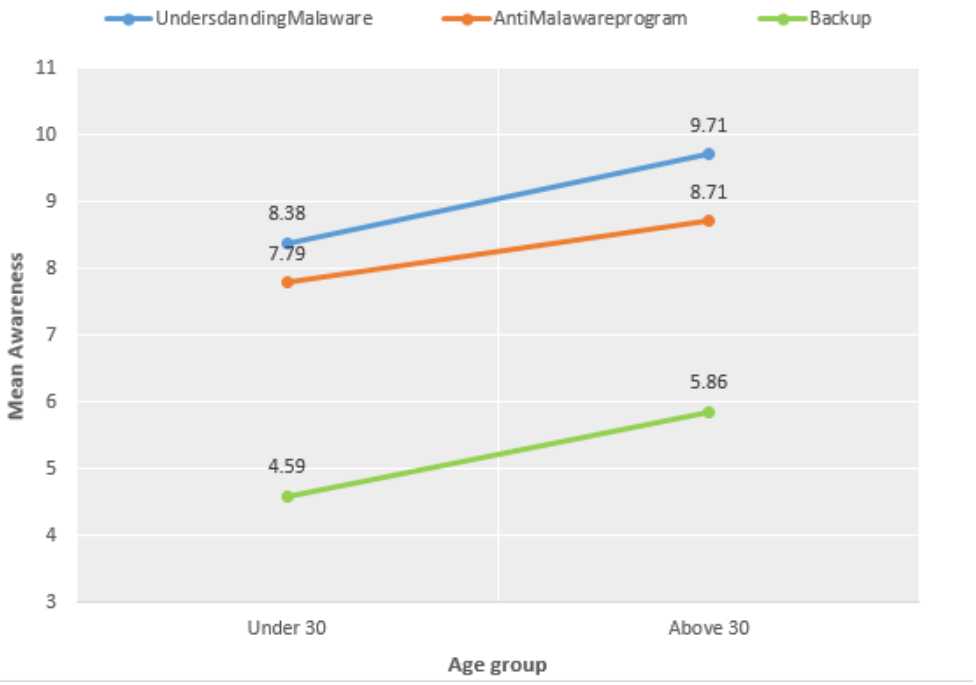


Figure 7.28 Malware awareness at the pre-test stage (age wise)

7.4.2.2. Education level and the malware awareness differences at the pre-test stage

As the one-way ANOVA results indicated, awareness about the anti-malware program differed across the education levels (F = 4.6, $p < 0.05$). Other differences were not significant; understanding malware (F = 1.92, $p > .05$), backup (F = 1.38, $p > .05$).

Table 7.10 Education levels and the malware awareness differences

		Sum of Squares	*df*	Mean Square	*F*	*Sig.*
Understanding Malware	Between Groups	37.84	2	18.92	1.92	.16
	Within Groups	462.98	47	9.85		

	Total	500.82	49			
Anti-Malware program	Between Groups	52.89	2	26.44	4.60	.02
	Within Groups	270.50	47	5.76		
	Total	323.38	49			
Backup	Between Groups	10.19	2	5.10	1.39	.26
	Within Groups	173.09	47	3.68		
	Total	183.28	49			

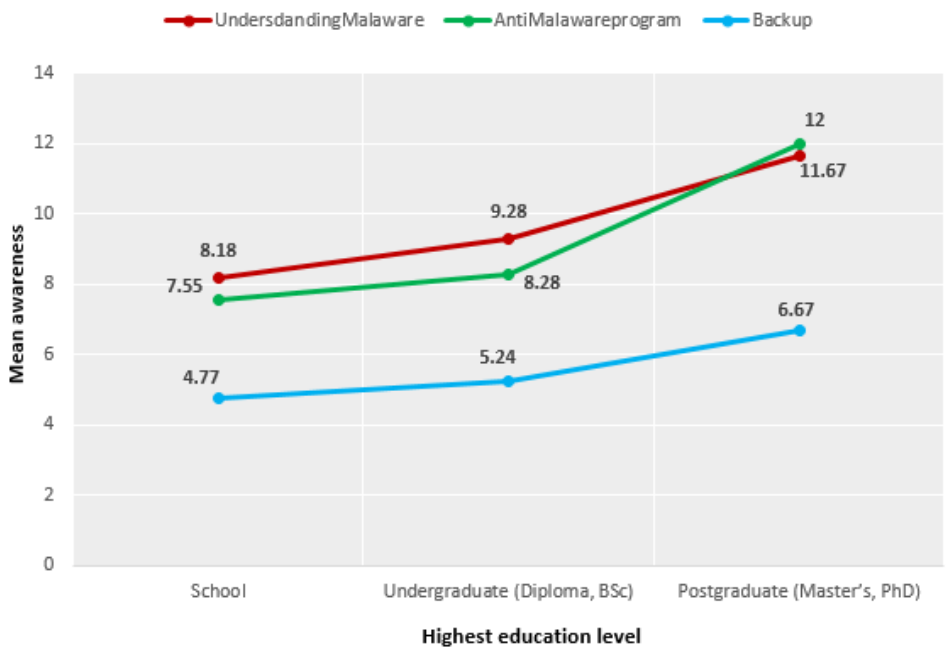


Figure 7.29 Awareness differences according to the highest education level

7.4.2.3. Pre-test and post-test difference in malware experiences

Pre-test and post-test results were significantly differed in understanding malware (t = -25.19, $p < .05$), understanding anti-malware programs (-31.58, $p < .05$) and understanding about backup (-24.35, $p < .05$).

Table 7.11 . t-test results of malware experience

		Mean	*SD*	*SE*	95% Confidence Interval of the Difference		*t*	*df*	*Sig.*
					Lower	Upper			
Pair 1	Test – Understanding Malware	-17.96	4.07	.58	-19.13	-16.79	-30.87	48	.000
Pair 2	Test – Anti Malware program	-19.57	3.51	.50	-20.58	-18.56	-39.01	48	.000
Pair 3	Test - Backup	-14.02	3.40	.49	-14.10	-13.04	-28.86	48	.000

The direction of t value indicated that understanding about malware in all three departments was increased after the program. As in the following Figure, post-test mean scores have experienced a significant increase.

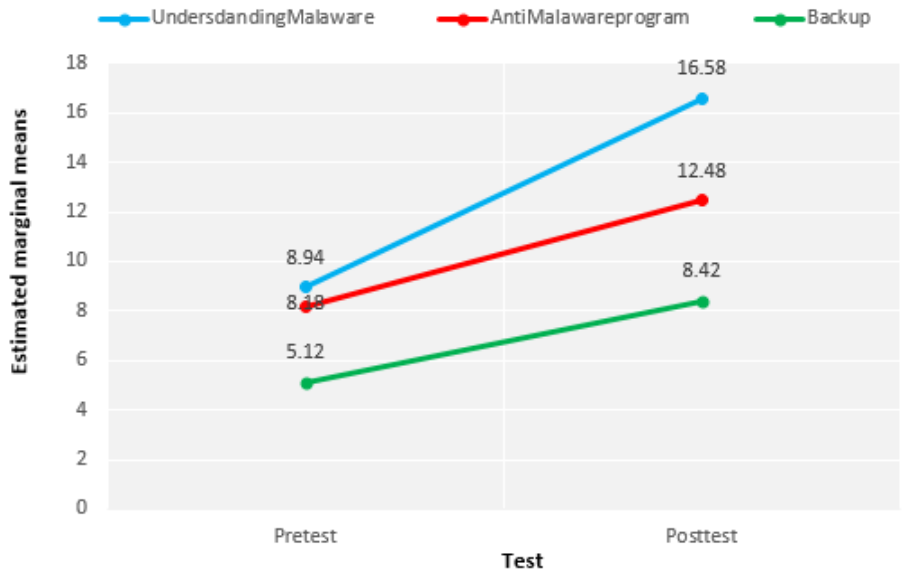


Figure 7.30 Mean plot of malware understanding

Malware experience differed in the pre-test and post-test results. Hence a two-way MANOVA was conducted to examine the effect of age group and test (pre-test / post-test) on malware experience. There was a statistically significant interaction between the effects of age group and test on malware experience, Wilks' lambda (Λ) = .85, *p* = .002. And the effect size was large ($\eta^2 = 0.15$).

Table 7.12 Two-way MANOVA results of malware experience

Effect		Value	F	Hypothesis df	Error df	Sig.	Partial Eta Squared
Intercept	Pillai's Trace	.97	896.281[b]	3.000	94.000	.000	.966
	Wilks' Lambda	.03	896.281[b]	3.000	94.000	.000	.966
	Hotelling's Trace	28.61	896.281[b]	3.000	94.000	.000	.966
	Roy's Largest Root	28.61	896.281[b]	3.000	94.000	.000	.966
Test	Pillai's Trace	.64	55.509[b]	3.000	94.000	.000	.639
	Wilks' Lambda	.36	55.509[b]	3.000	94.000	.000	.639
	Hotelling's Trace	1.77	55.509[b]	3.000	94.000	.000	.639
	Roy's Largest Root	1.77	55.509[b]	3.000	94.000	.000	.639
Age	Pillai's Trace	.02	.715[b]	3.000	94.000	.546	.022
	Wilks' Lambda	.98	.715[b]	3.000	94.000	.546	.022
	Hotelling's Trace	.02	.715[b]	3.000	94.000	.546	.022

		Roy's Largest Root	.02	.715[b]	3.000	94.000	.546	.022
Test * Age		Pillai's Trace	.15	5.544[b]	3.000	94.000	.002	.150
		Wilks' Lambda	.85	5.544[b]	3.000	94.000	.002	.150
		Hotelling's Trace	.18	5.544[b]	3.000	94.000	.002	.150
		Roy's Largest Root	.18	5.544[b]	3.000	94.000	.002	.150

a. Design: Intercept + Test + Age + Test * Age

b. Exact statistic

According to the two-way MANOVA, Malware experience differed across age groups and tests. Figure 7.31 displays these differences clearly, where at the pre-test stage respondents who aged above 30 had a better malware experience. But at the post-test stage respondents who aged under 30 had a better malware experience than the above 30 group.

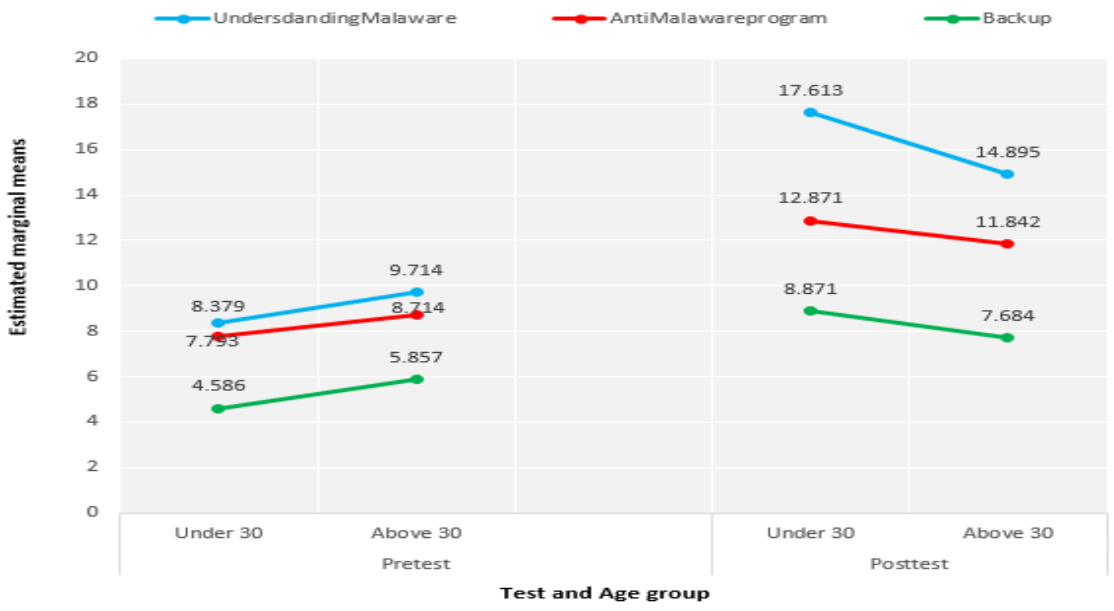


Figure 7.31 . Effects of test and age on the malware experience

7.4.2.4. Heuristics evaluation of post-test results

Game usability (-33.34, $p < 0.05$), learning content (-37.75, $p < 0.05$) and ability to enjoy (--32.96, $p < 0.05$) significantly differed between under 30 and above 30 respondents. Due to the means of the usability, learning content, enjoyability and the direction of the t-values, it can conclude that there is a statistically significant decrease in usability, learning content and enjoyability after age 30.

Table 7.13 Usability, learning content and enjoyability across two age groups

		Mean	*SD*	*SE*	95% Confidence Interval of the Difference		*t*	*df*	*Sig.*
					Lower	Upper			
Pair 1	Age - Usability	-18.50	3.92	.56	-19.62	-17.39	-33.34	49	.000
Pair 2	Age - Learning Content	-19.54	3.66	.51	-20.58	-18.50	-37.75	49	.000
Pair 3	Age - Fun Enjoyment	-14.82	3.18	.45	-15.72	-13.92	-32.96	49	.000

Usability, learning content and enjoyability was significantly decreased after age 30. Usability was decreased from 21.26 to 17.63, learning content was decreased from 22.1 to 19 and enjoyability was decreased from 17.29 to 14.42.

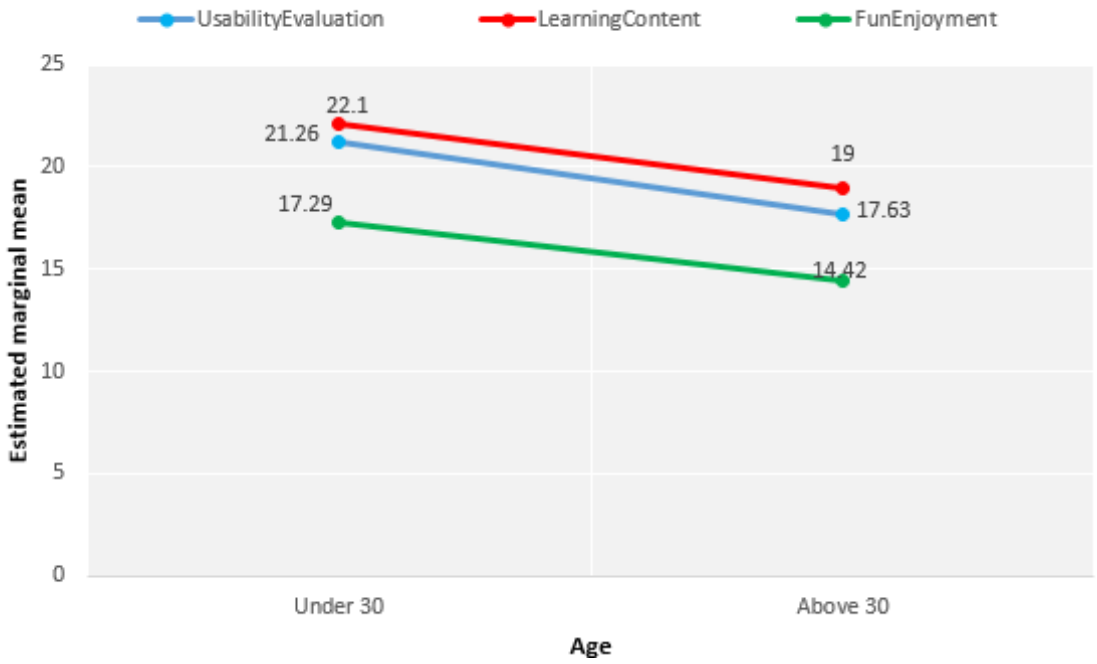


Figure 7.32 Usability, learning content and enjoyment across age groups

7.6. Discussion

Pre/post password game: Of the total data breaches, 35% of them were found to be because of human factors reflecting the poor awareness and strategies adopted by the people in regards to cyber security (Crucial Research, 2014). More than 90% of the data breaches across the world were found to be the result of using weak passwords (Beyer & Brummel, 2015). In addition, 2,802,478,934 web users using “123456” as their password in 2014, according to the Crucial Research report. Accordingly, in the pre-study results, many of the participants used ‘123456’ as their password or a combination of alphabets and numbers that can be easily targeted as shown in the Table 7.2. Similarly, in Figure 7.2 and Figure 7.6 reflects the level of awareness about the concept of password including the length, mix of characters, ability to remember passwords of more than eight characters, and also the understanding of password strength. All the aspects of the password awareness were found to be of very low awareness. These findings suggest that the humans or general public activities are one of the major causes which are making it easy for the cyber attackers in enforcing cyber-attacks. One of the major reasons for this situation is the rapid growing number of Internet users, and the lack of awareness about cyber security among them. In a report published by WaterIsac (2015), creating cyber security awareness and using strong passwords are the two important cyber security measures outlined in the top 10 measures. The following major people related issues in cyber security were identified by Crucial Research (2014).

- Lack of knowledge and awareness
- A relaxed culture
- Ineffective training programs
- Lack of management training
- An environment that does not encourage teamwork
- Cultural differences

Addressing these issues by organizations, governments and other organizations can effectively improve the cyber security aspects among the people. As discussed in previous sections Teymourlouei (2015) has suggested various methods such as backup, using Malware Guardian programs, creating strong passwords etc. using which the people can monitor, diagnose, and prevent any cyber-attack. Moreover, savvy users likely require different training content than naïve users. They need training tailored to their particular learning needs in order to make smart decisions in cyber space (Beyer and Brummel, 2015). For the end users who have no or very few awareness about cyber security, the awareness programs must be developed with the information about basic security measures. Similarly, for end users who have some knowledge, the awareness programs must be developed considering their knowledge levels and the new threats arising. Teymourlouei (2015) found that creating strong passwords could as one of the effective means of securing from cyberattacks by the users, which highlights the importance of creating strong and complex passwords. Similarly, WaterIsac (2015) supported the same idea of creating strong passwords. The findings from the literature review and previously conducted studies stressed the importance of creating password security awareness, which is identified as one of the most common human error factors that can lead to a data breach and found that gamification can be used as a technique to address the issue to a large extent.

Accordingly, the Password Protector game was developed considering the needs and requirements of Saudi population. The study has identified positive impact of the game on creating awareness among the participants. One of the major developments observed among the participants about the awareness about password in the post-study results was that majority of them (70%) were found to be fully aware of the concept of password strength. There was a significant improvement in the awareness levels as in the pre-study only 18% of them were found to be fully aware of the concept of password strength as evident from Figure 7.2. Similarly, significant improvements were observed in the ability to remember passwords of more than eight characters Figure 7.3, using different set of

characters in creating passwords Figure 7.4. The mean strength of the password in pre-study was 59.1, which increased to 80.2 after the study. The increase in these abilities can be attributed to the increase in the awareness and knowledge of using passwords by playing the game, where participants are required to remember the password they created and enter in the next level. In addition, the password meter has helped the participants to understand and create complex passwords, as it is evident from the Table 7.1, where the complex passwords with strength of 100% were observed. This denotes the significant improvement among the participants in creating strong and complex passwords.

The password game was evaluated in terms of usability, learnability and enjoyability. The heuristics evaluation strategy was originally designed to assess the usability of software programs. They assess the user opinion about a given user interface and assess the usability component of the interface. It tries to understand how easily and effectively the users of an application will be able to reach the application objectives. Several versions of heuristics evaluation methods exist and in the context of mGBL, there have been few works that have designed strategies for evaluating learning based games (Korhonen and Koivisto, 2006; Pinelle, et al., 2008; Zaibon and Shiratuddin, 2010). Almost all the usability aspects including control features, interface design, visual appeal, audio, and layout were rated very good and excellent by more than 75% of the participants. Similar results were observed in learnability (content, raising awareness, information, easy to learn); and also, in enjoyability in learning about passwords and fun in playing the game. These results reflect that the Password Protector game was found to be engaging and effective in raising cyber security awareness relating to the passwords. In correlation analysis various findings were observed. It was observed that the participants who were aged 30 and above were able to use better characters for creating complex passwords and also in remembering them compared to their counterparts. It was also observed that level of education had little impact on the creation of awareness, as a result the game can be used by larger section of the people. There were few limitations/comments observed in

the game by few participants which included such as diversifying levels, increasing challenge or levels, setting up alerts and reminders for users to re-exercise, changing sounds, and increasing complexity/hardness. However, one of the interesting comments identified was that the game is suitable for younger generation, who are relatively new to Internet, and are more prone to security threats. The overall comments analysis reflects that majority of the participants were happy with the game, however few design aspects were suggested to be improved.

Supporting the results, the larger *t* value and *p* value of 0.00001 (<0.05) validates the results as significant. It is worthy to note that there are considerable number of participants' who were not finding it easy to remember password more than eight characters long. It can be used as a benchmark for creating complex passwords with varied combinations to achieve higher password strength.

Additionally, significant changes were observed in the experience of creating password before and after the study. The direction of t-value has proved to be significant in this area with an improvement of 17.10 ± 5.54. The results show that by playing the Password Protector game there is a significant positive experience among the participants' in creating strong passwords. In further analysing the results it was observed that the participants' aged under 30 had better experience compared to the participants' aged above 30, reflecting that the younger participants found the game more useful in terms of raising awareness in creating strong passwords and also in improving skills and knowledge. The heuristics evaluation of the usability, learning content and enjoyability has found that the Password Protector game had low impact in these aspects for the participants' aged above 30, when compared to the participants' aged below 30. These results reveal that the Password Protector game is more attractive and had more positive impact on the participants under the age of 30, as the usability, learning content and enjoyability aspects for this group achieved steep increase in the results. The ANOVA results indicated that the awareness means at school level education (12.9), and graduate level education (17.86) were not significantly differed. This

reflects that education had a minimal impact on awareness about creating strong passwords.

Pre/post Malware Guardian

Teymourlouei (2015) has suggested selecting strong and different passwords, keeping the personal information confidential, using anti-virus softwires, avoiding public Wi-Fi's, safe browsing like disabling password reminders, blocking pop-ups, setting Internet security zone level etc., regular software updates, using firewalls, being cautious while downloading free software (freeware), avoiding P2P (Peer to Peer) downloads, using email security, incident reporting, and most importantly regular backup for preventing the data loss as the major ways to be adopted by the users to prevent themselves from a cyber-attack. However, the pre-study survey results, have found that the level of awareness about malware and related threats was very poor Figure 7.11 and Figure 7.14. Even minor aspects like anti-virus use Figure 7.15, difference between manual and automatic scanning Figure 7.17 and the importance of backup Figure 7.18 were not understood by the participants.

Comparing the pre and post study results for malware guardian game, it was observed that most of the participants developed good understanding about the concepts of malware after completing the study as they were aware of the most of the concepts stated by Teymourlouei (2015). Bogdanov (2015) has identified that malware attacks can be even delivered from the trusted sources, which reflects the complex nature of malware attacks. Therefore, there is a need for effective awareness creating platforms to minimise the attacks and the data loss. Malware Guardian game related games as developed by various sources (Federal Trade Commission, 2017; Australian Department of Broadband Communications and the Digital Economy, 2017; National Centre for Missing & Exploited Children, 2017; cyber security challenge UK, 2017) were found to be having significant results in creating awareness about malwares.

In addition, they were able to identify and understand different types of malware and the harm they could cause; and the need for backup and program updates. Malware Guardian game was evaluated for its usability, learnability and enjoyability. Almost all the usability aspects including control features, interface design, visual appeal, audio, and layout were rated very good and excellent by more than 75% of the participants. Similar results were observed in learnability (content, raising awareness, information, easy to learn); and also, in enjoyability in learning about passwords and fun in playing the game. These results reflect that the Malware Guardian game was found to be engaging and effective in raising cyber security awareness relating to the Malware. However, differences were observed in relating the education and understanding the malware concepts, backup, and anti-malware software. The participants were able to identify various threats identified by US Department of Homeland Security (2016). Significant improvement was also observed in understanding the importance of backup, anti-malware software, and updates Figure 7.15 and Figure 7.18 after using the malware game by the participants. Raising such awareness levels could greatly contribute the damages caused by malware attacks as identified by FireEye (2017). Participants with higher education levels had a better understanding compared to those with low education levels.

Various findings were observed in the correlation analysis of the malware guardian game study results. The understanding of main concepts of malware including backup, anti-malware software s, and types and impact of malwares was not significantly differed across the age groups at pre-test stage, reflecting the poor knowledge across all the age groups. Although awareness levels were increased in the post-study analysis, no significant differences were observed among the age groups. There are few limitations that were observed in the Malware Guardian game by the participants which included that the game must allow the OS update, increasing time for each level, good design of bugs, and using 3D technology in the game. Most of the limitations were related to design specifications. However,

the objective of the game for generating the awareness was successfully achieved. These limitations can be used as the suggestions for further developing the game.

Additionally, significant changes were observed in post study analysis of Malware Guardian game in three main areas including understanding the concept of malware; understanding the anti-malware programs; and understanding the importance of backup among the participants', with all the observations achieved *p*-value (<0.05) and t-values proving the results to be significant. Further analysing the results, the Malware Guardian game was found to be having better experience in these three aspects among the participants' aged under 30 when compared to the participants' aged above 30. It indicates that the younger participants are more involved in the game and had good experience. The MANOVA results indicated that the participants below age 30 years had a significant improvement in understanding malware, malware programs, and the importance of backup compared to those participants aged above 30 years. The results clearly indicated that the gamification had a major impact in creating awareness across the younger population compared to the older population. The heuristics evaluation of the Malware Guardian game revealed similar results compared to password game. Participants' aged under 30 had better experiences in usability, learning content and enjoyability aspects compared to those aged above 30. This specific trend is observed across all the questions in the survey, and the reason might be because of more engagement of young people with digital/mobile devices and using them as a means of accessing various services including education and knowledge sharing.

7.7. Summary

This chapter focused on the investigation of Password Protector and Malware Guardian games in creating cyber security awareness and evaluating the games using heuristics evaluation strategy. The results from the pre and post study survey analysis for both games have shown significant improvements in the level of understanding of the participants' about creating strong passwords, password

strength; identify malware, malware attacks, need for anti-malware programs, backup as protective strategy, and increasing awareness levels. Both games achieved higher ratings in the heuristics evaluation process concerning awareness levels, usability, learning contents, and fun and enjoyability features. However, participants aged below 30 found both games more engaging and effective in creating awareness by improving knowledge, compared to those aged above 30.

The results suggested that both Password Protector and Malware Guardian games can be more engaging with younger participants. The study has highlighted several key points in the analysis which can be used as the focus points for further extending the research or future research works.

Chapter Eight

Summary and Conclusions

8. Conclusions and future work

Cyber security is one of the major areas of concerns across the globe, and the threats arising in cyberspace has been growing rapidly. The costs incurred, the data lost, the people affected has also been on the rise. With the increasing adoption of Internet technologies and the rising mobile and Internet users across the globe has increased the size of cyberspace which is the playground for launching various attacks through malwares, viruses, worms, etc. by the cyber attackers. As in the cyberspace everything is connected, and people are the most important component in the cyberspace. There are various security attacks that take place every day in the cyberspace with or without the knowledge of the general Internet users. The rising Internet population who are not fully aware of the cyber threats is one of the major advantages for the cyber attackers to initiate and launch various advance cyber-attacks that may not be even recognised by the security tools if not updated regularly. Therefore, there is an increasing need to create awareness among the people about the threats arising from the cyberspace and the measures to be put in place to combat such threats. The public cyber security is one of the important areas that need to be addressed through various solutions.

Creating awareness should result in the behavioural change in the people in the ways they access Internet. Most importantly awareness programs must be engaging and effective in increasing the knowledge levels of the users. In this thesis, this issue is addressed through gaming approach. Games are applications that include the use of graphics, puzzles, and interactive features which attracts the players' attention and engages them in playing the game with good concentration levels to win the game. The gaming approach is an effective method in gaining attention of the users and making learning enjoyable when compared to the traditional awareness methods like oral education, TV ads, or other methods which could have minimal impact in acquiring the viewers' attention.

As the part of study, the cyber security awareness levels of the people in Saudi Arabia were investigated through a quantitative method (survey) to gather the results from larger population. It was found that the cyber security awareness levels of the Internet users are very low, and there is a rapid increase in the Internet and mobile users in Saudi Arabia. In addition, there are not many awareness programs that are aimed at cyber security identified in the region, and majority of them were not happy with the current initiatives being taken by the responsible authorities to increase the cyber security awareness. It was observed that there is a rise in the cyber-attacks in the recent years with advanced techniques that are hard to be detected. It was also found in the study that majority of the people were interested in using an application type of cyber security model to increase their knowledge levels.

Therefore, keeping in view of the problem in the country regarding the rising cyber threats and lower awareness levels, the advantages of gaming approach for creating awareness, two mobile games, focusing on the two major and common aspects (Password and Malware) of cyber security were developed and evaluated in this study. The Password Protector game educates the importance of creating strong passwords in an effective and interactive manner. Similarly, the Malware Guardian action game engages the users in attacking various types of malware through right tools, along with other aspects like backup and updates. Both games were evaluated using heuristic techniques, including the three aspects: learning, enjoyability, and usability. The change in the awareness levels was assessed using a pre and post study survey and it was found that both the games had a strong impact on the participants' and their knowledge levels has observed a significant improvement. In addition, the usability, learnability, and enjoyability aspects of both the games were found to be effective. However, it was found that the young players (<30 years) were more involved in the games and their knowledge levels has seen a sharp increase when compared to the older players (>30 years).

Thus, the thesis has found that gamification (through Password Protector and Malware Guardian games) is an effective way to increase the cyber security awareness among the general public in Saudi Arabia and is an effective way to combat public cyber security threats.

8.1. Research Summary

This study is discussed in four sections including the findings from literature review, the cyber security awareness in Saudi Arabia (problem), the use of gamification as an approach for study, and the evaluation of the approach (two games including Password Protector and Malware Guardian). The major findings and contribution of the study can be summarised in the following points:

- Literature Review has identified that the issues concerning cyber security are increasing and evolving through the time with updated techniques that are hard to be identified and mitigated. There are various cyber security practices outlined by various organizations to restrict and prevent cyber threats. However, lack of awareness is one of the major problems identified by various researchers for increasing public cyber security threats and concerns and various programs and initiatives were suggested for increasing the cyber security awareness. It is interesting to note that about 46% of the world population is connected to Internet. More than 90% of the data breaches are discovered by external parties and 63% of the data breaches are caused by weak, or default or stolen passwords. Most of the public cyber security threats and attacks are caused due to lack of awareness about safety measures among the public. Majority of the security attacks are targeted at common people and it was identified that simple errors like using weak passwords can be an easy node to attack One of the important aspects of combating cyber security threats is the role of users who need to be aware of various security practices in order to combat cyber security attacks. The literature review has helped in reviewing the importance and the need for enhancing the knowledge of cyber security

among the public through effective approaches like Mobile applications, and it is identified as one of the effective approaches.

- Saudi Arabia is one of the fastest growing countries in the Arab region and has been transforming its operations through extensive investments in technology. From the case study, it was observed that there is an increasing trend in the cyber-attacks and rising security issues in the country. It was also found that the number of studies focusing on the aspects of cyber security and awareness are very few, and there was no study found in these aspects, investigating the role of application based cyber security awareness, which is one of the major research gaps identified.

- The pilot study conducted through a survey conducted for assessing the current levels of cyber security aspects (cyber security awareness, practices, and incident reporting) among the public has found high internet usage using various types of devices and mainly for the purpose of entertainment, communication, social networking etc., which are few major modes used for security attacks. In addition, poor security practices such as not using backups, updates, antivirus software etc. were found to be the result of poor awareness levels about cyber security practices.

- Awareness approaches are related to the behavioural aspects of the people, and therefore need methods that would be interesting and attract the attention of the users. Gamification in this scenario can be an effective medium for raising cyber security awareness, and various studies has implemented this technique and found positive results in increasing the awareness of the users. The systematic review of 12 papers investigated has found positive results in using gamification method for raising cyber security awareness, and 10 popular cyber security games were reviewed to analyse the security aspects that were introduced through the games to the users, and found that most of them focused on data loss prevention,

security against malware, and identity theft etc. Majority of the games were developed for students or employees but no games were found with general public as audience, which again is one of the major research gaps identified.

- Considering these factors and using the idea of using gamification as a method for security awareness, 12 mobile game ideas were designed which included Vulnerability Patching, Leak Data Game, Backup Cloud, Phishing Email, Cyber security Helpdesk, Anti-virus, Network Tunnel, Security Incidents, Social Media, Encryption, Password Protector, and Malware Guardian. Given the safety measures, passwords and malwares are the most common security aspects concerned with the general public users. Though creation of the complex passwords is an effective security measure, the attitudes of people towards creating secure passwords are not very favourable. Similarly, malwares are the commonly used means for security attacks that can be spread easily across the cyberspace. Considering these factors, the study considered the development of two mobile games including the Password Protector and Malware Guardian among the 12 that were designed.

- One of the most important aspects of the study is the young participants' in the study and the majority of beginners in using Internet technologies in both Password Protector and Malware Guardian games. Significant improvements can be seen among the participants' in both games in increasing their knowledge about cyber security aspects related to password protection and malware attacks. The participants were able to create stronger and complex passwords after playing the game and the mean password strength achieved was 80.16, which when compare with pre-study mean of 59.12 reflects a significant improvement. Considering the overall results for the Password Protector game, it can be stated that the game has significantly improved the awareness levels of the participants',

its usability, learning, fun and enjoyability features are liked by majority of them.

- Similarly, the pre and post survey results of Malware Guardian game have proved to be similar to the Password Protector game. One of the key points to be noted from the analysis of the results is that majority of the participants were not aware of any concepts related to malware attacks, anti-malware software, and mainly back up as a prevention strategy for data loss during malware attacks, as evident from the pre study survey results. However, the Malware Guardian game has proved to be successful in creating awareness about malware attacks, threats associated with it, using anti-malware software programs, and backup strategy for prevention of data loss during malware attacks. The awareness levels of the participants were significantly improved after playing the game, as evident from the post study survey results analysis.

8.2. Research Achievements

This study was conducted with an objective of addressing the issue of cyber threats using cyber security awareness as a major solution. The literature review in this thesis identified various issues relating to cyber security, including the practices, rise in threats, awareness levels, major public security threats, reviewed application based approach towards cyber security awareness and adding valuable literature to the research database.

This thesis identified the need for cyber security awareness in Saudi Arabia among the general public and has identified various measures b such as organizing national and international events, providing educational and training courses, hosting national and international competitions, conducting public lectures etc. are being taken in the country to combat cyber security threats. In addition, various problems relating to the cyber security in the country were identified, among which poor awareness levels among the public is identified as one of the major problems.

Game-based approaches for raising cyber security awareness was investigated in this thesis. A systematic review of the game-based studies for awareness was conducting and major gaming applications for cyber security awareness were reviewed; contributing valuable information to the research? area in the field of cyber security.

As a part of the study 12 games were designed for cyber security awareness; out of which two games were developed and implemented. The remaining games can be used for further development in combatting other types of cyber threats.

The evaluation study of both Password Protector and Malware Guardian games reflects the effectiveness of gaming approach in raising the public cyber security awareness, thus combating the public security threats. The usability study using heuristic approach has identified the ease of use of gaming as a means to improve the knowledge levels (learning) by engaging the users (enjoyment).

8.3. Research Limitations

The study has focused on one of the important aspects of the cyber world: Cyber security. The scope of cyber security is vast in terms of threats associated and the measures to be taken to safeguard from threats. Considering these, aspects the limitations of this thesis include the following:

- Only specific areas relating to password protection and malware protection are considered as the part of thesis though there are other threats such as identity theft, sniffing, traps etc., which is one of the major limitations.
- Only people from specific region, Saudi Arabia are considered for the study. However, as gamification can be related to socio-psychological and cultural aspects, the impact of such games may or may not deliver same results in other regions.
- The majority of the participants in the study were belonging to younger generation; therefore, the impact of the games on older generation is not clearly addressed in this work.

- The study was cross-sectional and evaluated the results from short duration study. No further longitudinal study was conducted to check the impact in long term.
- The study used only password and malware concepts from the cyber security aspects. There are still many other areas which people need to be aware of.
- There was no study conducted if the games led to any behavioural change among the participants.

8.4. Recommendations for future work

- Implement and evaluate similar games which focus on other areas of cyber security. A new study with design and evaluating the games for other areas of cyber security awareness such as identity theft, phishing, virus attacks etc. can be conducted to test the applicability of gamification on various cyber security issues and related awareness generation.

- Incorporate and modify the Password Protector and Malware Guardian games based on the comments from the participants and revaluate the games. Both the games can be modified according to the participants feedbacks and comments and re-evaluate their impact on improving the awareness levels.

- Link Malware Guardian game to Anti-Malware lab to make it more realistic. The game can be linked to the Anti-malware labs such as Kasper-sky, AVS security, Avast etc., so that users can play in a real-time environment and be updated with the latest security threats and malwares, making it as a real-time learning process.

- Develop social networking and integrate with the games for creating competition among the players and a platform to interact and learn. Using the power of social media can further enhance the experience by sharing the scores, using multi-user environment for enhancing competition, and providing a way for social interaction through messaging. This integrated

design can be used for developing new cyber security awareness games and evaluate their impact.

- Apply the gamification concept on the different age groups and revaluate the games and their impact. Systematically conduct various studies on a target population defined by various age groups in order to identify on which particular group of people can the gamification process be more effective in creating awareness.

8.5. The Future of Cyber Security Awareness

Cyber security is one of the important areas that need to be addressed as the number and types of security threats are evolving with huge potential to create major losses, in parallel to the developments across the technology. Saudi Arabia is a country where there have been major developments in the field of technology and rapid increase in the adoption of Internet and communication technologies was observed. Accordingly, the rise in cyber threats was also observed in the country. With majority of the people moving towards Internet technology with low awareness about Internet related security threats can be a major issue concerning the country. Considering it as the major issue, this thesis used gamification as a method to increase the cyber security awareness among the people in Saudi Arabia.

To address the issue two major areas of security are considered which include password protection and malware protection. Accordingly, two mobile games including Password Protector and Malware Guardian were developed and evaluated through a survey for assessing the impact in creating awareness. A significant increase in the awareness levels for both games was found. Thus, this approach and the two games can be applied in the context of creating cyber security awareness and can support the development of future research in the related areas. The scope for research in cyber security related aspects is very vast, accordingly the following possible extensions to this work are identified.

- Investigated other major security incidents or threats that target the public and evaluate the possibility of raising awareness through other application based techniques.
- Use the remaining 10 designs proposed in the study for developing the games relating to cyber security threats and evaluate them in the aspects of learnability, enjoyability, and usability.
- The same concepts can be used for developing the right solutions to cyber security through cyber security awareness in other countries experiencing increasing cyber threats and poor public awareness levels about cyber security.
- Further, a comprehensive strategy can be developed through an extensive research study proposing gamification as an effective means to raise cyber security awareness and combat increasing cyber threats.

References

References

1. “High School Cyber Security Game,” Global CyberLympics.
2. Abawajy, J. (2012). User preference of cyber security awareness delivery methods. Behaviour and Information Technology, 33(3), pp.237-248.
3. Abrams, T. (2017). The Importance of Data Backup and Recovery in Any Security Strategy. [online] Dgtechllc.com. Available at: http://www.dgtechllc.com/blog/the-importance-of-data-backup-and-recovery-in-any-security-strategy [Accessed 3 Jan. 2018].
4. Adele, D. *(*2016). A cyber security culture research philosophy and approach to develop a valid and reliable measuring instrument. 2016 SAI Computing Conference (SAI).
5. al-Hussein, I. (2017). 60 million cyber attacks targeted Saudi Arabia in one year. AlArabiya.net. Dammam. [online] Available at: https://english.alarabiya.net/en/media/digital/2017/05/02/60-million-cyber-attacks-targeted-Saudi-Arabia-in-one-year.html [Accessed 4 Jan. 2018].
6. Al-Mayman, H. (2018). Microsoft report reveals top 3 cyberthreats in Saudi Arabia. [online] Available at: http://www.arabnews.com/node/1380911/saudi-arabia [Accessed: 03/12/2018]
7. Albano, K. & Kessem, L. (2017). The Full Shamoon: How the Devastating Malware Was Inserted Into Networks. [online] Available at: https://securityintelligence.com/the-full-shamoon-how-the-devastating-malware-was-inserted-into-networks/ [Accessed: 03/12/2018].
8. Almeida TA, Yamakami A (2010) Content-Based Spam Filtering. In: The 2010 International Joint Conference on Neural Networks (IJCNN), Barcelona, pp 1–7.
9. Arachchilage N. A. G. and Love S. (2013). *A game design framework for avoiding phishing attacks.* Journal of Computing and Human Behaviour, vol. 29, no. 3, pp. 706–714.

10. Arachchilage N. A. G. and Love S. (2014). *Security awareness of computer users: A phishing threat avoidance perspective*. Journal of Computing and Human Behaviour, vol. 38, pp. 304–312.
11. Arachchilage, G. and Asanka, N. (2012). Security awareness of computer users: A GBL approach , Brunel University, School of Information Systems. Available at: http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.425.7856and rep=rep1and type=pdf [Accessed 19 Jan. 2017]
12. Ariyapperuma S. and Minhas A. (2005). *Internet security games as a pedagogic tool for teaching network security.* Frontiers in Education Proceedings 35th Annual Conference.
13. Ashford, W. (2015). Top 10 Cybercrime stories of 2015. Computer Weekly. [online] Available at: http://www.computerweekly.com/news/4500260419/Top-10-cyber-crime-stories-of-2015 [Accessed 29 Jan. 2016].
14. Australian Computer Society (2016). Cyber security Threats Challenges Opportunities. [online] Australian Computer Society, pp.2-20. Available at: https://www.acs.org.au/content/dam/acs/acs-publications/ACS_Cyber security _Guide.pdf [Accessed 3 Jan. 2018].
15. Australian Department of Broadband Communications and the Digital Economy (2017). “Stay Smart Online Cyber security Education Modules - Primary.” [Online]. Available: https://budde. staysmartonline.gov.au/primary/main.php#. [Accessed: 03-Jan-2017].
16. Bada M., Creese, S., Goldsmith, M., Mitchell, C., and Phillips E. (2014). Computer Security Incident Response Teams (CSIRTs) An Overview. Available at: https://www.sbs.ox.ac.uk/cyber security - capacity/system/files/CSIRTs.pdf [Accessed 3 Jan. 2018]
17. Bada, M and Sasse, A; (2014) Cyber Security Awareness Campaigns: Why do they fail to change behaviour? Global Cyber Security Capacity Centre, University of Oxford: Oxford, UK.

18. Baig, A. (2017). 10 Internet Security Tools for Online Privacy Protection • The Security Awareness Company. [online] The Security Awareness Company. Available at: https://www.thesecurityawarenesscompany.com/2017/03/29/10-Internet-security-tools-online-privacy-protection/ [Accessed 3 Jan. 2018].
19. Bambenek, J. (2017). Cyber Security Awareness Tip #8: Anti-Virus, Anti-Spyware, and Other Protective Software - SANS Internet Storm Center. [online] SANS Internet Storm Center. Available at: https://isc.sans.edu/forums/diary/Cyber+Security+Awareness+Tip+8+Anti Virus+AntiSpyware+and+Other+Protective+Software/3468/ [Accessed 3 Jan. 2018].
20. Banerjee, A., Cole, S., Duflo, E. and Linden, L. (2007). *Remedying education: Evidence from two randomized experiments in India*, Quarterly Journal of Economics, 122 (3), 1235-1264.
21. Ben-Asher, N. and Gonzalez, C. (2015). Effects of cyber security knowledge on attack detection. Computers in Human Behavior, 48, pp.51-61.
22. Berman, S. (2013). Why planning is key to combating cyber threats and attacks. The Guardian. [online] Available at: https://www.theguardian.com/media-network/media-network-blog/2013/sep/06/planning-key-cyber-threat-attack [Accessed 3 Jan. 2018].
23. Beyer, R.E. and Brummel, B. J. (2015). Implementing Effective Cyber Security Training for End Users of Computer Networks. Society for Human Resource Management and Society for Industrial and Organizational Psychology. Available at: https://www.shrm.org/hr-today/trends-and-forecasting/special-reports-and-expert-views/Documents/SHRM-SIOP%20Role%20of%20Human%20Resources%20in%20Cyber%20Security.pdf [Accessed 2 Dec. 2017]
24. Bodhani, A. (2017). 'Advanced' cyber threat attacks Saudi Arabia - ITP.net. [online] ITP.net. Available at: http://www.itp.net/615846-advanced-cyber-threat-attacks-saudi-arabia [Accessed 4 Jan. 2018].

25. Bogdanov, V. (2015). KEY CYBER SECURITY CHALLENGES FOR 2016. Intersog. Available at: http://intersog.com/blog/key-cyber security - challenges-for-2016/ [Accessed 3 Jan. 2018].
26. Boyle, S. (2011). An Introduction to Games-based learning. [online] Ucd.ie. Available at: https://www.ucd.ie/t4cms/UCDTLT0044.pdf.pdf [Accessed 18 Jan. 2017].
27. Brinda, T., Reynolds, N., Romeike, R. and Schwill, A. (2015). Key competencies in informatics and ICT. University of Potsdam.
28. Bronk, C. and Tikk-Ringas, E. (2013). The Cyber Attack on Saudi Aramco. Survival, 55(2), pp.81-96.
29. Bruijn, H. and Janssen, M. (2017). Building Cyber security Awareness: The need for evidence-based framing strategies. Government Information Quarterly, 34(1), pp.1-7.
30. Choi, M. S., Levy Y., and Hovav A. (2013), The Role of User Computer Self-Efficacy, Cyber security Countermeasures Awareness, and Cyber security Skills Influence on Computer Misuse. Available at: https://eric.ed.gov/?id=ED563192 [Accessed 22 May. 2017].
31. Choucri, N., Madnick, S. and Ferwerda, J. (2013). Institutions for Cyber Security: International Responses and Global Imperatives. Information Technology for Development, 20(2), pp.96-121.
32. Clark, K., Stikvoort, D., Stofbergen, E. and van den Heuvel, E. (2014). A Dutch Approach to Cyber security through Participation. IEEE Security and Privacy, 12(5), pp.27-34.
33. CMO Council Middle East (2015), 'Facts and Figures', 2015. [online]. Accessed: http://www.cmocouncil.org/mena/facts_stats.php [Accessed: 28- Nov- 2015]
34. Costabile, M. F., Angeli, A. C. D., Lanzilotti, R., Ardito, C., Buono, P. and Pederson, T. (2008). *Explore! Possibilities and challenges of mobile learning.* Proceedings of the twenty-sixth annual SIGCHI conference on Human factors in computing systems, Florence, Italy

35. Crucial Research (2014). People's Role in Cyber Security: Academics' Perspective. A white paper by Crucial Research. Available at: https://www.crucial.com.au/pdf/Peoples_Role_in_Cyber_Security.pdf [Accessed 3 Jan. 2018]
36. Cyber security challenge UK (2017). "cyber security challenge uk.". Available at: http://cyber security challenge.org.uk/. [Accessed: 03-Jan-2017]
37. Dasgupta D., Ferebee D. M., and Michalewicz Z. (2013). *Applying puzzle-based learning to cyber security education.* Proceedings of the 2013 on InfoSecCD'13: Information Security Curriculum Development Conference, p. 20.
38. Denning T., Lerner A., Shostack A., and Kohno T. (2013). *Control-Alt-Hack: the design and evaluation of a card game for computer security awareness and education.* Proceedings of the 2013 ACM SIGSAC conference on Computer and communications security, pp. 915–928.
39. Department of Health and Human Services (2017). *ONC Game 103 | Cybersecure: Contingency Planning.* Available at: http://www.healthit.gov/sites/default/files/CyberSecure_103_FINAL/index.html [Accessed 18 Jan. 2017].
40. Department of Homeland Security (2018). Cyber security Overview. [online] Department of Homeland Security. Available at: https://www.dhs.gov/cyber security -overview [Accessed 1 Jan. 2018].
41. Dhananjay, Raman, A. and Kaushik, S. (2016). A Comprehensive Study of Contemporary Tools and Techniques in the Realm of Cyber Security. IITM Journal of Management and IT. Volume 7, Issue 1.
42. Doyle, K. (2017). Preventing cyber attacks starts with the individual. Available at: https://www.itweb.co.za/content/VJBwEr7nNol76Db2 [Accessed 3 Jan. 2018].
43. European Union Agency For Network And Information Security. (2017). ENISA overview of cyber security and related terminology. Version 1. Available at: https://www.enisa.europa.eu/publications/enisa-position-

papers-and-opinions/enisa-overview-of-cyber security -and-related-terminology [Accessed 7 Dec. 2017]

44. Fdez-Riverola F, Iglesias E, D´ıaz F, M´endez J, Corchado J (2007) SpamHunting: An Instance-based Reasoning System for Spam Labelling and Filtering. Decision Support Systems 43(3):722–736, DOI 10.1016/j.dss.2006.11.012, Available at: http://linkinghub.elsevier.com/retrieve/pii/S0167923606002041 [Accessed 14 Dec. 2017]
45. Federal Bureau of Investigation (2017) “Kids Games,” FBI. Available at: https://www.fbi.gov/fun-games/kids/kids-games. [Accessed: 03-Jan-2017].
46. Federal Trade Commission (2017). “OnGuardOnline.” [Online]. Available: http://www.onguardonline.gov/media. [Accessed: 02-Jan-2017].
47. FireEye (2017). What is Cyber Security? | FireEye. [online] FireEye. Available at: https://www.fireeye.com/current-threats/what-is-cyber security.html [Accessed 9 Dec. 2017].
48. Fonseca B., Rosen J.D. (2017) Cyber security in the US: Major Trends and Challenges. In: The New US Security Agenda. Palgrave Macmillan, Cham
49. Fowler, F. (2014). Survey research methods. London: Sage Publication.
50. Geers K. (2010). *Live fire exercise: preparing for cyber war.* Journal of Homeland. Security. Emergency. Management, vol. 7, Issue no. 1.
51. Ghazvini, F., Earnshaw, R.A., Robison, D. and Excell, P.S., (2009). *Designing Augmented Reality Games for Mobile Learning Using an Instructional-Motivational Paradigm*, International Conference on CyberWorlds, CW '09, pp.312-319, 7-11 September 2009,
52. Gondree M., Peterson Z. N., and Denning T. (2013). *Security through play.* Secure. Privacy. IEEE Journals, vol. 11, no. 3, pp. 64–67.
53. Goodwin, C.F. and Nicholas J. P. (2013). Developing a National Strategy for Cyber security : FOUNDATIONS FOR SECURITY, GROWTH, AND INNOVATION. Available at: http://download.microsoft.com/download/b/f/0/bf05da49-7127-4c05-bfe8-

0063dab88f72/developing_a_national_strategy_for_cyber_security_.pdf [Accessed 7 Dec. 2017]

54. Groll, E. (2017). Cyberattack Targets Safety System at Saudi Aramco. [online] Available at: https://foreignpolicy.com/2017/12/21/cyber-attack-targets-safety-system-at-saudi-aramco/ [Accessed: 03/12/2018]
55. Hayani Noor Abd Rahim, Suraya Hamid, Miss Laiha Mat Kiah, Shahaboddin Shamshirband, Steven Furnell, (2015) "A systematic review of approaches to assessing cyber security awareness", Kybernetes, Vol. 44 Issue: 4, pp.606-622, https://doi.org/10.1108/K-12-2014-0283
56. Hendrix M., Al-Sherbaz, A. and Victoria, B. (2016). *Game-based cyber security training: are serious games suitable for cyber security training?*. International Journal of Serious Games, Volume 3, Issue 1, pp. 53-61.
57. Hruza P., Sousek, R. and Szabo S. (2014). Cyber-attacks and attack protection. International Institute of Informatics and Systemics. Available at: http://www.iiis.org/CDs2014/CD2014SCI/SCI_2014/PapersPdf/SA975KW.pdf [Accessed 3 Jan. 2018]
58. Information Assurane Support Environment (2017), “CyberProtect.” [Online]. Available at: http://iase.disa.mil/eta/Lists/IA%20Simulations/AllItems.aspx. [Accessed: 03-Jan-2017]
59. Internet Crime Complaint Center (IC3) (2016). “Business E-mail Compromise: The 3.1 Billion Dollar Scam", Ic3.gov. Available at: https://www.ic3.gov/media/2016/160614.aspx. [Accessed: 16- Sep- 2016].
60. Internetlivestats.com (2017). Number of Internet Users (2016) - Internet Live Stats. [online] Internetlivestats.com. Available at: http://www.Internetlivestats.com/Internet-users/ [Accessed 29 Jan. 2017].
61. Irvine C. E. and Thompson M. (2003). *Teaching objectives of a simulation game for computer security.* DTIC Document.
62. Irvine C. E. and Thompson M. (2003). *Teaching objectives of a simulation game for computer security.* DTIC Document.

63. Ismail, Z., Kiennert, C., Leneutre, J. and Chen, L. (2016). Auditing a Cloud Provider's Compliance With Data Backup Requirements: A Game Theoretical Analysis. IEEE Transactions on Information Forensics and Security, 11(8), pp.1685-1699.
64. Jaggo, J. (2016). Game Development Life Cycle. [online] Courses.cs.ut.ee. Available at: https://courses.cs.ut.ee/MTAT.03.263/2016_fall/uploads/Main/slides6 [Accessed 26 Jan. 2017].
65. Jain, S. (2017). Game Development Life Cycle.. [online] game-development-life-cycle-sumit-jain. Available at: https://www.linkedin.com/pulse/game-development-life-cycle-sumit-jain [Accessed 26 Jun. 2017].
66. Johnson, C. (2014). Architectures for Cyber security Incident Reporting in Safety-Critical Systems. Disaster Management: Enabling Resilience, pp.127-141.
67. Juniper Research (2016), "Cybercrime will Cost Businesses Over $2 Trillion by 2019 - Juniper Research", Juniperresearch.com, 2016. [Online]. Available: http://www.juniperresearch.com/press/press-releases/cybercrime-cost-businesses-over-2trillion. [Accessed: 16- Sep- 2016].
68. Kaul, C. and Prasad B. M. K. (2015), Analysis of the Cyber Attacks over the Past Decade. International Journal of Innovations in Engineering and Technology (IJIET).
69. Kayali F., Wallner G., Kriglstein S., Bauer G., Martinek D., Hlavacs H., Purgathofer P., and Wölfle R. (2014). *A Case Study of a Learning Game about the Internet in Games for Training, Education, Health and Sports.* pp. 47–58. Published by Springer.
70. Ke, F. (2008). A case study of computer gaming for math: Engaged learning from gameplay?. Computers and Education, 51(4), pp.1609-1620.

71. Korhonen, H. and Koivisto, E., 2006. Playability heuristics for mobile games. s.l., In Proceedings of the 8th conference on Human-computer interaction with mobile devices and services.
72. Kurkovsky, S. (2009). *Engaging students through mobile game development*. ACM SIGCSE Bull, 41, pp.44-48.
73. Lei, S. (2014). THE NIST CYBER SECURITY FRAMEWORK: OVERVIEW AND POTENTIAL IMPACTS. Vol. 10, Iss. 4, (Summer 2014): 16-19. American Bar Association. Available at: https://www.americanbar.org/content/dam/aba/publications/scitech_lawyer/2014/summer/nist_cyber security _framework_overview_potential_impacts.authcheckdam.pdf [Accessed 22 Dec. 2017]
74. Liu, J., Xiao Y, Li, S., Liang W. and Chen C (2012), "Cyber Security and Privacy Issues in Smart Grids", IEEE Communications Surveys and Tutorials, vol. 14, no. 4, pp. 981-997.
75. Louisville free Public library (2017). Introduction to Google Docs. [online] Lfpl.org. Available at: http://www.lfpl.org/jobshop/docs/google-docs.pdf [Accessed 22 Jan. 2017].
76. Mackenzie A. and Maged M. (2015). Cyber security Skills Training: An Attacker-Centric Gamified Approach. Technology Innovation Management Review; Ottawa Vol. 5, Iss. 1, (Jan 2015): 5-14.
77. Mangus, B. (2017). It's National Cyber security Awareness Month!. [online] Kaspersky.com. Available at: https://www.kaspersky.com/blog/cybersec-awareness-month-2017/19676/ [Accessed 3 Jan. 2018].
78. McGoogan C. (2015). "Cyphinx could recruit the cyber security experts of the future (Wired UK)," Wired UK. [Online]. Available at: http://www.wired.co.uk/news/archive/2015-10/01/cyphinxcyber security - game. [Accessed: 03-Jan-2017].
79. Mckenna, S., Staheli, D. and Meyer, M. (2015). Unlocking user-centered design methods for building cyber security visualizations. 2015 IEEE Symposium on Visualization for Cyber Security (VizSec).

80. Mehta S. and Singh V. (2013). A STUDY OF AWARENESS ABOUT CYBERLAWS IN THE INDIAN SOCIETY. International Journal of Computing and Business Research (IJCBR). Volume 4 Issue 1 January 2013. ISSN (Online) : 2229-6166.
81. Metzger, M. (2015). Cyphinx: an online game to train the cyber security specialists of the future. SC Media. [online] Available at: https://www.scmagazineuk.com/cyphinx-an-online-game-to-train-the-cyber security-specialists-of-the-future/article/535195/ [Accessed 19 Jan. 2017].
82. Microsoft (2017). What is Microsoft Office 365 Business | FAQs. [online] Products.office.com. Available at: https://products.office.com/en-us/business/microsoft-office-365-frequently-asked-questions [Accessed 23 Jan. 2017].
83. Miniwatts Marketing Group (2016), "Middle East Internet Statistics, Population, Facebook and Telecommunications Reports", Internetworldstats.com, 2016. [Online]. Available at: http://www.Internetworldstats.com/stats5.htm. [Accessed: 16- Sep- 2016].
84. Mirkovic, J. and Benzel, T. (2012). Teaching Cyber security with DeterLab. IEEE Security and Privacy Magazine, 10(1), pp.73-76.
85. Mittal, S. (2016). Understanding the Human Dimension of Cyber Security. Indian Journal of Criminology and Criminalistics (ISSN 0970 – 4345), Vol .34 No. 1 Jan- June,2015, p.141-152. Available at: https://ssrn.com/abstract=2975924
86. Molnar, A. and Frias-Martinez, M. (2011). *Educamovil: Mobile educational games made easy.* Proceedings of the World Conference on Educational Multimedia, Hypermedia and Telecommunications, pp. pp.3684–3689, Chesapeake, VA: AACE.
87. Moslemzadeh Tehrani, P., Abdul Manap, N. and Taji, H. (2013). Cyber terrorism challenges: The need for a global response to a multi-jurisdictional crime. Computer Law and Security Review, 29(3), pp.207-215.
88. Nadeau, M. (2017). Future cyber security threats and challenges: Are you ready for what's coming?. CSO. Available at:

https://www.csoonline.com/article/3226392/security/future-cyber security-threats-and-challenges-are-you-ready-for-whats-coming.html [Accessed 3 Jan. 2018].

89. NATIONAL CENTER FOR MISSING and EXPLOITED CHILDREN (2017) “NSteens.”. Available at: http://www.nsteens.org/. [Accessed: 03-Jan-2017].
90. National Institute of Standards and Technology (2014). Framework for Improving Critical Infrastructure Cyber security Version 1.0. Availableat: https://www.nist.gov/sites/default/files/documents/cyberframework/cyber security -framework-021214.pdf [Accessed 7 Dec. 2017]
91. Nazri, Nadhirah and Mohamad Ali, Noor Azian and Ibrahim, Jamaludin (2015) Survey on mobile and wireless security awareness: user perspectives. International Journal of Science and Research (IJSR), 4 (1). pp. 1287-1292. ISSN 2319-7064
92. NIST, T. (2018). *Framework Documents*. [online] NIST. Available at: https://www.nist.gov/cyberframework/framework [Accessed 22 May 2018].
93. Nova Labs (2017) “Cyber security Lab | NOVA Labs | PBS.” [Online]. Available: http://www.pbs.org/wgbh/nova/labs/lab/cyber/. [Accessed: 03-Jan-2017]
94. Nyeste P. G. and Mayhorn C. B. (2010). *Training Users to Counteract Phishing.* Proceedings of the Human Factors and Ergonomics Society Annual Meeting, vol. 54, pp. 1956–1960.
95. Oblinger, D. (2006). Simulations, Games, and Learning. [ebook] Educase Learning Initiative. Available at: https://www.educause.edu/ir/library/pdf/ELI3004.pdf [Accessed 19 Jan. 2017].
96. Parliament of Australia (2010). Hackers, Fraudsters and Botnets: Tackling the Problem of Cyber Crime. [online] House Standing Committee on Communications, pp.55-60. Available at: https://www.aph.gov.au/parliamentary_Business/Committees/House_of_R

epresentatives_Committees?url=coms/cybercrime/report.htm [Accessed 19 Jan. 2017].

97. Pastor V., Díaz G., and Castro M. (2010). *State-of-the-art simulation systems for information security education, training and awareness in Education Engineering (EDUCON)*. IEEE Journals, pp. 1907–1916.
98. Pauli, D. (2016). Shamoon malware returns to again wipe Saudi-owned computers. [online] Available at: https://www.theregister.co.uk/2016/12/02/accused_iranian_disk_wiper_returns_to_destroy_saudi_orgs_agencies/ [Accessed: 03/12/2018]
99. Paullet, K. and Pinchot, J. (2014). *Mobile malware: Coming to a smartphone near you*. Issues in Information Systems, 15(2), pp. 116-123.
100. Paulsen, C., McDuffie, E., Newhouse, W. and Toth, P. (2012). NICE: Creating a Cyber security Workforce and Aware Public. IEEE Security and Privacy Magazine, 10(3), pp.76-79.
101. Perlroth, N. & Krauss, C. (2018). A Cyberattack in Saudi Arabia Had a Deadly Goal. Experts Fear Another Try. [online] Available at: https://www.nytimes.com/2018/03/15/technology/saudi-arabia-hacks-cyberattacks.html [Accessed: 03/12/2018]
102. Pinelle, D., Wong, N. and Stach, T., 2008. Heuristic evaluation for games: usability principles for video game design.. s.l., In Proceedings of the SIGCHI Conference on Human Factors in Computing Systems.
103. PricewaterhouseCoopers (2015). 2015 INFORMATION SECURITY BREACHES SURVEY. Available at: https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/432412/bis-15-302-information_security_breaches_survey_2015-full-report.pdf [Accessed 19 Jan. 2017].
104. Pusey, P. and Sadera, W. (2011). Cyberethics, Cybersafety, and Cyber security. Journal of Digital Learning in Teacher Education, 28(2), pp.82-85.

105. Reuters (2013). Saudi Arabia faces major cyber attack. Reuters. Available at: http://gulfnews.com/news/gulf/saudi-arabia/saudi-arabia-faces-major-cyber-attack-1.1184977 [Accessed 4 Jan. 2018].

106. Rowan, M. and Josh D. (2014). Privacy Incongruity: An analysis of a survey of mobile end-users. Proceedings of the International Conference on Security and Management (SAM); Athens : 1-5. Athens: The Steering Committee of The World Congress in Computer Science, Computer Engineering and Applied Computing (WorldComp).

107. Schweitzer D. and Brown W. (2009). *Using visualization to teach security.* Journal of. Computing Science. Coll., vol. 24, no. 5, pp. 143–150.

108. Schweitzer D. and Brown W. (2009). *Using visualization to teach security.* Journal of. Computing Science. Coll., vol. 24, no. 5, pp. 143–150.

109. Sercombe, A. and Papadaki, M. (2012). *Education in the'Virtual'Community: Can beating Malware Man teach users about Social Networking Security?.,* Advances in Communications, Computing, Networks and Security, 10 (1). pp. 146-150. ISBN: 978-1-84102-358-8.

110. Shackelford, S. J. Proia, A.A.Martell, B.,and Craig, A. N. (2014). Toward a Global Cyber security Standard of Care: Exploring the Implications of the 2014 NIST Cyber security Framework on Shaping Reasonable National and International Cyber security Practices. TEXAS INTERNATIONAL LAW JOURNAL Volume 50, Symposium Issue 2. Available at: http://www.tilj.org/content/journal/50/14%20SHACKELFORD%20PUB%20PROOF.pdf [Accessed 22 Dec. 2017].

111. Shamseddine, R. and Kalin, S. (2017). Saudi entertainment authority says hit by cyber attack. [online] reuters.com. Available at: https://www.reuters.com/article/us-saudi-cyber-attack/saudi-entertainment-authority-says-hit-by-cyber-attack-idUSKCN1C427R [Accessed 4 Jan. 2018].

112. Shay R., Komanduri, S., Kelley, P.G., Leon, P.G., Mazurek, M., Bauer, L., Christin, N., Cranor, L.F. (2010). *Encountering Stronger Password*

Requirements: User Attitudes and Behaviors. Symposium on Usable Privacy and Security (SOUPS) 2010, July 14–16, 2010, Redmond, WA USA.

113. Shih, Y. H., Hou, H. T. and Wu, Y. T. T. (2011). *A Review on the Concepts and Instructional Methods of Mini Digital Physics Games of PHYSICSGAMES.NET, Edutainment'11.* Proceedings of the 6th international conference on E-learning and games, edutainment technologies, LNCS, 6872, pp.517–521.
114. Singer, P. and Friedman, A. (2014). Cyber security and cyberwar. New York: Oxford University Press, pp.11-14.
115. Slusky, L. and Partow-Navid, P. (2012). Students Information Security Practices and Awareness. Journal of Information Privacy and Security, 8(4), pp.3-26.
116. Sowells, J. (2017). Cyber Security And The Challenges In 2018. Hacker Combat Community. [online] Available at: https://hackercombat.com/cyber security -challenges-2018/ [Accessed 3 Jan. 2018].
117. Statista (2015). U.S. number of smartphone apps used per day 2015 | Statistic. [online] Statista. Available at: https://www.statista.com/statistics/473831/number-of-daily-smartphone-apps-used-usa/ [Accessed 19 Jan. 2017].
118. Symantec (2016), "Attackers Target Both Large and Small Businesses". [Online]. Available at: https://www.symantec.com/content/dam/symantec/docs/infographics/istr-attackers-strike-large-business-en.pdf. [Accessed: 16- Sep- 2016].
119. Taylor B, Fingal D, Aberdeen D (2007) The War Against Spam : A report from the Front Line. In: Workshop on Machine Learning in Adversarial Environments for Computer Security (NIPS 2007), pp 1–3.
120. Teed, R. (2017) "Game-Based Learning", Games, 2017. Available at: http://serc.carleton.edu/introgeo/games/index.html. [Accessed: 24- May- 2017].

121. Teymourlouei, H. (2015). Quick Reference: Cyber Attacks Awareness and Prevention Method for Home Users. World Academy of Science, Engineering and Technology International Journal of Computer and Systems Engineering. Vol:9, No:3, 2015.
122. Tian, F., Lv, F., Wang, J., Wang, H., Luo, W., Kam, M., Setlur, V., Dai, G., and Canny, J. (2010). *Let's Play Chinese Characters: Mobile Learning Approaches via Culturally Inspired Group Games.* Proceedings of 28th International Conference on Human Factors in Computing Systems, Atlanta, 1 (4), 1603-1612.
123. Tobey, D., Pusey, P. and Burley, D. (2014). Engaging learners in cyber security careers. ACM Inroads, 5(1), pp.53-56.
124. Trybus, J. (2014). GAME-BASED LEARNING: WHAT IT IS, WHY IT WORKS, AND WHERE IT'S GOING. [online] Available at: http://www.simcoachgames.com/pdfs/WP-Trybus-Game-based-learning.pdf [Accessed 13 Oct. 2017].
125. Trybus, J. (2014). GAME-BASED LEARNING: WHAT IT IS, WHY IT WORKS, AND WHERE IT'S GOING. [online] Available at: http://www.simcoachgames.com/pdfs/WP-Trybus-Game-based-learning.pdf [Accessed 13 Oct. 2017].
126. Virvou, M., Katsionis, G., and Manos, K. (2005). Combining Software Games with Education: Evaluation of its Educational Effectiveness. Educational Technology and Society, 8 (2), 54-65.
127. WaterISAC (2015). 10 Basic Cyber security Measures Best Practices to Reduce ExploiTable Weaknesses and Attacks. [online] WaterISAC, pp.3-10. Available at: https://ics-cert.us-cert.gov/sites/default/files/documents/10_Basic_Cyber security _Measures-WaterISAC_June2015_S508C.pdf [Accessed 3 Jan. 2018].
128. Watkins, B. (2014). The Impact of Cyber Attacks on the Private Sector. [online] Briefing Paper 3/2014. Available at: http://www.amo.cz/wp-content/uploads/2015/11/amocz-BP-2014-3.pdf [Accessed 3 Jan. 2018].

129. Whitty, M., Doodson, J., Creese, S. and Hodges, D. (2015). Individual Differences in Cyber Security Behaviors: An Examination of Who Is Sharing Passwords. Cyberpsychology, Behavior, and Social Networking, 18(1), pp.3-7.
130. Williams, E., Morgan, P. and Joinson, A. (2017). Press accept to update now: Individual differences in susceptibility to malevolent interruptions. Decision Support Systems, 96, pp.119-129.
131. Woods, D. (2017). Why You Must Build Cyber security Into Your Applications. Forbes. [online] Available at: https://www.forbes.com/sites/danwoods/2017/04/20/why-you-must-build-cyber security -into-your-applications/#76373aef1768 [Accessed 3 Jan. 2018].
132. Xia, R., Machida, F. and Trivedi, K. (2014). A Markov Decision Process Approach for Optimal Data Backup Scheduling. 2014 44th Annual IEEE/IFIP International Conference on Dependable Systems and Networks.
133. Zaibon, S. and Shiratuddin, N., 2010. Heuristics evaluation strategy for mobile game-based learning.. s.l., In Wireless, Mobile and Ubiquitous Technologies in Education (WMUTE), 2010 6th IEEE International Conference on Wireless, Mobile, and Ubiquitous Technologies in Education.

Appendices

Appendix A Cyber Security, awareness and incident reporting – A Survey of Users knowledge, Attitudes and prevention

Centre for Security, Communications and Network Research (CSCAN)

The survey will be conducted with the general public across the KSA to gain an understanding of their level of awareness about cyber security, cybercrime and Incident reporting.

The questions are classified into four sections:

- ***Section A:*** Primarily focuses on demographics
- ***Section B*****:** Cyber security practices
- ***Section C:*** Cybercrime awareness
- ***Section D*****:** Incident reporting

This survey is being conducted for PhD research at University of Plymouth, United Kingdom.

Should you have any question about the study or you wish to receive a copy of the results, please contact the researcher via address or email below:

Researcher details:

Faisal Alotibi

Centre for Security, Communications and Network Research (CSCAN)

School of Computing and Mathematics
University of Plymouth, Plymouth, PL4 8AA, United Kingdom

E-mail:

faisal.alotaibi@plymouth.ac.uk

Project Supervisors:

Prof Steven Furnell

Dr Ingo Stengel

Dr Maria Papadaki.

If you have any concern regarding the way the study has been conducted, please contact the secretary of the Faculty of Science and Environment Research Ethics Committee:

Paula Simson
009, Smeaton, Drake Circus
Faculty of Science and Environment
University of Plymouth, Plymouth, PL4 8AA, United Kingdom

Phone:+44 (0)1752584503
E-mail to: paula.simson@plymouth.ac.uk

A note on privacy

This survey is anonymous.

The record kept of your survey responses does not contain any identifying information about you unless a specific question in the survey has clearly asked for this.

All answers will be treated confidentially and respondents will be anonymous during the collection, storage and publication of research material. The survey is hosted online within the Centre for Security, Communications and Network Research (CSCAN). Responses are collected online and stored in a secure database. Once the survey has been taken offline participant responses will be extracted, statistically analysed and published into a suitable academic journal. In addition these results may be used and published in a PhD thesis. Your responses will be treated as confidential at all times and data will be presented in such a way that your identity cannot be connected with specific published data.

This survey is designed for adult participation. If you are **UNDER 18 YEARS, PLEASE DO NOT ANSWER THIS SURVEY.** Anyone 18 years old or above can take part in the survey and has the right to withdraw up until the final submission of their responses.

If you click 'Next', you confirm that you have read and understood the information given, understand that your 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: Participant Demographics

1) Select your gender.

- Male
- Female

2) Select your age group (in years).

- 18-29
- 30-39
- 40-49
- 50+

3) What is your highest level of education?

- School
- Undergraduate (Diploma, BSc)
- Postgraduate (Master's, PhD)

4) How often do you use the Internet and Internet-related services? (E.g. Email, WhatsApp, News, YouTube).

- Frequently throughout the day
- Once or twice a day
- Less frequently (once a week, once month)

5) What are your Internet/ Digital devices skills level?

- Beginner/Basic (e.g. start computer and phone, go to specified web page. Use Word. Use social media).
- Intermediate (e.g. able to install and run special software, make modifications to the settings of the computer, have a good understanding of hardware and software).
- Expert (e.g. computer engineering, database administration, network engineering).

6) Of the following, which digital devices do you use regularly? Tick all that apply.

- Desktop
- Laptop

- Smart phone
- Tablet
- Other, please specify

7) What type of connectivity services do you use in your daily activities? Tick all that apply.

- ☐ Public Wi-Fi (e.g. in coffee shop)
- ☐ Private Wi-Fi (e.g. in your home)
- ☐ Mobile/cellular phone network (e.g. 3G/4G)
- ☐ Broadband (wired)
- ☐ Do not know
- ☐ Other, please specify

8) For what purposes do you use the Internet? Tick all that apply.

- ☐ Professional reasons (e.g. remote access VPNs)
- ☐ Education or information seeking (news, articles)
- ☐ Social networking
- ☐ Government services, online banking, e-commerce, etc.
- ☐ Entertainment (e.g. playing games)
- ☐ Communication (e.g. email, Skype, etc.)
- ☐ Other, please specify

Section B: Cyber Security Practices

9) **A**- What operating systems do you use on your desktop/laptop? Tick all that apply.

- ☐ Windows 8
- ☐ Windows 7
- ☐ Windows XP
- ☐ Older Windows version
- ☐ Macintosh
- ☐ Linux
- ☐ Do not know

☐ Other, please specify

B- What operating systems do you use on your smart phone/Tablet? Tick all that apply.

☐ Blackberry
☐ Symbian
☐ iOS
☐ Android
☐ Windows phone
☐ Do not know
☐ Other, please specify

10) Some of the most commonly used security tools and applications for laptops, Tablets, mobiles, etc. are given below. Select which of these you have used on your digital devices. Tick all that apply.

☐ Anti-virus
☐ Firewall
☐ Authentication (e.g. password, PIN)
☐ Encryption
☐ Software update
☐ Backup
☐ None
☐ Other, please specify

11) How secure do you feel your digital devices (e.g. computers and phones) are?

- Very secure
- Somewhat secure
- Neutral
- Somewhat insecure
- Not secure at all
- Not sure (difficult to determine)

12) Some security practices are described below. Please choose your common reaction for each practice.

Security practices	Always	Sometimes	Never
I check the legitimacy of a website before accessing it	○	○	○
I create a password that contains my personal information (e.g. last name, date of birth)	○	○	○
I am aware of the danger when clicking on banners, advertisements or pop-up screens that appear when surfing the Internet	○	○	○
I give due attention to privacy settings on my social media account(s) (e.g. Facebook)	○	○	○
Social media services protect my personal information	○	○	○
I read the terms and conditions carefully before using any website	○	○	○
I change the passwords of important accounts (such as online banking) frequently	○	○	○
I feel safe when using public Wi-Fi	○	○	○
I feel my digital devices (computer, smartphones) has no value to hackers, they do not target me	○	○	○
I regularly install software updates	○	○	○
I am careful about clicking on links in an email or social media post	○	○	○

13) What digital devices do you have Internet security on (e.g. anti-virus)?

- □ Desktop
- □ Laptop
- □ Smart phone
- □ Tablet
- □ None of the above
- □ I do not know

14) If you use Internet security (e.g. anti-virus), is this kept up to date in terms of threat filters and signatures?

- ○ Yes, I believe it is automatically updated
- ○ Yes, I manually updated
- ○ I do not know

Section C: Cybercrime Awareness

15) How do you keep yourself updated about cyber crime? Tick all that apply.

a- Online sources:	**b- Offline sources:**
☐ TV, news, radio ☐ Internet, website, email bulletins, blogs, etc. ☐ Government websites (e.g. CERT) ☐ Internet service provider ISPs ☐ Rely on automatic updates ☐ I do not feel that I keep myself updated ☐ Other, please specify ____	☐ Newspapers, magazines, Posters ☐ Professional activities: conferences, meetings, briefings, etc. ☐ Internet service provider ISPs ☐ Government or professional reports ☐ I do not feel that I keep myself updated ☐ Other, please specify. ____

16) What is your opinion of each of the following statements? Select the appropriate response for each.

Statement	Strongly agree	Agree	Neutral	Disagree	Strongly disagree
I think one should avoid disclosing personal information online	○	○	○	○	○
I feel that the risk of becoming a victim of Cybercrime has increased in the past year	○	○	○	○	○
I am concerned that my online personal information is not secure enough	○	○	○	○	○
I feel that I am well protected against cyber crime	○	○	○	○	○
I am willing to accept increased Internet surveillance from the government if it can enhance Internet security	○	○	○	○	○

I believe that the laws in effect are effective in managing the Cybercrime problem	○	○	○	○	○
I feel informed about the threat of cyber crime	○	○	○	○	○

17) There are several activities that constitute cyber crimes. How often have you experienced or been victim of the following situations? Select the appropriate response for each.

Activities	**Often**	**Occasionally**	**Never**	**Do not know**
Received phishing emails (e.g. asking for money, personal information or bank account details)	○	○	○	○
Identity theft (somebody stealing your personal data and impersonating you, e.g. tweeting under your name)	○	○	○	○
Malware (e.g. virus) infection of a device	○	○	○	○
Being unable to access online services (e.g. banking services) because of cyber attacks.	○	○	○	○

Accidentally encountering material that promotes hatred or religious extremism	○	○	○	○
Online extortion (a demand for money to avert or stop extortion, or to avert scandal)	○	○	○	○

18) Some of the most common cyber crimes are presented below. What is your opinion of each of the following statements? Select the appropriate response for each.

Statement	**Strongly agree**	**Agree**	**Neutral**	**Disagree**	**Strongly disagree**
I am concerned about identity theft (somebody stealing your personal data and impersonating you, e.g. tweeting under your name)	○	○	○	○	○
I am not concerned about accidentally encountering child pornography online	○	○	○	○	○
I am concerned about receiving phishing emails (e.g. asking for money, personal information or bank account details)	○	○	○	○	○

I am concerned about not being able to access online services (e.g. banking services) because of cyber attacks.	○	○	○	○	○
I am concerned about accidentally encountering material that promotes hatred or religious extremism	○	○	○	○	○
Other, please specify					

19) What do you feel about the threat of cyber crimes in the future?

- ○ They will become a more serious issue in the future
- ○ The threat will vanish eventually
- ○ No significant change
- ○ Do not know
- ○ Other, please specif

20) Considering each of the following parties, please rate the extent to which you believe they are responsible for raising awareness of cyber crime

Responsible	Strongly agree	Agree	Neutral	Disagree	Strongly disagree
The government	○	○	○	○	○

The media	○	○	○	○	○
Those offering online/Internet-based services (e.g. banks, online retailers, telecommunication companies, etc.)	○	○	○	○	○
User itself	○	○	○	○	○
Education system	○	○	○	○	○
Other, please specify					

21) What do you think the role of the government should be in combating cyber crimes? Please tick all that apply

- □ No role
- □ Have stricter laws and punishments for cyber crimes
- □ Work towards providing a global cyber security framework
- □ Monitor organisations misusing consumer information
- □ Make people aware of cyber crime
- □ Do not know
- □ If other, please specif

Section D: Incident Reporting

22) Have you been a victim of cyber crime? (E.g. lost data or email account, device infected with virus or spyware, stole your picture/s or digital device/s).

- Yes
- No

A- If Yes, When you had been a victim of cyber crime, did you report it?

- Yes, I did
- No, I did not

If Yes, **To whom did you report or contact? (Please check all that apply)**

- ☐ Saudi eGovernment Portal
- ☐ Saudi CERT
- ☐ Police
- ☐ Committee for the Promotion of Virtue and the Prevention of Vice
- ☐ Others

If No, **What was/were the reason/s? (Please check all that apply)**

- ☐ I did not know what the crime was
- ☐ I did not know who to write report about cyber crime
- ☐ I did not know what the impact on me will be
- ☐ I did not know how to describe or write reports about Cybercrime
- ☐ I feel it is waste of time
- ☐ I think that there is no value of reporting
- ☐ I did not trust the third party
- ☐ I fixed the problem by myself
- ☐ Not sure
- ☐ Other

B- If No, If you become a victim of Cybercrime would you like to report it?

- Yes, I would
- No, I would not

If Yes, **To whom would you report or contact? (Please check all that apply)**

- ☐ Saudi eGovernment Portal
- ☐ Saudi CERT
- ☐ Police
- ☐ Committee for the Promotion of Virtue and the Prevention of Vice
  Do not know but will ask friends for advice
- ☐ Others

If No, **What is/are the reason/s? (Please check all that apply)**

- ☐ I do not know what the crime was
- ☐ I do not know who to write report about cyber crime
- ☐ I do not know what the impact on me will be
- ☐ I do not know how to describe or write reports about Cybercrime
- ☐ I feel it is waste of time
- ☐ I think that there is no value of reporting
- ☐ I do not trust the third party
- ☐ I fixed the problem by myself
- ☐ Not sure
- ☐ Other

Appendix B: Ethical approval confirmation

RESEARCH WITH PLYMOUTH UNIVERSITY

22 April 2015

CONFIDENTIAL
Faisal Alotaibi
School of Computing, Electronics and Mathematics

Dear Faisal

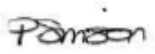
Ethical Approval Application

Thank you for submitting the ethical approval form and details concerning your project:

Enhancing cyber security to reduce cyber crime

I am pleased to inform you that this has been approved.

Kind regards



Paula Simson
Secretary to Faculty Research Ethics Committee

Cc. Prof Steven Furnell

Faculty of Science and Engineering
Plymouth University
Drake Circus
PL4 8AA

+44 (0) 1752 584 584
F +44 (0) 1752 584 540
W www.plymouth.ac.uk

Mrs Christine Mushens BA
Faculty Business Manager

Appendix C: Instructions of Password Protector Game

Data Collection Procedures
The Password Protector game is intended to help raise awareness of creating strong password. The study requires you to download and play the Password Protector game. Additionally, you are requested to take part in two short surveys – one survey before the beginning of the study period, and the other after the study period. The steps to be followed by the participants are listed below. 1. Read the consent form carefully and sign your acceptance to take part in the study. 2. Take part in the “pre-test survey” that assesses your understanding about the malware concept. 3. Download the Password Protector game from the provided link on to your android device of your choice (i.e. Tablet or smartphone) The instructions to play the game are listed below. The aim of the game is to create and remember strong passwords, which you are required to create and then re-enter from a set of available characters against a time limit. The strength of the password is rated, and creating/remembering better passwords scores more. When you enter the game first time, will start with help information and tips which is help to create stronger password and for more score. Here are the tips: 1. Use at least 8 characters

2. Use both upper and lower-case letter
3. Use more than one number
4. Use symbols

In the next screen, the game levels are shown. Select “Level 1” if you are playing the game for the first time.

In the next screen, start to create your password and selected characters by double-click/tap on the on-screen keyboard, or drag and drop characters from the keyboard to the password box.

After you have created (and remembered!) a sufficiently strong password successfully, you can move to the next levels.

The stages of this study are outlined below.

Step 1: (Pre-test survey) Password Protector

Description: This survey aims to assess your awareness of creating strong passwords prior to playing the game.

To start the survey, please visit the link (will provided later) into the web address (URL) of your browser and answer the survey.

Step 2: start Playing the Password Protector game

Description: The mobile game prototype is designed and implemented to teach adult to create secure passwords.

You are given 2 weeks to play the game. The game runs on your mobile device and the researcher will help you if needed.

Step 3: (Pro-test survey) Password Protector

Description: You are given final survey including some details about secure passwords and are required to answer questions.

You are also required to complete a survey to evaluate your subjective satisfaction of mobile game prototype interface and knowledge about password.

To take the test, please type the link (will provided later) into the web address (URL) of your browser and answer the survey.

Appendix D: Pre-test Survey: A mobile games-based approach to enhance Cyber Security awareness in Saudi Arabia.

Centre for Security, Communications and Network Research (CSCAN)

The survey will be conducted with the adult users across the KSA to gain an understanding The purpose of this questionnaire is to measure level of experiences to create strength password. The password mobile game focuses to train adult on creating awareness about best practices for creating strength password. This survey will take 3-5 minutes.

The survey aims to investigate the user experience and behavior with creating strength password , there are 2 main section organized as follow

Background/demographic - Overview of respondents'' background consisting of age, gender education background, Internet usage, Internet/devices skills

Experience with strength password - analysis of respondents' strength password experience.

This survey is being conducted for PhD research at University of Plymouth, United Kingdom.

Should you have any question about the study or you wish to receive a copy of the results, please contact the researcher via address or email below:

Researcher details:

Faisal Alotibi

Centre for Security, Communications and Network Research (CSCAN)

School of Computing, Electronics and Mathematics
University of Plymouth, Plymouth, PL4 8AA, United Kingdom

E-mail:

faisal.alotaibi@plymouth.ac.uk

Project Supervisors:

Prof. Steven Furnell

Dr Ingo Stengel

Dr Maria Papadaki.

If you have any concern regarding the way the study has been conducted, please contact the secretary of the Faculty of Science and Environment Research Ethics Committee:

Paula Simson
009, Smeaton, Drake Circus
Faculty of Science and Environment
University of Plymouth, Plymouth, PL4 8AA, United Kingdom

Phone:+44 (0)1752584503
E-mail to: paula.simson@plymouth.ac.uk

A note on privacy

This survey is anonymous.

The record kept of your survey responses does not contain any identifying information about you unless a specific question in the survey has clearly asked for this.

All answers will be treated confidentially and respondents will be anonymous during the collection, storage and publication of research material. The survey is hosted online within the Centre for Security, Communications and Network Research (CSCAN). Responses are collected online and stored in a secure database. Once the survey has been taken offline participant responses will be extracted, statistically analysed and published into a suitable academic journal. In addition these results may be used and published in a PhD thesis. Your responses will be treated as confidential at all times and data will be presented in such a way that your identity cannot be connected with specific published data.

This survey is designed for adult participation. If you are **UNDER 18 YEARS, PLEASE DO NOT ANSWER THIS SURVEY.** Anyone 18 years old or above can take part in the survey and has the right to withdraw up until the final submission of their responses.

If you click 'Next', you confirm that you have read and understood the information given, understand that your 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 : Questions for collecting Participant Demographics

1) Select your gender.

- Male
- Female

2) Select your age group (in years).

- 18-29
- 30-39
- 40-49
- 50+

3) What is your highest level of education?

- School
- Undergraduate (Diploma, BSc)
- Postgraduate (Master's, PhD)

4) How often do you use the Internet and Internet-related services? (E.g. Email, WhatsApp, News, YouTube).

- Frequently throughout the day
- Once or twice a day
- Less frequently

5) How would you rate your skill level in relation to using digital devices and the Internet?

- Beginner/Basic (e.g.I can start the computer and phone, go to specified web page. Use Word. Use social media).
- Intermediate (e.g. able to install and run special software, make modifications to the settings of the computer, have a good understanding of hardware and software).
- Expert (e.g. writing my own code, setting up networks, database administration).

Section B :Experience of creating a password

6 : What is your opinion of each of the following statements? Select the appropriate response for each.					
	Strongly agree	Agree	Neutral	Disagree	Strongly disagree
I understand the concept of password strength	○	○	○	○	○
Increasing the password length increases the strength of the password	○	○	○	○	○
Use of different character types (letters, numbers, etc) in my password increases its strength	○	○	○	○	○
I can remember passwords of more than 8 characters	○	○	○	○	○
I find password meters useful in checking if my password is strong or not	○	○	○	○	○

Q7: Try to create a Strong password:

Q8: Do you have any additional comments, questions, or concerns you would like to share?

Appendix E: Post-test Survey: A mobile games-based approach to enhance Cyber Security awareness in Saudi Arabia.

Centre for Security, Communications and Network Research (CSCAN)

Purpose:

The survey aims to gather user feedback after playing the Password Protector game. This survey will take 5-7 minutes There are 4 section's organized as follows:

- **Password awareness**: Has playing the game changed the level of awareness around password protection issues?
- **Usability aspects:** Analysis of the user experience of various usability factors
- **Learning aspects:** Analysis of the user experience of various learning factors
- **Enjoyment aspects:** Analysis of the user experience of various enjoyment factors

This survey is being conducted for PhD research at University of Plymouth, United Kingdom.

Should you have any question about the study or you wish to receive a copy of the results, please contact the researcher via address or email below:

Researcher details:

Faisal Alotibi

Centre for Security, Communications and Network Research (CSCAN)

School of Computing, Electronics and Mathematics
University of Plymouth, Plymouth, PL4 8AA, United Kingdom

E-mail:

faisal.alotaibi@plymouth.ac.uk

Project Supervisors:

Prof. Steven Furnell

Dr Ingo Stengel

Dr Maria Papadaki.

If you have any concern regarding the way the study has been conducted, please contact the secretary of the Faculty of Science and Engineering Research Ethics Committee:

Paula Simson
009, Smeaton, Drake Circus
Faculty of Science and Environment
University of Plymouth, Plymouth, PL4 8AA, United Kingdom

Phone:+44 (0)1752584503
E-mail to: paula.simson@plymouth.ac.uk

A note on privacy

This survey is anonymous. The record kept of your survey responses does not contain any identifying information about you unless a specific question in the survey has clearly asked for this.

All answers will be treated confidentially and respondents will be anonymous during the collection, storage and publication of research material. The survey is hosted online within the Centre for Security, Communications and Network Research (CSCAN). Responses are collected online and stored in a secure database. Once the survey has been taken offline participant responses will be extracted, statistically analysed and published into a suitable academic journal. In addition these results may be used and published in a PhD thesis. Your responses will be treated as confidential at all times and data will be presented in such a way that your identity cannot be connected with specific published data.

This survey is designed for adult participation. If you are **UNDER 18 YEARS, PLEASE DO NOT ANSWER THIS SURVEY.** Anyone 18 years old or above can take part in the survey and has the right to withdraw up until the final submission of their responses.

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: Experience of creating a password

Q6 : What is your opinion of each of the following statements? Select the appropriate response for each.					
	Strongly agree	Agree	Neutral	Disagree	Strongly disagree
I understand the concept of password strength	○	○	○	○	○
Increasing the password length increases the strength of the password	○	○	○	○	○
Use of different character types (letters, numbers, etc) in my password increases its strength	○	○	○	○	○
I can remember passwords of more than 8 characters	○	○	○	○	○
I find password meters useful in checking if my password is strong or not	○	○	○	○	○

Q7: Try to create a strong password:

Section B: Usability Content

Rate the usability components on a scale of 1 to 5 (1-very poor, 2-poor, 3-good, 4-very good, 5-excellent)

	Game Usability components	Rate
1	The audio-visual design is suitable for the game	
2	The screen layout is easy to understand	
3	The screen layout is visually appealing	
4	The user interface design is logical	
5	The game is easy to control	

Section C : Learning Content

Rate the contents of the game in terms of imparting knowledge on a scale of 1 to 5 (1 **Strongly Disagree, 2 Disagree, 3 Neutral, 4 Agree, 5 Strongly Agree*)***

	Learning Content components	Rate
1	The contents provided in the game are easy to learn and understand	
2	The game provides useful information	

3	The game helps to raise cyber security awareness	
4	The game content convinced me to be more cautious about cyber security	
5	The learning contents were presented in a fun and engaging manner	

Section D: enjoyability contents

Rate the fun and enjoyment aspects of the game on a scale of 1 to 5 (**where 1 is the worst and 5 is the best*****)***

	Game enjoyability components	**Rate**
1	Learning about cyber security is more interesting using the game	
2	Playing Password Protector is fun	
3	I prefer to learn more cyber security using such games	
4	Rate how enjoyable it was to learn about passwords through the game	

Q: Do you have any additional comments, questions, or concerns you would like to share?

Appendix F: Instructions of Malware Guardian game

Data Collection Procedures
The Malware Guardian game is intended to help raise awareness of malware attacks. The study requires you to download and play the Malware Guardian game. Additionally, you are requested to take part in two short surveys – one survey before the beginning of the study period, and the other after the study period. The steps to be followed by the participants are listed below. 1. Read the consent form carefully and sign your acceptance to take part in the study. 2. Take part in the “pre-test survey” that assesses your understanding about the malware concept. 3. Download the Malware Guardian game from the provided link on to your android device of your choice (i.e. Tablet or smartphone) The instructions to play the game are listed below. 1. The aim of the game is to defend your system against potentially malicious files, while allowing safe files to be downloaded. Identifying the malicious files requires the use of up-to-date anti-malware protection, and protecting against the effects of malicious files that might get through requires effective use of backup. 2. When you enter the game first time, click on “Play” option to start playing the game. 3. In the next screen, the game levels are shown. Select “Level 1” if you are playing the game for the first time.

4. In the next screen, the game displays a message on the importance of taking “backup” of the device and prompts you to click “Continue” to take backup.
5. Once the “backup” action is performed in the game, click on “Play” button to play the game.
6. On the screen, a computer device is displayed. The computer is attacked by files that could be a malware or harmless file.
7. Every time, a file appears, tap on the file to see the type of file and the associated message and then choose “destroy” action to destroy the file before it infects the computer.
8. Further, you will be prompted to update the anti-malware software. Updating the software provides “ammunition” that is required to destroy malware attacking the computer devices.
9. If the “update” action is not performed, then ammunition is lost and the computer device in the game will be destroyed.
10. After destroying the malware successfully, you can move to the next levels.

The stages of this study are outlined below.

Step 1: (Pre-test survey) Malware Guardian

- **Description:** This survey aims to assess your awareness of malware and related security issues prior to playing the game.

To start the survey, please visit the link (will provided later) into the web address (URL) of your browser and answer the survey.

Step 2: Play the Malware Guardian game

Description: You are given 2 weeks to play the game. The game runs on your Android mobile device and the researcher will help you if needed.

The researcher will stay in touch with the participants face-to-face if possible or online via skype or Email.

Step 3: (Pro-test survey) Malware Guardian

- **Description:** This survey again asks some questions relating to malware awareness, in order to assess whether or not the game has had any effect upon your related views and understanding. It also provides an opportunity to evaluate the game itself.

Please type the link (will provided later) into the web address (URL) of your browser and answer the survey.

Appendix G: Pre-test Survey: A mobile games-based approach to enhance Cyber Security awareness in Saudi Arabia.

Centre for Security, Communications and Network Research (CSCAN)

Purpose:

The purpose of this questionnaire is to measure Malware awareness. The Malware Guardian game focuses on training the computer users on the ability to identify different types of malware and then use specific anti-malware solution to destroy the malware, this survey will take 3-5 minutes.

The survey aims to investigate the user experience and behaviour with malware, there are 2 main sections organized as follow:

Background/demographic - Overview of respondents" background consisting of age, gender education background, Internet usage, Internet/devices skills

Experience with Malware and protection method - analysis of respondents' malware experience, anti-malware software, and backup

This survey is being conducted for PhD research at University of Plymouth, United Kingdom.

Should you have any question about the study or you wish to receive a copy of the results, please contact the researcher via address or email below:

Researcher details:

Faisal Alotaibi

Centre for Security, Communications and Network Research (CSCAN)

School of Computing, Electronics and Mathematics
University of Plymouth, Plymouth, PL4 8AA, United Kingdom

E-mail:

faisal.alotaibi@plymouth.ac.uk

Project Supervisors:

Prof. Steven Furnell

Dr Ingo Stengel

Dr Maria Papadaki.

If you have any concern regarding the way the study has been conducted, please contact the secretary of the Faculty of Science and Environment Research Ethics Committee:

Paula Simson
009, Smeaton, Drake Circus
Faculty of Science and Environment
University of Plymouth, Plymouth, PL4 8AA, United Kingdom

Phone:+44 (0)1752584503
E-mail to: paula.simson@plymouth.ac.uk

A note on privacy

This survey is anonymous. The record kept of your survey responses does not contain any identifying information about you unless a specific question in the survey has clearly asked for this.

All answers will be treated confidentially and respondents will be anonymous during the collection, storage and publication of research material. The survey is hosted online within the Centre for Security, Communications and Network Research (CSCAN). Responses are collected online and stored in a secure database. Once the survey has been taken offline participant responses will be extracted, statistically analysed and published into a suitable academic journal. In addition these results may be used and published in a PhD thesis. Your responses will be treated as confidential at all times and data will be presented in such a way that your identity cannot be connected with specific published data.

This survey is designed for Computer adult participation. If you are **UNDER 18 YEARS, PLEASE DO NOT ANSWER THIS SURVEY.** Anyone 18 years old or above can take part in the survey and has the right to withdraw up until the final submission of their responses.

If you click 'Next', you confirm that you have read and understood the information given, understand that your 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 : Questions for collecting Participant Demographics

1) Select your gender.

- Male
- Female

2) Select your age group (in years).

- 18-29
- 30-39
- 40-49
- 50+

3) What is your highest level of education?

- School
- Undergraduate (Diploma, BSc)
- Postgraduate (Master's, PhD)

4) How often do you use the Internet and Internet-related services? (E.g. Email, WhatsApp, News, YouTube).

- Frequently throughout the day
- Once or twice a day
- Less frequently

5) How would you rate your skill level in relation to using digital devices and the Internet?

- Beginner/Basic (e.g.I can start the computer and phone, go to specified web page. Use Word. Use social media).
- Intermediate (e.g. able to install and run special software, make modifications to the settings of the computer, have a good understanding of hardware and software).
- Expert (e.g. writing my own code, setting up networks, database administration).

Section B: Malware experiences

6: What is your opinion of each of the following statements? Select the appropriate response for each.

	Strongly agree	Agree	Neutral	Disagree	Strongly disagree
I have a good understanding of the concept of malware	o	o	o	o	o
I am aware of the different types of malware that might attack my system	○	○	○	○	○
Malware has the ability to take over my computer remotely	○	○	○	○	○
I am aware of the different effects that malware can have upon my system	○	○	○	○	○

7: What is your opinion of each of the following statements? Select the appropriate response for each.

	Strongly agree	Agree	Neutral	Disagree	Strongly disagree
I can understand why anti-malware software is so important	○	○	○	○	○
It is important to keep anti-malware program up-to-date	○	○	○	○	○

I understand the difference between manual and automated malware scanning	○	○	○	○	○

8: What is your opinion of each of the following statements? Select the appropriate response for each.

	Strongly agree	Agree	Neutral	Disagree	Strongly disagree
It is important to backup the files in my computer regularly	○	○	○	○	○
Backup are a useful safeguard to protect against malware	○	○	○	○	○

Q9: Do you have any additional comments, questions, or concerns you would like to share?

Appendix H: Post-test Survey: A mobile games-based approach to enhance Cyber Security awareness in Saudi Arabia.

Centre for Security, Communications and Network Research (CSCAN)

Purpose:

The survey aims to investigate the user experience and behavior with malware, and investigate the user acceptance of the new proposed tools from **Usability, Learning, Enjoyment** aspects, This survey will take 5-7 minutes there are 4 main section organized as follow

There are 4 section's organized as follows:

Malware awareness: Has playing the game changed the level of awareness around malware and related security issues?

Usability aspects: Analysis of the user experience of various usability factors

Learning aspects: Analysis of the user experience of various learning factors

Enjoyment aspects: Analysis of the user experience of various enjoyment factors

This survey is being conducted for PhD research at University of Plymouth, United Kingdom.

This survey is being conducted for PhD research at University of Plymouth, United Kingdom.

Should you have any question about the study or you wish to receive a copy of the results, please contact the researcher via address or email below:

Researcher details:

Faisal Alotaibi

Centre for Security, Communications and Network Research (CSCAN)

School of Computing, Electronics and Mathematics
University of Plymouth, Plymouth, PL4 8AA, United Kingdom

E-mail:

faisal.alotaibi@plymouth.ac.uk

Project Supervisors:

Prof. Steven Furnell

Dr Ingo Stengel

Dr Maria Papadaki.

If you have any concern regarding the way the study has been conducted, please contact the secretary of the Faculty of Science and Environment Research Ethics Committee:

Paula Simson
009, Smeaton, Drake Circus
Faculty of Science and Environment
University of Plymouth, Plymouth, PL4 8AA, United Kingdom

Phone:+44 (0)1752584503
E-mail to: paula.simson@plymouth.ac.uk

A note on privacy

This survey is anonymous. The record kept of your survey responses does not contain any identifying information about you unless a specific question in the survey has clearly asked for this.

All answers will be treated confidentially and respondents will be anonymous during the collection, storage and publication of research material. The survey is hosted online within the Centre for Security, Communications and Network Research (CSCAN). Responses are collected online and stored in a secure database. Once the survey has been taken offline participant responses will be extracted, statistically analysed and published into a suitable academic journal. In addition these results may be used and published in a PhD thesis. Your responses will be treated as confidential at all times and data will be presented in such a way that your identity cannot be connected with specific published data.

This survey is designed for adult participation. If you are **UNDER 18 YEARS, PLEASE DO NOT ANSWER THIS SURVEY.** Anyone use 18 years old or above can take part in the survey and has the right to withdraw up until the final submission of their responses.

If you click 'Next', you confirm that you have read and understood the information given, understand that your 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: Malware experiences

6: What is your opinion of each of the following statements? Select the appropriate response for each.					
	Strongly agree	Agree	Neutral	Disagree	Strongly disagree
I have a good understanding of the concept of malware	o	o	o	o	o
I am aware of the different types of malware that might attack my system	○	○	○	○	○
Malware has the ability to take over my computer remotely	○	○	○	○	○
I am aware of the different effects that malware can have upon my system	○	○	○	○	○

7: What is your opinion of each of the following statements? Select the appropriate response for each.

	Strongly agree	Agree	Neutral	Disagree	Strongly disagree
I can understand why anti-malware software is so important	○	○	○	○	○
It is important to keep anti-malware program up-to-date	○	○	○	○	○
I understand the difference between manual and automated malware scanning	○	○	○	○	○

8: What is your opinion of each of the following statements? Select the appropriate response for each.

	Strongly agree	Agree	Neutral	Disagree	Strongly disagree
It is important to backup the files in my computer regularly	○	○	○	○	○
Backup are a useful safeguard to protect against malware	○	○	○	○	○

Section B : Usability Content

Rate the usability components on a scale of 1 to 5 (1-very poor, 2-poor, 3-good, 4-very good, 5-excellent)

	Game Usability components	Rate
1	The audio-visual design is suitable for the game	
2	The screen layout is easy to understand	
3	The screen layout is visually appealing	
4	The user interface design is logical	
5	The game is easy to control	

Section C : Learning Content

Rate the contents of the game in terms of imparting knowledge on a scale of 1 to 5 (1* Strongly Disagree, 2 Disagree, 3 Neutral, 4 Agree, 5 Strongly Agree*)

	Learning Content components	Rate
1	The contents provided in the game are easy to learn and understand	
2	The game provides useful information	
3	The game helps to raise cyber security awareness	

4	The game content convinced me to be more cautious about cyber security	
5	The learning contents were presented in a fun and engaging manner	

Section D : enjoyability Content

Rate the fun and enjoyment aspects of the game on a scale of 1 to 5 (**where 1 is the worst and 5 is the best*****)***

	Game enjoyability components	**Rate**
1	Learning about cyber security is more interesting using the game	
2	Playing Malware Guardian is fun	
3	I prefer to learn more cyber security using such games	
4	Rate how enjoyable it was to learn about malware through the game	

Q: Do you have any additional comments, questions, or concerns you would like to share?

Appendix J: Ethical approval for both practical trials (Password Protector And Malware Guardian)

RESEARCH WITH PLYMOUTH UNIVERSITY

15 August 2017

CONFIDENTIAL
Faisal Alotaibi
School of Computing, Electronics and Mathematics

Dear Faisal

Ethical Approval Application

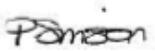
Thank you for submitting the ethical approval form and details concerning your project:

A mobile games based approach to enhance cybersecurity awareness in Saudi Arabia.

I am pleased to inform you this has been approved, however, please note the following recommendations from the committee:

- Section 4.2 is not very clear, and section 4.1 provides a minimum; the committee are also interested in the maximum to figure out impact.
- Consider providing an indication of how long the participation will involve on the front of the information section (Use a heading indicating that it is an information section)
- Consider re-structuring the documents named: **"Pre-test Survey: ...."**
  Use headings to point out at information sections, consent, etc.
  Integrate the privacy section into the body of the information section, having this as a small print notice at the end may not provide the correct message.
  Consider using a checklist of main points before consent, or an overview at the start of the information section

Kind regards



Paula Simson
Secretary to Faculty Research Ethics Committee

Cc. Prof Steve Furnell

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 Jayne Brenen
Head of Faculty Operations