Design and Evaluation of Mobile Games for Enhancing Cyber Security Awareness

F. Alotaibi[1], S. Furnell[123], I.Stengel[14], M.Papadaki[1]
[1]*Centre for Security, Communications and Network Research, University of Plymouth, Plymouth, UK,* [2]*Security Research Institute, Edith Cowan University, Perth, Western Australia,* [3]*Centre for Research in Information and Cyber Security, Nelson Mandela University, Port Elizabeth, South Africa,* [4]*Hochschule Karlsruhe, University of Applied Sciences Karlsruhe, Germany*

Abstract

The ever-increasing threats on cybersecurity have consequently increased the need for enhanced awareness about cybersecurity and its various threats among public. This paper presents the design aspects of the two mobile gaming applications: Password Protector and Malware Guardian. Further, different mobile games concept developed during the course of the study is also presented. Password Protector aimed at educating the users about the need for creating strong and complex passwords, remembering and changing them frequently. Meanwhile, Malware Guardian was aimed at educating players about different security threats, security issues, the risks associated with it and the tools to be used for preventing these attacks. The design methodology of both games is presented in this paper along with the heuristic evaluation and analysis of the developed games. The design methodology of both games is presented in this paper along with the heuristic evaluation and analysis of the developed games. 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 Password and Malware awareness.

1. Introduction

The ever-increasing threats on the security of information technology systems and in the cyber world have raised the importance of the cybersecurity awareness for both individuals and organizations. However, being aware about cybersecurity is not given enough importance and is often neglected, especially in workplaces. For any organization, it is important that the employees are aware and up-to-date with cybersecurity threats as it can potentially reduce incidents of security breaches. However, according to UK Cyber Security Breaches Survey, it was observed that only 30% of the organizations provide awareness regarding cybersecurity to their employees [1]. The research study presented aims at addressing the issue of creating cybersecurity awareness by employing gameplay methods over traditional approaches to make awareness process more engaging. As a part of study, 12 game concepts were shortlisted, and a brief overview of these games is presented, along with the design concepts of two selected games, Password Protector and Malware Guardian, and also evaluates the games using a heuristic evaluation approach. guidelines include complete descriptions of the fonts, spacing, and related information for producing your proceedings manuscripts. Please follow them.

2. Background Study

It is important that the users are trained to be cybersecurity 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 behavioral change among users. 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, behavioral change, and cybersecurity training [2].

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 [3]. A good game takes 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 penalized for the wrong ones. This process encourages the player to use the correct tools and thereby empowers them with right knowledge that can 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 [4]. In the literature, there are fewer studies that have applied games-based learning approach for cybersecurity awareness. The study presented is aimed at addressing this research gap.

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 [8]. 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. [9].

Game based learning is a process which uses exercises (competitive/scoring) to motivate users in learning according to specific learning objectives [10]. 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 [11]. Many research studies were conducted and still being conducted to analyze 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 don't 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. [12]. 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 [13].

3. Ideas for Cyber Security Awareness Games

The A few research studies have shown that games can be used to impact security awareness [5,6,7]. 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 cybersecurity 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.

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 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. 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.

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 the type of data being collected from their devices. The aim of this game is to make the users aware about the importance of data privacy and the type of information being collected from their devices from the Internet. The idea behind the game is to represent the data transfer between the user device and the Internet in the form of network packets. 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 needs to be allowed to the Internet.

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.

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 email. 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 if it to the right if it is a safe email.

3.5. Cybersecurity Helpdesk

This is a puzzle game, where the player would be enacting the role of a cybersecurity support worker. On the game interface, is a computer network with different types of computing devices connected to the cyber space. The computing devices might be facing a cybersecurity 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 cybersecurity 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.

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 an 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 presented with malware and viruses which they need to destroy before it reaches the computer. 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. 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.

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. 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.

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 cybersecurity incident. This is a puzzle-based game that aims at educating players about cybersecurity incident reporting practices. In the game the user will be posed with a cybersecurity 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 cybersecurity incident. There will be a time restriction on the game of 30 seconds within which the user needs to decide the right option.

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.

3.10. Encryption

In this game, the user learns the importance of encrypting the files using 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.

The remaining other two games are Password game and Malware game, which were selected for the design and development. These two games are selected for implementation because they form a part of most of the applications over the Internet. For example, password is a common security aspect which can be related with most of the applications; whether it is social media applications, emails or any other customized applications over the Internet. Similarly, malware/virus/worms etc. are major security problems that all the Internet users are facing with. So, based on the larger scope for security concerns, and to create maximum security related awareness these two games are selected which have wider reach. The design aspects evaluation of these two games are discussed in detail in the next section.

4. Games Design

4.1. Password Protector

4.1.1. Intended Learning. The game aims at training the users to create complex, and strong passwords. An important and a basic measure for cybersecurity is having safe and secure passwords, and changing them frequently. This game would train the users 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.

4.1.2. Concept. 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. The game allows the players to practice strong password creation in a competitive context. The players are provided with a 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 password 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.

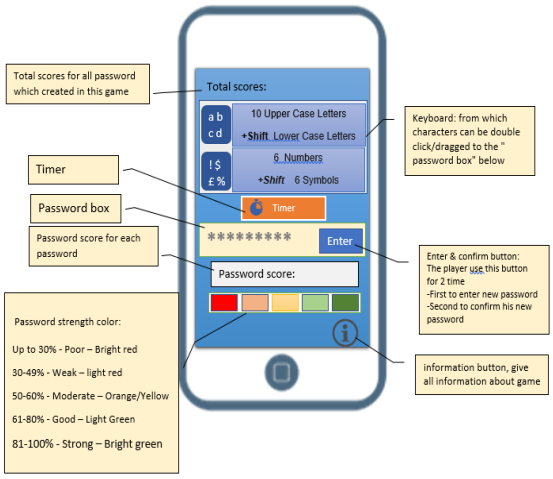

Figure 1. Password game Features

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 option is provided in the game. The user can achieve high scores in creating and remembering the password in short time duration.

The lesser the time is, the higher the score would be. There are currently seven levels proposed for the game, where the difficulty level increases as the game progresses to the next levels. A prototype of the game is presented in Figure 2.

Figure 2. Password Game Prototype

The scoring technique is based on the complexity of the password created. The password strength factors are calculated as per the guidelines of CSCAN [14]. 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 center 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 (~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/)

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

4.2. Malware Guardian

4.2.1. Intended Learning. This game aims at training the players with skills to understand and identify malicious software and creates awareness about the importance of using up-to-date anti-malware protection systems and taking backups as a safety measure. In the game, the players have the task of defending their system by roleplaying as a anti-malware package that scans file as it approaches a computer device. The player blocks the files that are malicious before it reaches the computer device. The game includes different types of malware such as viruses, trojans, spyware, ransomware that can infect the computer devices in different ways. Only clean and uninfected files must reach the computer device in the game and the player is rewarded/penalized based on the number of malware reaches the device. The player tasks is also parallelly combined with the task of updating the malware software and taking regular backups of the device.

4.2.2 Concept. 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 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 back-up 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 to destroy the new threats.

Figure 3. Malware Game Prototype

The score is calculated depending on the number of bugs destroy by the players. For example, if the player destroys all the five bugs, the score would be 50, if he destroys 4, it scores 40, and so on. However, the time can be fixed to create more sporting spirit among the players. 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 malware issues fixed, the player gets the score, and ends the game. The prototype model of the game is shown in the Figure 3.

5. Evaluation Methodology

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 design, usability, 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 [15, 16, 17]. 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.

5.1. Study Setting & Participants

The study was conducted using an online link for the survey, and the participants included the general adult Internet users from the Kingdom of Saudi Arabia (KSA). All participants were selected based on their interest. Two survey links are created separately for Password Protector and Malware Guardian. Potential participants were approached through email, WhatsApp, and other social media platforms. After the interested participants gave their consent to take part, they were sent a message with the purpose of study along with the survey links (Pre and Post) and download link. 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.

5.2. Sampling

The survey links for both games along with the download links were sent to the different people using email groups and social media. The study was also promoted using social media platforms such as Twitter and Telegram. A total sample of 50 was achieved for each game who undertook both pre and post-study surveys.

5.3. 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 questions were designed based on a review of the literature on games-based learning and are aimed at identifying the participants experience with the game and how impactful the games are in creating awareness about cybersecurity. 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 Password Protector includes the same questions as same questions as the pre-study, plus 14 additional questions focusing on the aspects of awareness (1), usability (5), learning content (4), and fun & 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. Again, the post-study questionnaire included the same questions as the pre-study, plus the 14 additional questions to assess participant feedback.

The questionnaires were translated to Arabic language for better understanding among the Saudi participants.

6. Results

6.1. Password Protector Survey Results

The majority of the participants (60%) in the study fall under the age group of 18-29. About 28% of the total participants come under the age group of 30-39, 10% under 40-49, and only 2% or one participant with age above 50 years participated in the study. A significant increase in the awareness levels about the password strength and the importance of password

security was observed from the results, which are presented in Figure 4.

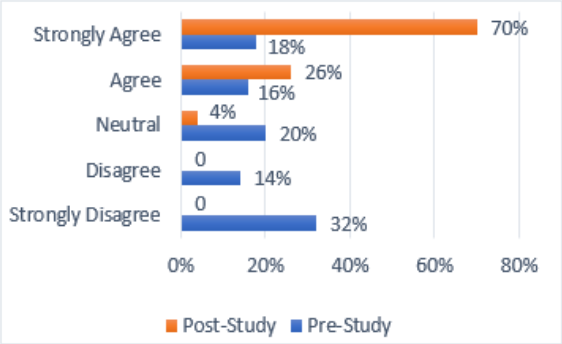

Figure 4. Responses for 'I understand the concept of Password Strength'

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. Table 1 below presents the means and standard deviations of the password strength before and after playing the games, which reflect a significant improvement in the password strength.

Table 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

The results are evaluated using paired sample t test at 0.05 confidence intervals. The t test compares the difference between the two means and explains if they are different from each other. The t-score reflects the difference between results within the same group at two different time periods. The t value was found to be -7.28, and p value was found to be 0.00001, which is less than 0.05. The results thus have shown that there is a significant improvement among the participants in creating strong passwords after playing the Password Protector game.

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 ($t = -24.753$, $p = 0.000$).

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. The experience of creating a password significantly differ (-30.707, $p < 0.05$) between pre-test and post-test. Due to the means of the pre-test and post-test xperience 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 study from 1.49 ± 0.051 to 18.60 ± 5.819 ($p < 0.05$); an improvement of 17.101 ± 5.541.

By using heuristic evaluation, it was observed that the Game usability (-30.872, $p < 0.05$), learning content (39.01, $p < 0.05$) and ability to enjoy (-28.863, $p < 0.05$) 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.

Usability Results: 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.

Learnability Results: 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 cybersecurity awareness, and convincing players to become cautious about cybersecurity. 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.

Enjoyability Results: 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 which include learning about cybersecurity, 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. More than 78% of the participants rated very good and excellent for all the aspects about fun and enjoyability in the game.

6.2. Malware Guardian Survey Results

Majority of the participants (58%) in the study fall under the age group of 18-29. About 34% of the total participants come under the age group of 30-39, 8%

under 40-49, and there are no participants with age above 50 years participated in the study. Majority of the 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, which can be noticed from Figure 5.

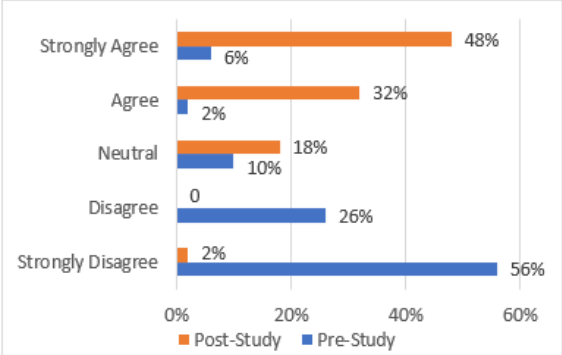

Figure 5. Responses for 'I have a good understanding about Malwares'

At the pre-test stage the only significant difference in awareness was observed in the backup ($F = 5.772$, $p < 0.05$). Understanding malware ($F = 2.175$, $p > 0.05$) and anti-malware program ($F = .214$, $p > 0.05$) were not significantly differed across the two age groups.

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) = .850, $p = .002$. And the effect size was large ($\eta^2=0.15$). According to the two-way MANOVA, Malware experience differed across age groups and tests. 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.

By using heuristic evaluation, it was observed that the Game usability (-33.337, $p < 0.05$), learning content (-37.750, $p < 0.05$) and ability to enjoy (--32.958, $p < 0.05$) 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 con+65012clude that there is a statistically significant decrease in usability, learning content and enjoyability after age 30.

Usability Results: The usability aspects of Malware 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 game. The results have shown greater satisfaction levels of the participants in relation to the usability features of the malware game.

Learnability Results: 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 understandability through Malware 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 game.

Enjoyability Results: While there are very few responses for poor and very poor options concerning the fun and enjoyment features of the Malware 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 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 game, which include learning about cyber-security, fun playing the game, preference of learning more using similar games, and the enjoyability.

7. Discussion

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. 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 17.101 ± 5.541. 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 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. Considering the overall results for the game, it can be stated that it has significantly improved the awareness of the participants, and its usability, learning, fun and enjoyability features are liked by majority of them.

The pre and post survey results of Malware Guardian proved to be similar to those of Password Protector. 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 back-up 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.

Additionally, significant changes were observed in post-study analysis of Malware Guardian in three main areas including understanding the concept of malware; understanding the anti-malware programs; and understanding the importance of back-ups among the participants, with all the observations achieved p-value (<0.05) and t-values proving the results to be significant. Further analysis of 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 heuristics evaluation of Malware Guardian revealed similar results compared to Password Protector. Participants aged under 30 had better experiences in usability, learning content and enjoyability aspects compared to those aged above 30. Comparing and analysing the overall survey results of Malware Guardian, it can be stated that the game has proved to be successful in creating awareness, and its usability, learning, fun and enjoyability features are again liked by the majority of players.

8. Conclusions

Awareness programs are important to address the challenges posed by rapidly changing technological systems. The paper presents design aspects of the two mobile games being developed to spread awareness on cybersecurity. The games developed in this study incorporate two important aspects of cybersecurity: strong password creation and protection against malware. Both Password Protector and Malware Guardian games are designed effectively using effective interactive features to enhance the usability.

This study also 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, back-ups 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 games can be more engaging with younger participants. The study has highlighted few key points in the analysis which can be used as the focus points for further extending the research or future research works.

7. References

[1] Klahr, R., Shah, J.N, Sheriffs, P., Rossington, T., Pestell, G., Button, M. and Wang, V., (2017). Cyber Security Breaches Survey 2017, Main report, April 2017, Department for Culture, Media and Sport, London, UK.

[2] Hendrix, M., Al-Sherbaz, A. & Victoria, B., (2016). Game based cyber security training: are serious games suitable for cyber security training? International Journal of Serious Games, 3(1), pp. 53-61.

[3] Boyle, S., (2011). An Introduction to Games-based learning, s.l.: UCD Dublin.

[4] Trybus, J., (2014). Game-Based Learning: What it is, Why it Works, and Where it's Going, s.l.: New Media Institute.

[5] Denning T., Lerner A., Shostack A., and Kohno T., "Control-Alt-Hack: the design and evaluation of a card game for computer security awareness and education," in Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security, pp. 915–928, 2013.

[6] Gondree M., Peterson Z. N., and Denning T., "Security through play," Secur. Priv. IEEE, vol. 11, no. 3, pp. 64–67, 2013.

[7] Nyeste P. G. and Mayhorn C. B., "Training Users to Counteract Phishing," in Proceedings of the Human Factors and Ergonomics Society Annual Meeting, vol. 54, pp. 1956–1960, 2010.

[8] Boyle, S., (2011). An Introduction to Games-based learning, s.l.: UCD Dublin.

[9] Trybus, J., (2014). Game-Based Learning: What it is, Why it Works, and Where it's Going, s.l.: New Media Institute.

[10] Teed, R. "Game-Based Learning", Games, (2017). [Online]. Available: http://serc.carleton.edu/introgeo/ games/index.html. [Accessed: 24- May- 2017].

[11] Oblinger, D., (2006). "Simulations, games, and learning," Educause Learning Initiative.

[12] Ke, F., (2008). "A case study of computer gaming for math: Engaged learning from gameplay?," Computers & Education, vol. 51, pp. 1609-1620.

[13] Virvou, M., et al., "Combining software games with education: Evaluation of its educational effectiveness," Educational Technology & Society, vol. 8, pp. 54-65, 2005.

[14] CSCAN, (2017). "Rate your Password", Centre for Security, Communications and Network Research, University of Plymouth, Available: https://www.cscan.org /passwordstrength/. Last accessed 15th Oct 2017.

[15] Korhonen, H. & 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.

[16] Pinelle, D., Wong, N. & 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.

[17] Zaibon, S. & 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.

