The Effectiveness of Online Gaming as part of a Security Awareness Program

WA Labuschagne[1], MM Eloff[2]
[1] Council for Scientific and Industrial Research (CSIR), Pretoria, South Africa
[2] Institute for Corporate Citizenship, University of South Africa (UNISA), Pretoria, South Africa
WLabuschagne@csir.co.za
Eloffmm@unisa.ac.za

Abstract:
Using cyberspace to conduct business and personal duties has become ubiquitous to an interconnected society. The use of information technology has provided humanity with a platform to evolve and contribute to the advancement of society. However duality also exists within the realm of cyberspace as shown by the expanding threats originating from cyber criminals who uses the information superhighway for nefarious purposes.

Companies usually invest large amounts of money in the implementation of hardware and software controls to deter and prevent attacks on assets within these establishments. For example firewalls and anti-virus software are updated as threats evolve. In spite of these controls the weakest link in this security chain is still the human element whose actions can be considered as erratic and unpredictable thus posing a threat to the security of the organization.

Security awareness programs aim to equip users of cyberspace with the necessary knowledge to identify and mitigate threats emanating from these platforms, including the Internet.

Numerous security awareness frameworks exist which prescribes the required steps to design and implement an efficient and effective security awareness program. An understanding of the different steps is required to develop and customize such a program for a specific environment. Furthermore different methods which include training, newsletters and websites are used to deliver the security awareness content to the participants. The nature of these methods could be ineffective and be considered mundane and strenuous to the participants who do not always have the technical background in information technology, which, in turn could threaten the success of the implemented program. Therefore a proficient solution should be considered to attract and captivate a diverse group of employees when doing security awareness training. Moreover the effectiveness of these programs should be measured with the application of metrics defined within security awareness programs.

This paper discusses the implementation and findings of a security awareness program. The aim of the security awareness program was to determine the effectiveness of using online gaming as an information security knowledge delivery method to enhance the efficacy of the participant's awareness to identify and mitigate threats encountered within cyberspace. Subsequently the paper proposes improvements to the design of the security awareness program used during the study.

Keywords: Security awareness, online gaming, effectiveness, education, metrics

1. Introduction

The Internet has penetrated all aspects of daily living within society. The speed in which technology has become part of normal day to day activities created a sense of panic as users attempt to understand on how to use these new technologies. The issue of using these technologies not the only concern as cyber criminals have turned to these to prey on unsuspecting users. The arsenal available to criminals is vast and very effective against users who unknowingly would engage in actions to their own detriment as they are not aware of the threats and how to mitigate these (Kim et al. 2011). An example is the use of social networking sites. Facebook has been widely adopted and used by users to keep in contact with friends. But the Facebook platform has also been used by criminals with great success as shown by the Koobface malware which infected 400,000 and 800,000 computers in 2010 (Villeneuve, Deibert & Rohozinski 2010). In another example Labuschagne demonstrated how social media sites could also be used to profile users based on comments and posts (Labuschagne, Eloff & Veerasamy 2012). In addition users have to learn about implementing security features on a computer to protect them from network threats, for example, using a firewall. Users without the technical skills, struggle to adopt these security tools for several reasons including the user's technology adoption intention (Kumar, Mohan & Holowczak 2008). The use of a security awareness program equips computer users with knowledge to mitigate the threats that could be encountered on these platforms.

Many institutions have realized the impact of this and have started implementing awareness programs. Broadband Internet within schools in Taiwan achieved a 100% penetration in 2009. As a proactive measure by the Taiwan Ministry of Education, a security awareness program was launched to equip teachers with the necessary knowledge, whom in turn would transfer this knowledge to the scholars (Chou & Peng 2011). Computer security is defined as securing the platform from external threats and having peace of mind that the computer system is secured (Landwehr 2001). Security awareness would entail equipping users with knowledge to identify and mitigate external threats. In another way, it is defined as being exposed to knowledge about information security related content. This newly acquired knowledge would then in turn change future behaviour. Many companies implements security awareness programs to prepare their employees for the threats originating from the digital cyber world. Several frameworks exists which provide guidance in designing, developing and deploying security awareness programs. The European Union Agency for Network and Information Security (ENISA), the SANS Security Awareness Roadmap and the National Institute of Standards and Technology (NIST) framework were some of the existing frameworks that were analyzed to determine a solution for the security awareness program used in this study.

This paper discusses the implementation of a security awareness program to determine the effectiveness of online gaming as part of such a program. The first section of the paper provides a background on the different perspectives of security awareness programs; this is followed by a discussion of the security awareness program implemented at the University of Venda in South Africa. The analysis and findings are described next and the paper concludes with recommendations to Information Security Managers who plan to deploy a security awareness program.

2. Security Awareness Perspectives

Security awareness programs can be designed and developed using existing frameworks. However many programs exist and the best suited framework should be selected to achieve the goals of increased security in the given domain. The ENISA framework is comprehensive and follows sequential phases which include individual steps to achieve the goal; however each phase must be completed first before continuing with the next phase. The first phase of the ENISA consists of 14 steps which includes numerous of meetings to determine the needs and identifying the goals to address the needs, selecting and recruiting a team and obtaining a budget. The second phase consists of 5 steps to execute and manage the awareness program. The last phase consists of 7 steps to evaluate and adjust the awareness program. Many of these steps require input and approval from stakeholder which potentially could increase the time to deliver the awareness program (ENISA 2010).

The SANS Security Awareness Roadmap provides an easy to interpret flow of objectives to be taken in order to implement an awareness program. This roadmap starts at no awareness program, then commences by developing an awareness program that is compliance and security metrics focussed but also promotes awareness and change resulting in long term sustainment. It provides a guide to what each objective entails and what the deliverable of each objective is. However the guide does not prescribe actions, hence additional research might be required by a novice who wants to implement a security awareness program (SANS 2010).

The NIST Awareness Framework provides enough detail to a novice to implement a security awareness program and also has been used in other studies related to security awareness programs. The NIST framework consists of four phases (Wilson & Hash 2003). The first phase entailed designing the awareness program by conducting a needs analysis. The participants of the study were students from the University of Venda. They used this security awareness program to enhance their skills as part of a community program to train people within rural areas on end user security. Another need was to determine what the current security awareness levels of the students were whom attended the awareness program. The second phase required the development of the program which included the material used during the execution of the program. The content had to address topics specific to threats end users might encounter within the cyberspace domain. The security awareness program was implemented in the third phase. This entailed identify methods to effectively deliver the material to the participants of the awareness program. The framework implementation concludes with evaluation and feedback after the program was competed.

Several studies have shown the effectiveness of security awareness programs. Eminagaoglu, Ucar and Eren (2009) implemented as security awareness program which focused on password usage of 2900 employees at a Turkish company. Three password audits were conducted over a period of a year to measure the effectiveness of the program. The results indicated a significant decrease in the use of weak passwords. Dodge, Carver and Ferguson (2007) conducted a security awareness study on phishing attacks in the United States of America. They determined that the awareness levels increased over a two year period. They developed a system that delivered phishing attacks to students and measured how many fell prey to the attack. The results showed a decrease in successful attacks as the users become more aware of the threat. Another security awareness program was implemented at an international gold mining company which had offices in 11 countries that focussed on policies, passwords, email and Internet use, mobile devises and incident reporting (Kruger & Kearney 2006). The effectiveness of the study was measured by using multiple-choice questions provided to the participants, resulting as an indicator of awareness levels. The study also recommended that security awareness tools should consist of a broad set of questions covering the topics, using a practical system and it should be automated. These recommendations were considered during the design and development of the online game used within this study. A study conducted on the ever changing information security domain highlights the importance of the continual delivery of security awareness programs as a mechanism to equip computer users with knowledge to deal with cyber threats (Dlamini, Eloff & Eloff 2009). In other words, security awareness programs should not be a once off event as threats evolve with the rapid change in technology. This is supported by Rezgui and Marks who explored factors that effects security awareness (Rezgui & Marks 2008). They found that working environments does play a role and that iterated training should be regular to be effective.

Security awareness content is delivered using various methods including, but not limited to, posters, classroom-style training, websites and newsletters. Subsequently the effectiveness of security awareness programs also needs to be measured as this mechanism could improve future security awareness programs. A study conducted by Khan (2011) on the effectiveness of the different security awareness methods listed, group discussions and educational presentations are the most effective. Other methods, such as email messaging, newsletters, video games, computer-based training (CBT) and posters were not as effective when looking at knowledge gained, attitude to change, subjective norms, change in behaviour and a component of intention. However, video games have been used in security training as they draw the attention of the users and allow the users to implement knowledge acquired within a given scenario (Cone et al. 2007).

Most end users access services on the Internet using a web browser. The majority of users either access their email, social networking site accounts or visiting web sites. Subsequently types of attacks were associated with each vector also known as a vulnerability. The content of the security awareness program were designed to address each of the potential threats. The identification of the topics resulted from the development an attack tree by the authors to determine the different vectors that could be used with malicious intent against unsuspecting end users. The graphical representations of the different attack vectors are depicted in

Figure 1.

The security awareness program discussed in this paper covered the following topics which subsumes the potential threats identified by the attack tree: Web Browsers, Passwords, Social Networking Sites, Cyber Bullying, Malware and Phishing.

The threats listed by the authors align with the threat landscape described by Veerasamy and Taute (2009) who conducted research in identifying what attack strategies and techniques were used against national, commercial, governmental and individual entities. The next section describes the implementation of the security awareness program.

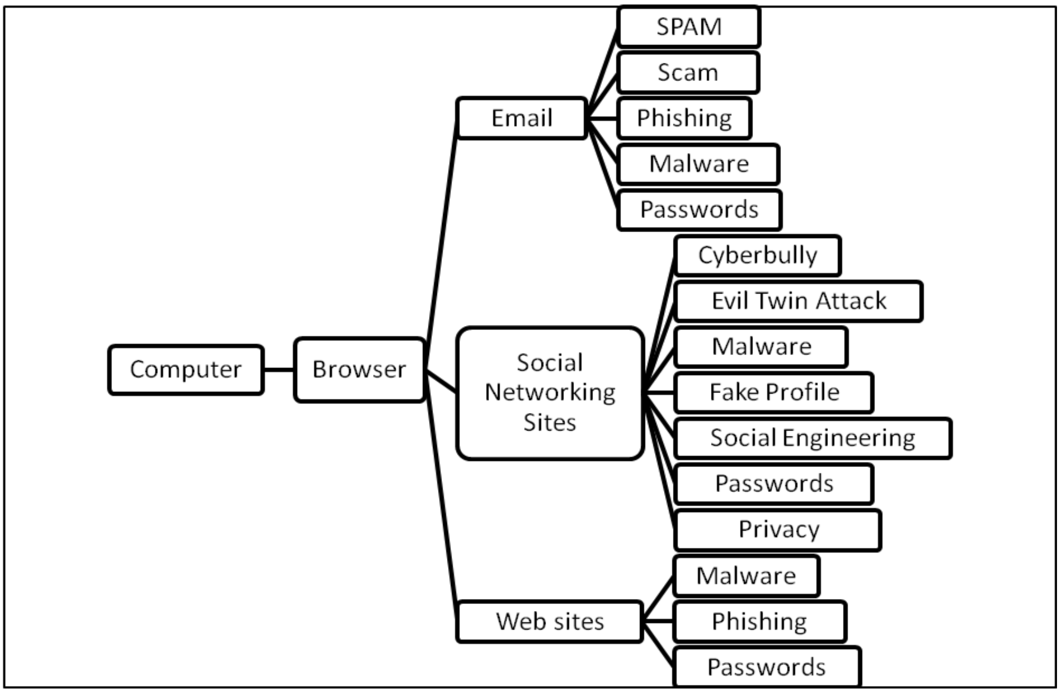

Figure 1: End User Attack Tree

3. Method

The participants were from 3rd year Computer Science class at the University of Venda, Thohoyandou, South Africa, but also formed part of rural development plan to educate people from the area about the different security threats encountered within the digital realm. A class of 40 participants attended the security awareness program. All participants were in the same venue for the day session. The security awareness program was initiated with the first survey (Pre Assessment) which also resulted in determining the awareness level baseline of the participants. This was followed by a training session which covered security topics identified during the analysis. The training sessions did not exceed 15 minutes per topic as it was a precautionary measure against mental fatigue (Wilson & Korn 2007). A second survey (Post Assessment 1) followed the completion of the training session. The objective of the second survey was to determine if the training session had an impact on the overall security awareness levels of the group. The program continued with the participants playing a social networking game online. The game was designed and developed with gamification concepts in an attempt to improve the retention of the content from the topics discussed during the training session. Some of the design concepts included but was not limited to a leaderboard indicating who has attained the most points, a progressbar to provide a graphical feedback on how far the user was in completing the game and a timeline to provide all users with a view of other events that occurred within the game. A prize was handed over to the winner of the online game and the security awareness program was concluded with the final survey (Post Assessment 2). The objective of the last assessment was to identify if the online game had an effect on the awareness levels of the participants.

Data was collected during the completing of the surveys as well as playing the online game. The surveys were accessed online by the participants and consisted of seven sections with five questions per section which totalled to 35 questions per survey. Each survey was designed to address the same objective across the different surveys for example, to determine if the participant understood the concept of weak passwords. Access to the surveys where controlled with a unique token number and was individually issued to each participant.

The online game was hosted within Facebook and the objective required from the users was to acquire points by answering security awareness related questions which correlated with the topics used during the awareness program. Random events occurred within the game which could deduct points from the user's accumulated points. An example of such events was a virus infection or hard drive failure. Users could prevent loosing points by obtaining an item which, once in possession, would counteract the event, for example, the virus infection would be negated if the user has an anti-virus item. Users could buy items by using points accumulated hence losing some points in order to prevent a substantial loss of points when an event occur.

4. Findings

All the survey data was analyzed for each session and the results are depicted in **Figure 2**. Each item in the survey had a correct answer. Each participant's survey results were programmatically calculated to determine what topics each participant understood and what individual topics needs to be revised. This was seen as the awareness level of the individual. The group's awareness level was determined by averaging all the results of the group for each survey.

The first assessment which is used as the baseline shows the groups awareness levels at about 21 correct answers out of a possible 35. The participants then attended the training session which after the second assessment resulted in about the same number of correct answers as before the training session. Next the group participated in playing the online game that focused on the security awareness topics. The results of the third assessment after playing the game, show a considerable decline in correct answers. It was expected that the number of correct answers should have increased which would support the notion that playing the online game should increase the retention of the knowledge on the security awareness topics. Astoundingly the opposite happened and the awareness levels of the group decreased.

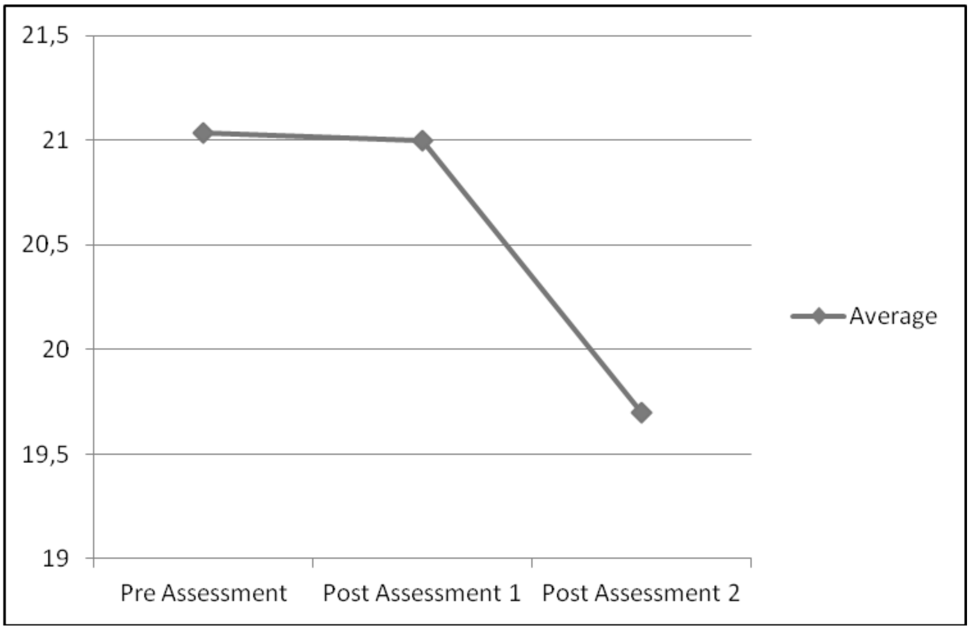

Figure 2:Session Averages

Next the online game data was analysed to determine if the results of the assessments are accurate in showing the negative effect of the online game on the group awareness levels. **Figure 3** shows the number of responses received during the playing of the game. Noticeable is the increase in responses as the deadline approached for the game play, which is mainly attributed by the prize which was handed to the participant with the most points.

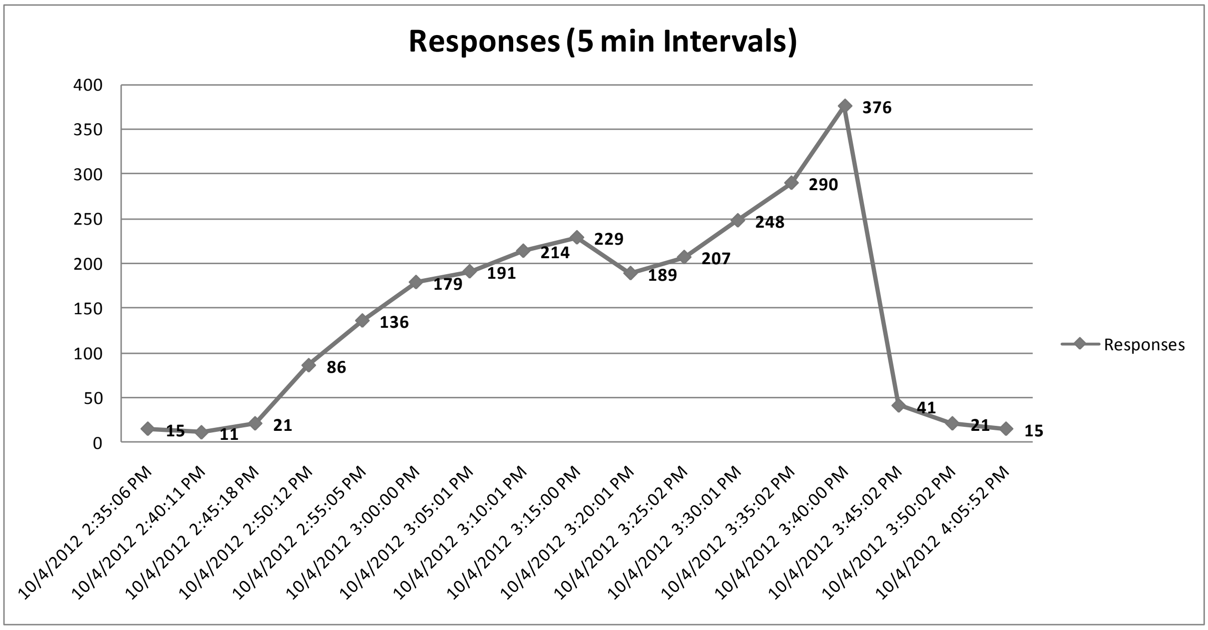

Figure 3:Average Response Time

The responses were classified to indicate how many were correct and incorrect (as depicted in **Figure 4**). Surprisingly the number of correct answers increased as the number of responses increased. This finding shows the participants knowledge on the awareness topics increased with time. Hence if the participants did not learn during the game play then the number of correct answers should have decreased and the number of incorrect answers should have increased. This could be due to the spacing effect as the recall of knowledge will decrease as time elapses. But the more the participants are exposed to the topic the longer they tend to remember it (De la Rouviere 2012).

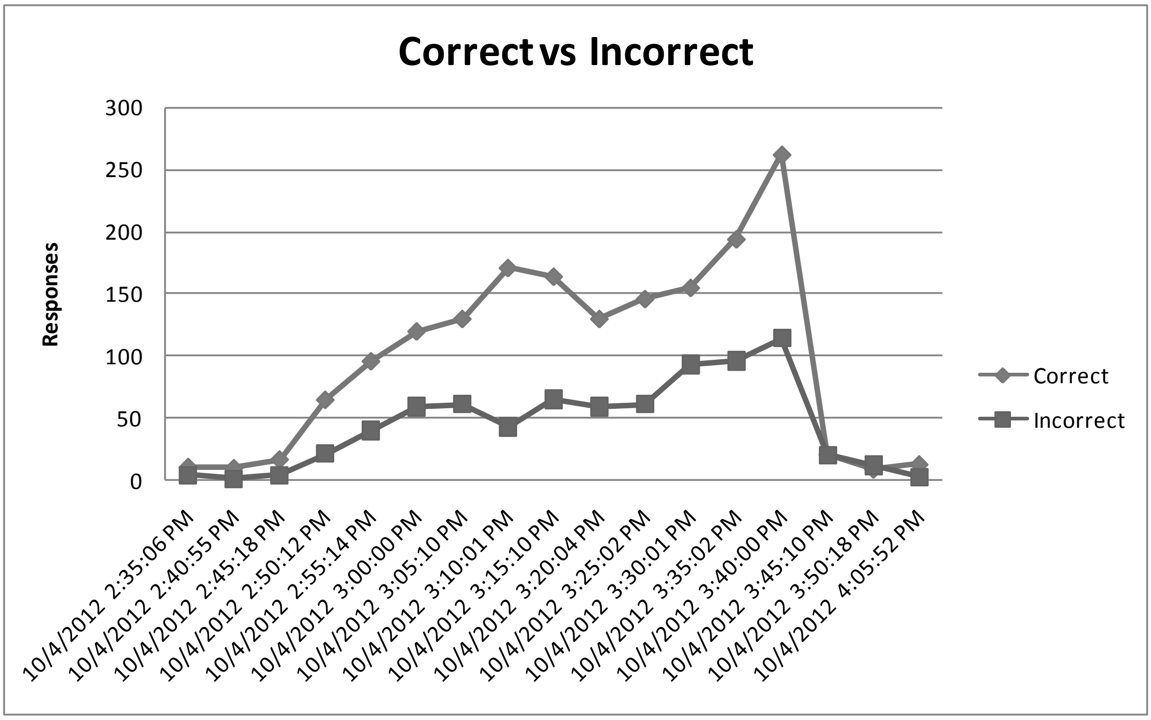

Figure 4:Response Classification

One of the metrics captured by the online game was the time it took for participants to read the question and then answer with the response. As the participants were in the same venue, the network latency affected all in the group the same way, therefore the response time calculations are consistent. An interesting observation shows that correct answers took a shorter time to answer than incorrect answers, even when more responses were submitted by the participants (See **Figure 5**). This also supports the notion that knowledge increased while playing the online game. Participants who did not know the answer had to consider the different options thus increasing the time to answer the questions. Participants, who had the knowledge, instinctively answered the questions quicker, hence a faster response time.

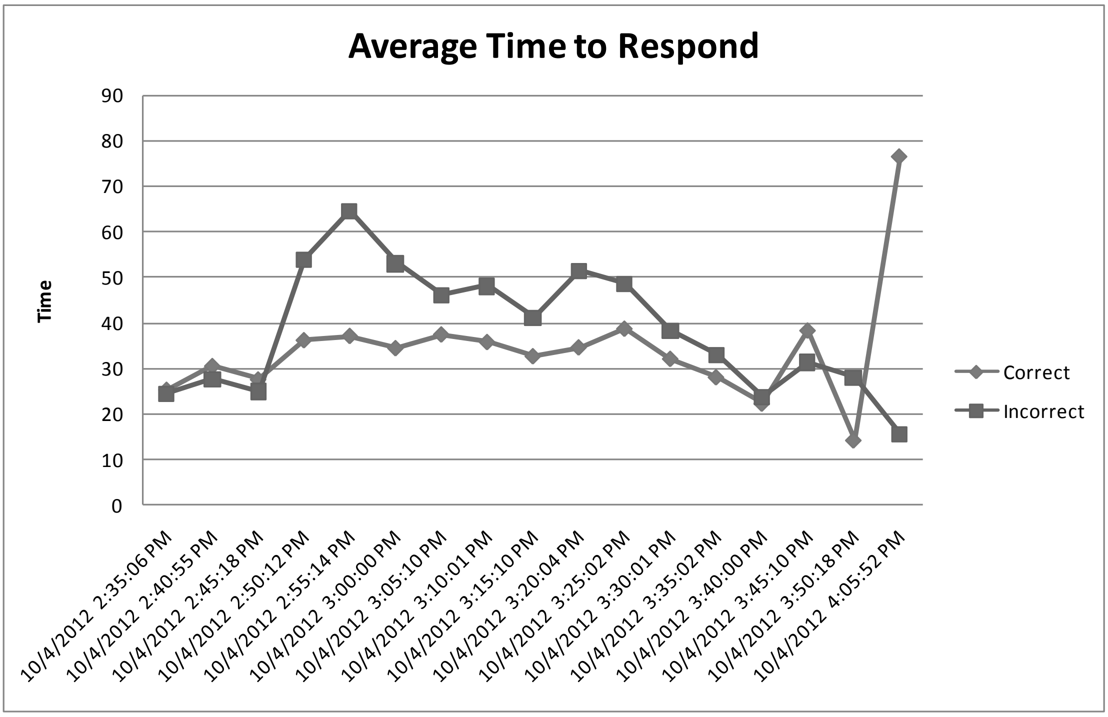

Figure 5: Average Response Time

Next the different topics answered in the online game were compared against the results from the second assessment (Post Assessment 1) and the last assessment (Post Assessment 2). The findings are depicted in **Figure 6**. The online game results show that all the topics except for Phishing and SPAM/Scam outperformed the individual topic results in the other assessments (Post Assessment 1 and 2). Also, if the online game had a positive effect on the awareness levels then the results of the last assessment (Post Assessment 2) should have improved against the results of the second assessment (Post Assessment 1). This was the finding except for Phishing, SPAM/Scam and malware however this is inconclusive in proving the positive effects of online gaming within this study however as discussed earlier the online game did indicate an increase in knowledge.

Alternatively the effect of the extrinsic motivation should be considered. The participants were competing for a prize as an incentive to partake in the study which was given after the completion of the online game. This would imply that the motivation for the students to partake in the study declined once the prize was handed over to the winner of the online game hence negatively affecting the results of the last assessment. This finding is aligned with results by Deci who examined the effect of extrinsic rewards on intrinsic motivation (Deci 1971). Subsequently the effects of the online game cannot be inferred due to the skewed results recorded during the last assessment.

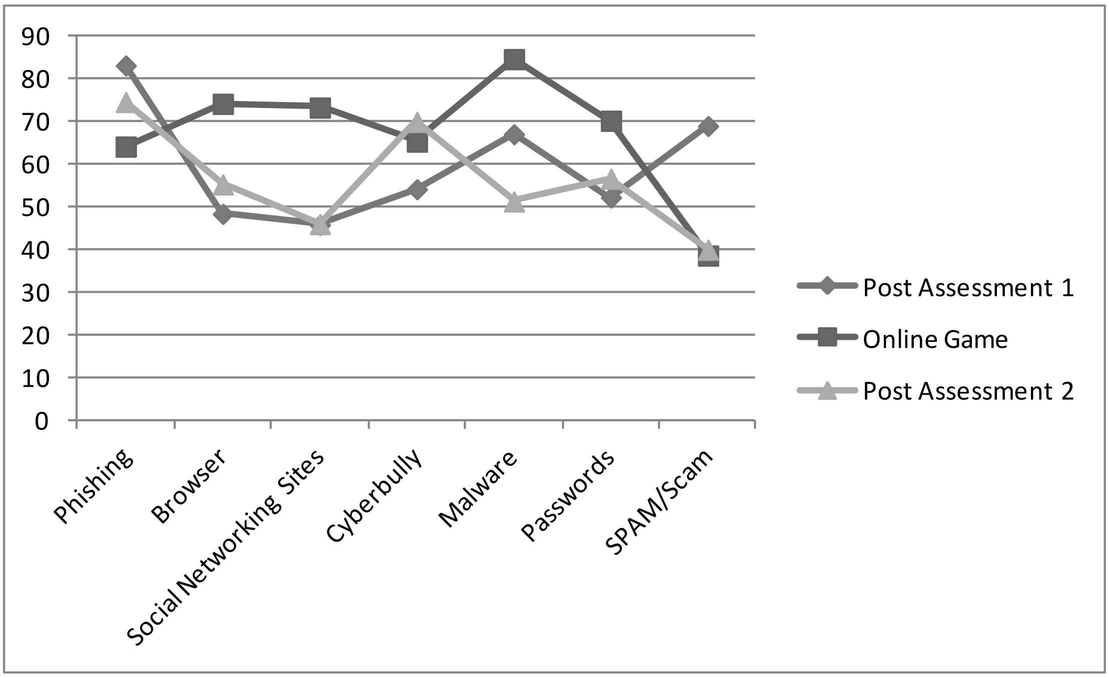

Figure 6: Comparing Online Game with Assessments

5. Conclusion

Technology has become part of everyday living and society has embraced it as these digital platforms, which include mobile devices and the Internet, improves living conditions. For example many errands can be completed by merely logging into an Internet connected devise and accessing services for example paying bills without leaving the comfort of their home. The duality of technology has become apparent as cyber criminals have seized the opportunity to use these platforms for nefarious purposes. Many users do not have the knowledge to identify these threats and mitigate it before harm is done. Security awareness programs are aimed at users who frequently use these digital platforms and to equip them with the appropriate knowledge to mitigate threats encountered within the cyberspace domain. Due to the nature of the computer domain, many users are not interested in the technical aspects as it is deemed complex and not interesting enough to engage the attention of the end user who is not technically inclined. This is detrimental to security awareness programs. These programs are delivered using various methods which include posters, training, presentations and websites. Games have been widely used to teach users about various topics as it is deemed fun. The use of games also provides a good indication if the user can implement new acquired knowledge within an environment. The effectiveness of games within security awareness programs was pursued in this study. The participant's security awareness levels were measured by using questionnaires that focussed on the different topics identified for the awareness program. The desired outcome of having an increase in the group awareness levels after the completion of the game play was not achieved. An investigation revealed that extrinsic rewards could have affected the intrinsic motivation which subsequently caused the participants to lose interest after game session. This subsequently meant the last questionnaire results which were critical in the study were affected. Thus it is the opinion of the authors that the final assessment (questionnaire) skews the results and cannot conclusively demonstrate that the gaming session can improve the security awareness levels of the participants. The study should be conducted again in future and only hand over the reward after the completion of the full program. However, analysis of the gaming session provided numerous findings that indicate learning has occurred. Participants substantially increased the number of responses as the session concluded, noticeably the correct responses increased as well. If the participants did not learn during the gaming session, then the incorrect responses would have increased. Another finding was the time for correct responses was shorter and consistent than incorrect responses which took longer. These findings provide feedback on improving future security awareness programs.

6. References

Chou, C. & Peng, H. 2011, "Promoting awareness of Internet safety in Taiwan in-service teacher education: A ten-year experience", The Internet and Higher Education, vol. 14, no. 1, pp. 44-53.

Cone, B.D., Irvine, C.E., Thompson, M.F. & Nguyen, T.D. 2007, "A video game for cyber security training and awareness", Computers & Security, vol. 26, no. 1, pp. 63-72.

De la Rouviere, N. 2012, 30 Jan 2012-last update, How To: Learn Better by Learning Less. [Homepage of MIH Media Lab], [Online]. Available: http://ml.sun.ac.za/2012/01/30/how-to-learn-better-by-learning-less/ [2013, 09/23].

Deci, E.L. 1971, "Effects of externally mediated rewards on intrinsic motivation.", Journal of personality and social psychology, vol. 18, no. 1, pp. 105.

Dlamini, M.T., Eloff, J.H.P. & Eloff, M.M. 2009, "Information security: The moving target", Computers & Security, vol. 28, no. 3–4, pp. 189-198.

Dodge, R.C. 2007, "Phishing for user security awareness", Computers & Security, vol. 26, no. 1, pp. 73-80.

Eminagaoglu, M., UÃ§ar, E. & Eren, S. 2009, "The positive outcomes of information security awareness training in companies-A case study", Information Security Technical Report, vol. 14, no. 4, pp. 223-229.

ENISA 2010, The new users' guide: How to raise information security awareness., European Network and Information Security Agency (ENISA).

Khan, B., Alghathbar, K.S., Nabi, S.I. & Khan, M.K. 2011, "Effectiveness of information security awareness methods based on psychological theories", African Journal of Business Management, vol. 5, no. 26, pp. 10862-10868.

Kim, W., Jeong, O., Kim, C. & So, J. 2011, "The dark side of the Internet: Attacks, costs and responses", Information Systems, vol. 36, no. 3, pp. 675-705.

Kruger, H.A. & Kearney, W.D. 2006, "A prototype for assessing information security awareness", Computers & Security, vol. 25, no. 4, pp. 289-296.

Kumar, N., Mohan, K. & Holowczak, R. 2008, "Locking the door but leaving the computer vulnerable: Factors inhibiting home users' adoption of software firewalls", Decision Support Systems, vol. 46, no. 1, pp. 254-264.

Labuschagne, W.A., Eloff, M.M. & Veerasamy, N. 2012, "The dark side of Web 2.0", IFIP Advances in Information and Communication Technology, vol. 386/2012, no. ICT Critical Infrastructure and Society, pp. 237-249.

Landwehr, C.E. 2001, "Computer security", International Journal of Information Security, vol. 1, no. 1, pp. 3-13.

Rezgui, Y. & Marks, A. 2008, "Information security awareness in higher education: An exploratory study", Computers & Security, vol. 27, no. 7-8, pp. 241-253.

SANS 2010, Security Awareness Roadmap, SANS Institute.

Veerasamy, N. & Taute, B. 2009, "Introduction to emerging threats and vulnerabilities to create user awareness", Information Security South Africa (ISSA), Johannesburg, South Africa.

Villeneuve, N., Deibert, R. & Rohozinski, R. 2010, Koobface: Inside a crimeware network, Munk School of Global Affairs.

Wilson, K. & Korn, J.H. 2007, "Attention during lectures: Beyond ten minutes", Teaching of Psychology, vol. 34, no. 2, pp. 85-89.

Wilson, M. & Hash, J. 2003, Building an Information Technology Security Awareness and Training Program, National Institute of Standards and Technology, Gaithersburg.