SOCIAL ENGINEERING AWARENESS GAME (SEAG): AN EMPIRICAL EVALUATION OF USING GAME TOWARDS IMPROVING INFORMATION SECURITY AWARENESS

Abdus-Samad Temitope Olanrewaju and Nur Haryani Zakaria

Universiti Utara Malaysia, Malaysia, samad.olanrewaju@gmail.com, haryani@uum.edu.my

ABSTRACT. The sharp rise of social engineering attacks in recent years poses serious threats to technology consumers. This is due to the degree of damage that can be done through social engineering. This paper seeks to elaborate on the use of a Social Engineering Awareness Game (SEAG) to improve the rate of awareness of social engineering. This game was tailored towards the needs of technology consumers that are intended to make use of it by ensuring that not only it is knowledgeable but also attractive and fun. In this paper we highlighted the objectives of this study and how it was done. A control laboratory experiment involving participants randomly assigned to either the experimental group or control group (using paper-based) to evaluate the outcome. The impact that the game had on the participants was recorded with an average of 71% improvement in their knowledge and awareness of social engineering, this made them to find the game beneficial and informative. The major drawback of the game is it needs to be more user-friendly and centered. We conclude by showing the need for more research to be put in place pertaining to the aspect of using games in the educational field especially in the network security field that has more threats growing rapidly.

Keywords: social engineering, information security awareness, educational games

INTRODUCTION

In a world of high human interaction both physically and electronically which has led to an increase in social relations, it is noticed that it is easier to con users to divulge personal secrets that could compromise the security of large networks to personal networks or social accounts. One of the most important issues in network security and equally amongst the oldest is the aspect of social engineering which ranges from insider threats to un-intentional insider threats.

Social engineering can be defined as an approach of gaining sensitive information from people which they are not likely to disclose under normal conditions through conviction and deception (Huber, Kowalski, Nohlberg, & Tjoa, 2009; Mataracioglu, 2010). It is efficient and can be carried out on large organizations because it is done on humans which is the weakest link in a network (Huber et al., 2009). According to recent studies, the rate of social engineering has been on the rise with its impact on the unsuspecting victims and firms (Deschatres, 2014; Krombholz, Hobel, Huber, & Weippl, 2013; Micro, 2014) that can lead to accounts and sensitive data to be compromised. This can be attributed to the low rate of awareness amongst

the populace towards the threat posed by social engineering (Karakasiliotis, Furnell, & Papadaki, 2006; Tolga Mataracioglu & Ozkan, 2011) and thus more awareness is required. The main objective of this study is to compare the effectiveness of the prototype-based approach as oppose to the traditional paper-based approach in improving the awareness of social engineering.

This study covers twelve basic terminologies in social engineering which are top challenges to both seasoned network administrators to end users because they all depend on the user behavior. The basic and most effective countermeasure against social engineering attacks is sensitization of users through awareness (Tolga Mataracioglu & Ozkan, 2011) which can be done using educative games.

RELATED WORK

Nowadays, games are widely becoming a popular medium to teach instructional concepts in areas like programming (Coelho, Kato, Xavier, & Gonçalves, 2011). Recent studies shows that education and training in computer security is often ordinary and uninteresting for both users and managers (Ryan, Stewart, & Verleger, 2013). Usually security games are obtainable from organizations to educate and train network security professionals and using it as a means of testing the security skills of hired professionals or to-be hired staffs (Ariyapperuma & Minhas, 2005).

Using games to teach has been of wide use especially in the network security and computer programming (Ryan et al., 2013). One such example is the *control-alt-hack* deployed a network game using cards. The game which is a multi-player card game aims at teaching the players issues related to network security especially that arises from hacking. This was done to improve the awareness that is on prioritization of computer security by making them understand and aware of the basic concepts of the different types of attack that a hacker might deploy and different technologies that is under the risk of being compromised (Denning, Lerner, Shostack, & Kohno, 2013).

Similarly, *Microsoft Elevation of Privilege* (EOP) is a card game that has more functionality and is more streamlined to network administrators in contrast to *control-alt-hack* that is meant for everybody. This game is aimed to increase awareness and equally support the available threat modelling that is in the computer networking industry. The attacks threats being implemented includes repudiation, Denial of service (DOS), tampering etc. (Microsoft, 2014).

Network nightmares is another type of networking game which was designed to enlighten the users about security threats that arises from hackers and how they attack computer nodes (Ryan et al., 2013). In their study, they implemented the game using the popular angry birds interface. The players are the hackers and they are assigned to look for vulnerabilities in the network with the possibility of a lot of nodes been exposed at a particular time.

Anti-Phishing Phil is an online game aimed at increasing the awareness of its users against phishing. The game which was designed in stages helps the user to understand all the basic details about phishing such as how to spot and evade a phishing attack. It was developed by the researchers at Carnegie Mellon University. The game which is an online game has much reachability and had been widely played (CMU Laboratory, 2008).

The use of academic games has equally been used in schools too. Papastergiou (2009) evaluated the effectiveness of a computer game in learning computer memory concepts taught in schools in comparison to a group of student that were not exposed to the game where they showed that game based learning improve student motivation and curricular knowledge in schools academic subject.

PROTOTYPE DEVELOPMENT

In this study, a prototype game was developed known as the "SEAG" (Social Engineering Awareness Games) which aims at exposing the players to basic concepts of social engineering with the ultimate goal to improve awareness. It was designed using Construct2 which is an open source game development software. The game consists of several levels. The levels were deemed necessary due to the need to keep the users glued to the game throughout and to monitor their improvement.

The first level starts with quiz like asking questions on the basics of social engineering. At this stage, players were introduced to the concepts of social engineering. Next, the second level is the memory match game which was adopted from Construct2 website (Kittiewan, 2012). At this stage, there was a card deck consisting of twenty-four cards, twelve social engineering terms and their respective pictures are reshuffled throughout the game whereby the players are to match the correct pictures respectively according to the correct definition. This game works in a way that the player opens up two cards at a time and compare. If the image corresponds to the definition, the cards leave the deck; otherwise the cards are re-covered and the players have to reselect. This level is more challenging whereby it intends to test the players of their mental alertness and ability to link pictures with definitions. This is necessary so as to give the players a live image of how the attacks are being carried out.

The third level then proceeds to mimic real life applications of the lessons learnt throughout the game. It uses real life scenarios and request players to fill in the answer by analyzing the scenario pertaining to threats and attacks of social engineering event. It is intended to test the player's ability to detect social engineering attacks which in turn would help the players from falling prey to the attacks.

METHODOLOGY

This study involved series of control laboratory experiment based on voluntary participation. The experiment sessions were advertised among the students in the university and once they agreed to participate, they were assigned randomly to either the experimental group or to the control group. This is following the design of experiment using the *between subject-design*. Below are the detailed steps each participants were required to do:

(1) Complete and sign a consent form to indicate willingness to participate in the study.
(2) Given a set of instructions on tasks they required to complete.
(3) All participants are supplied with a background reading materials for them to go through before proceeding to play the game. They are given approximately 15 minutes for this task. The idea is to give all participants some basic idea on social engineering and how it can happen. This is also to control the situation whereby the possibility of any participants who have *zero* knowledge on the subject matter can be minimized.
(4) Then they start to play the game. Those in the experimental group will have to go through the levels one by one and have time restrictions as well as requires certain numbers of scores to proceed to the following levels. In contrast, those in the control group were assigned a quiz-like booklet to complete. Those in the control group are instructed to complete each section[1] before proceeding to the next section so as to mimic the flow

[1] *Each session in the quiz-like booklet for the control group are considered equal to the levels in the prototype group.*

of the prototype game. However, the participants in the control group were not restricted by time or by any scores to proceed to the next section.

(5) Finally, before the session ends, a set of questionnaires was given to both groups to complete.

RESULTS

A total of twenty participants were successfully recruited for the control laboratory experiments with eleven male and nine female. The participants were aged between 18 – 40 years old. The participants are equally divided in terms of their IT background knowledge. Approximately 30% of the participants claimed to have some idea on social engineering because they had an experience of been a victim before. The following Table 1 displays the results of both paper-based and prototype-based (prototype) arranged according to the levels:

Table 1. Mean Score (Standard Deviation) for Paper-Based Versus Prototype-Based

Levels	Mean Score (Standard Deviation)	Percentage Score (%)
Paper Based		
Quiz section (Score/30)*	18.10 (6.70)	60.33
Memory match section (Score/12)	9.20 (2.44)	76.67
Real world scenario section (Score/100)	5.30 (1.89)	5.30
Prototype Based		
Quiz section (Score/120)	107.00 (23.12)	89.17
Memory match section (Score/100)	71.70 (9.06)	71.70
Real world scenario section (Score/100)	61.00 (16.63)	61.00

**Note: The maximum score varies between levels and approaches.*

Based on Table 1 above, for the first level (quiz section), the participants in the prototype-based group were found to perform better compared to the participants from the paper-based group. In contrast, for the next level (memory match section), participants from the paper based were found to perform better than prototype-based with an average score of 77% and 72% respectively. Meanwhile, in the third level (real world scenario section), the average score of the paper based was 5.3 with a SD of 1.89 while the prototype-based has 61 with a SD of 16.63. In the third level, 80% of the participants from the prototype-based were found to obtain score above 60% unlike the paper based with only half of them scoring above the threshold. The next section will further discuss on the analysis followed by detail discussion.

ANALYSIS & DISCUSSION

The prototype-based participant did better in the quiz section than the paper based due to the reason that six of the participants had been a victim of social engineering. Also on this note, the quiz level gave room for more questions to be answered if it can be done in the required timeframe and thus they get exposed to the questions more than the paper based which most of the participants did not acknowledge initially having fell prey of social engineering which might reflect their attitude and keenness towards the performance initially. In addition, they had no time limit which gave them the liberty of being less conscious unlike the in the game- based, seeing the time ticking off will increase individual consciousness in an attempt to reach the required threshold level.

In the memory match level, the paper-based group did slightly better than the prototype-based because their's was much more direct which involved drawing a line between matched cards unlike the prototype-based where the participants needs to turn over the shuffled card deck which is closed after two unmatched cards are opened. This process of opening the cards gave the prototype-based participants a better mental picture of the attack because they spent

a considerably much more time in this stage while opening different cards over and over again in search for the match. This further solidified the knowledge gained from the background reading and quiz section which they took. This has in fact, influenced the prototype-based performance whereby the participants performed better in the real world scenario compared to the paper-based.

On the overall, the knowledge of IT was not considered as a determinant factor in respect to the performance of the participants as the scores were almost even all round. This shows the awareness and knowledge of social engineering is still very low regardless of the field or specialization of the user. All the users were regular users of Internet and with their high rate of Internet exposure, their awareness about social engineering was still very low with only 30% of the participant acknowledging the fact that they have once being a victim while most of other participants have been victims without realizing it. This was known through the observational and interaction had with the participants. This was also reflected in the response given by the participants, whereby among the twelve social engineering terms discussed, on average, participants confessed on having knowledge about three terms only. Only one participant admitted had played an educative game before. This indicates low rate of game usage as a means to pass knowledge among students. This is a gap this study aims to fill in respect to social engineering

Prior to the participant's involvement in the game, they were asked to evaluate their knowledge on social engineering. The participant responded that the game approach was indeed beneficial to them in raising awareness with an average of 71% increment compared to before they were exposed to the game approach. In comparison with the traditional approach (i.e. paper-based) most participants agreed that they found the prototype-based beneficial and has impacted them more significantly than the paper-based. Most of the participants also agreed that the prototype-based would serve as a medium to increase the awareness of social engineering. In comparison between the two approaches, one significant response from the participants in the paper-based group was in the number of questions given in each section. Although, as a matter of fact, the same number of questions was retained for the two approaches, the participants in the prototype-based group did not raise any issue. This could indicate that the interactive aspect in the prototype-based has managed to attend the participants' attention and not to make them feel bored while playing the game which at the same time gaining knowledge about social engineering. This is one important finding that should be further manipulated particularly in educating users on difficult subject like social engineering or technical topics like information or network security.

CONCLUSION & FUTURE WORK

This study which was carried out as a step in improving the awareness on social engineering was done using a game prototype called SEAG. This was done in an effort in raising awareness in a fun and relatively easy way so as to make the users have a live experience of how the attacks are being carried out. It gave the participants an opportunity to be acquainted with twelve terms in a space of three levels. A paper based group was equally used to see the efficiency and comparison with the game based group where it was noticed that the game based did better in the quiz section because of time motivation and in the real world scenario due to a better mental picture gotten in the memory match section as a result of several cards being opened. It was equally noted that IT knowledge did not reflect much since most scores were almost even all through. SEAG is not a replacement for social engineering awareness through other channels and network security class lessons; however, it aims to serve as a complement to other efforts that was pre-used so as to enhance deep understanding. Although the number of participants involved in the study was small, the results received from the respondents were very promising. With larger population, more interesting results can be ex-

pected and until then the result of this study should be interpreted within its own context. Nevertheless, in conclusion, the results necessitates the need for more games to be deployed in the IT field especially network security learning because of its ever changing and challenging landscape. This is absolutely needed so as to make the teaching of key concepts and practical application easy and fun to learn.

REFERENCES

Ariyapperuma, S., & Minhas, A. (2005). Internet Security Games as a Pedagogic Tool for Teaching Network Security, 1–5.

CMU Laboratory. (2008). Anti Phishing Phil. Retrieved April 2, 2015, from http://www.ucl.ac.uk/cert/antiphishing/

Coelho, A., Kato, E., Xavier, J., & Gonçalves, R. (2011). Serious game for introductory programming. In *Lecture Notes in Computer Science* (Vol. 6944, pp. 61–71). doi:10.1007/978-3-642-23834-5_6

Denning, T., Lerner, A., Shostack, A., & Kohno, T. (2013). Control-Alt-Hack: the design and evaluation of a card game for computer security awareness and education. *CCS '13: Proceedings of the 2013 ACM SIGSAC Conference on Computer & Communications Security*, 915–928. doi:10.1145/2508859.2516753

Deschatres, S. (2014). Social Engineering: Attacking the Weakest Link in the Security Chain. Retrieved April 2, 2015, from http://www.symantec.com/connect/blogs/social-engineering-attacking-weakest-link-security-chain

Huber, M., Kowalski, S., Nohlberg, M., & Tjoa, S. (2009). Towards Automating Social Engineering Using Social Networking Sites. *CSE '09: Proceedings of the 12th IEEE International Conference on Computational Science and Engineering*, *3*, 117–124. doi:10.1109/CSE.2009.205

Karakasiliotis, A., Furnell, S., & Papadaki, M. (2006). Assessing end-user awareness of social engineering and phishing. *Information Warfare and Security Conference*, 60.

Kittiewan. (2012). Creating a Memory Match Game. Retrieved March 15, 2015, from https://www.scirra.com/tutorials/280/creating-a-memory-match-game/

Krombholz, K., Hobel, H., Huber, M., & Weippl, E. (2013). Social Engineering Attacks on the Knowledge Worker Categories and Subject Descriptors. *Security Information and Networks*, 28–35. doi:10.1145/2523514.2523596

Mataracioglu, T. (2010). Analysis of Social Engineering Attacks in Turkey. *Journal of National Research Institute of Electronics and Cryptology (UEKAE)*, *2*(4).

Mataracioglu, T., & Ozkan, S. (2011). User Awareness Measurement Through Social Engineering, 1–7. Retrieved from http://arxiv.org/abs/1108.2149

Micro, T. (2014). Social engineering attacks on the rise, part 1: eBay breach. Retrieved April 2, 2015, from http://blog.trendmicro.com/social-engineering-attacks-rise-part-1-ebay-breach/

Microsoft. (2014). Elevation of Privilege (EoP) Card Game. Retrieved April 2, 2015, from http://www.microsoft.com/en-us/sdl/adopt/eop.aspx

Papastergiou, M. (2009). Computers & Education Digital Game-Based Learning in high school Computer Science education : Impact on educational effectiveness and student motivation. *Computers & Education*, *52*(1), 1–12. doi:10.1016/j.compedu.2008.06.004

Ryan, W., Stewart, J., & Verleger, D. (2013). Network Nightmares : Using Games to Teach Networks and Security. *Fdg 2013*.