Edith Cowan University
Research Online

Australian Information Security Management Conference

Security Research Institute Conferences

2009

Playing Safe: A Prototype Game For Raising Awareness of Social Engineering

Michael Newbould
University of Plymouth

Stephen Furnell
Edith Cowan University

Originally published in the Proceedings of the 7th Australian Information Security Management Conference, Perth, Western Australia, 1st to 3rd December 2009
This Conference Proceeding is posted at Research Online.
http://ro.ecu.edu.au/ism/4

Playing Safe: A Prototype Game For Raising Awareness of Social Engineering

Michael Newbould[1] & Stephen Furnell[1,2]
[1] Centre for Security, Communications and Network Research
University of Plymouth, UK

[2] School of Computer and Security Science
Edith Cowan University, Western Australia

Abstract

Social engineering is now a major threat to users and systems in the online context, and it is therefore vital to educate potential victims in order to reduce their susceptibility to the related attacks. However, as with other aspects of security education, this firstly requires a means of getting the user's attention. This paper presents details of an awareness-raising game that was developed in order to educate users in a more interactive way. A board game approach, combining reference material with themed multiple-choice questions, was implemented as an initial prototype, and evaluated with 21 users. The results suggested that the approach helped to increase players' awareness of social engineering, with nobody scoring under 55% whilst playing the game, and 86% feeling they had improved their knowledge of the subjects involved.

Keywords

Security Awareness, Social Engineering, Phishing, Advance Fee Fraud, Spam.

INTRODUCTION

User awareness represents a significant challenge in the security domain, with the human factor ultimately being the element that is exploited in a variety of attack scenarios. This is most clearly illustrated with attacks focusing around social engineering techniques, in which the users' naivety, gullibility and simple good nature can often be leveraged to the benefit of an attacker. However, raising awareness of security issues in a manner that engages with users is not easy, and it is certainly true that simply providing advice and instruction in traditional forms can be less than effective. As an example, a survey of over 1,280 business users revealed that while 97% agreed that every individual in their organisation is responsible for security, a significantly lower proportion (72%) had read and understood their organisation's security policy (SAI Global, 2008). In many cases, the problems may relate to the manner in which security is promoted to users, with other survey evidence suggesting that the most common approaches are via handbooks, face-to-face training and induction programmes, with techniques such as computer-based training being used in a small minority of cases (BERR, 2008).

Recognising both the threat to users and potential benefits of addressing the audience in a different way, this paper summarises a project that was undertaken to improve user awareness of social engineering attacks in online contexts. In order to provide a more engaging means of interaction, the decision was taken to present related materials in the context of a game, in which users could both explore and be tested on topics of relevance (thus hopefully providing a more interesting way to learn).

The sections that follow begin by presenting background information on the social engineering threats targeted by the game, followed by a description of the game prototype itself, including the reasoning behind the decisions that were made, as well as explaining the defined requirements. Finally, discussion is devoted to the user evaluation of the prototype, and the results that were obtained from this.

ONLINE SOCIAL ENGINEERING THREATS

Social engineering in an IT context is based upon targeting the individual rather than directly attacking their system, and refers to techniques that exploit human weaknesses and manipulate people into breaking normal security procedures (ENISA, 2008). The attacker uses psychology to trick the user, convincing them to perform atypical actions or to divulge confidential information. Whilst social engineering did not originate from IT, the frequency of related attacks occurring in this context has increased significantly, especially with techniques such as phishing. As a consequence, a veritable goldmine has opened up for attackers, with millions of potential victims a single mouse click away.

There are a number of different types of social engineering attacks, and the remainder of this section will give an overview of these exploits, including looking at how they have evolved with new technology.
The most frequent type of social engineering attack is phishing (APWG, 2009). This typically involves an email from the attacker imitating an organisation such as banks in an attempt to trick the user into following a link and entering their

details. According to research carried out by Gartner (2007), between August 2006 and August 2007 3.6 million users lost money to phishing scams in the US, resulting in a combined loss of $3.2million, which indicates the scale of the problem.

Certain spam can be classed as a social engineering attacks as many offer enticements such as free images, a movie or friendship, with the aim of provoking intrigue and interest from the user. However, the related links or attachments often lead to malware, with the consequence that the user may be tricked into inviting damage to their system and data.

Another form of social engineering attack is advance fee fraud (also known as the 419 scam), in which an attacker usually exploits human greed or sympathy. When exploiting greed, the attacker suggests to the victim that they will get a large amount of money for sending a small amount of money first, usually explained as a release fee, bribe or legal fee. Other forms of this attack can consist of the attacker imitating a victim of a recent natural disaster – trying to exploit the reader's sympathy. Although most recipients of the emails do not respond there will always be a small but tangible proportion that does.

The perpetrators of these attacks are highly versatile when it comes to making use of new opportunities. The increase in the popularity of social networking sites has meant that targeted 'spear phishing' attacks are easier to carry out, with attackers making use of information that is freely available on these sites and targeting potential victims specifically via email, including some of the user's personal information to make the attempt look more convincing and authentic.

In view of the above, it is clear that users require support and awareness in order to protect themselves. Although a number of online sources exist if people are prepared to look for them, many are non-interactive and rely upon people having the interest and dedication to read the materials purely for their own sake. As such, dressing the awareness raising in a more enjoyable context could provide a means to reach users who may not otherwise have the dedication to investigate the topics for themselves. It was therefore decided that an educational, interactive application would be a good way to proceed, aiming the at everyday users (i.e. not overly technical or complicated) with the intention of making their learning more palatable than just reading pages of text. There are already examples of such approaches to be found, with a particularly good one being the Anti-Phishing Phil game from Carnegie Mellon University (Sheng et al. 2007). However. while phishing is currently the most common social engineering attack it is not the only one and there appears to be scope for further solutions aimed at the other forms of attacks.

BOARD GAME PROTOTYPE

There were a number of possibilities for the form of game to be developed, with early ideas including a role-playing game (RPG) that would enable the user to take control of a character and navigate through an area in order to achieve the main goal that would have been centred on answering questions and gaining knowledge. However, due to the fairly small development window available, the decision was taken to pursue a more straightforward board game approach. This would have accompanying website literature that could be referred to should the user be unable to answer a question, allowing an interactive way to learn rather than simply reading materials without a task to focus upon. The main aim was to develop a working prototype that could be evaluated and then further developed within follow-on research.
It was important that the game was fairly simplistic in terms of how it would be played as the aim of this was to educate users, not to require them to read pages of instructions informing them of how to play the game. A board game ensured that the solution would be easy to understand and therefore maximise time to educate the user whilst still having an interactive interface.

The board included 32 squares, with each assigned to one of four social engineering topics (with the named categories being phishing, advance fee fraud and spam, along with a fourth category labelled 'other', which addressed the less common attacks). Each category was represented by a different colour on the game board (e.g. phishing was red and advance fee fraud was yellow), with the number of times each colour appears on the board being pre-determined by the extent of the threat concerned. For example, as phishing was identified as one of the most damaging form of social engineering, red squares appear more frequently than the advance fee fraud questions.

For the quiz element, a multiple-choice format was selected as it was felt to provide an effective way to pose questions and collect users' responses. For the prototype, simple text-based presentation was used for the options, but further development would permit the same multiple-choice approach to be used in conjunction with questions involving images and/or audio/video content.

The player's score is tracked throughout the game in order to provide an extra level of motivation to the user, and thus increase their knowledge and education. Although not implemented in the prototype, a high score feature would represent an easy addition, and could be further extended to track scores in a multiplayer context.

Rather than being a straight forward 'roll and move forward' type of game, the option to move back was added. Upon rolling, all squares were to dim, with the available squares staying lit. Whilst this offered nothing other than a minor addition to gameplay, it was felt it was adding something that could be more useful in a later development. For example, if a 'bonus' square was added in a future version, the option to move backwards may allow for the user to get there quicker. This reasoning would also be the same if there were other targets to achieve, (for example, if they were given the task of answering a certain number of phishing questions within a set time).

The following steps outline the general game flow, indicating how the operations work from the users' perspective:

1. Upon opening the game the user is greeted with the main menu. From here they can view the instructions and click 'start game' or just click 'start game' without reading viewing the instructions.
2. The user enters their name, selects their piece, and clicks 'submit'.
3. Upon submitting their name and piece, the game begins (see Figure 1). The user clicks 'start' to begin the dice animation, upon clicking 'stop' the selector stops.
4. With a number selected, all squares are dimmed, with the two possible movable squares staying lit.
5. Upon choosing a square the user's piece is moved to the chosen location and a question is asked (see Figure 2)
6. The user then selects an answer and feedback is immediately provided.
7. Depending on whether the user gets the answer right or wrong, the square deactivates and contains a tick or a cross.
8. Upon answering all questions, or clicking the 'quit' button, the user is given their score and can either close the game completely, or click 'finish' which will take them back to the main menu.

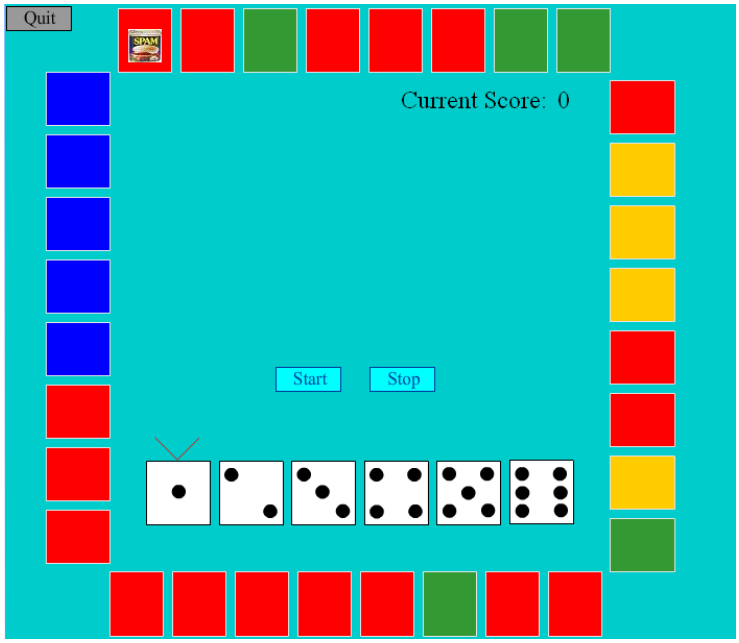

Figure 1 - The main game board

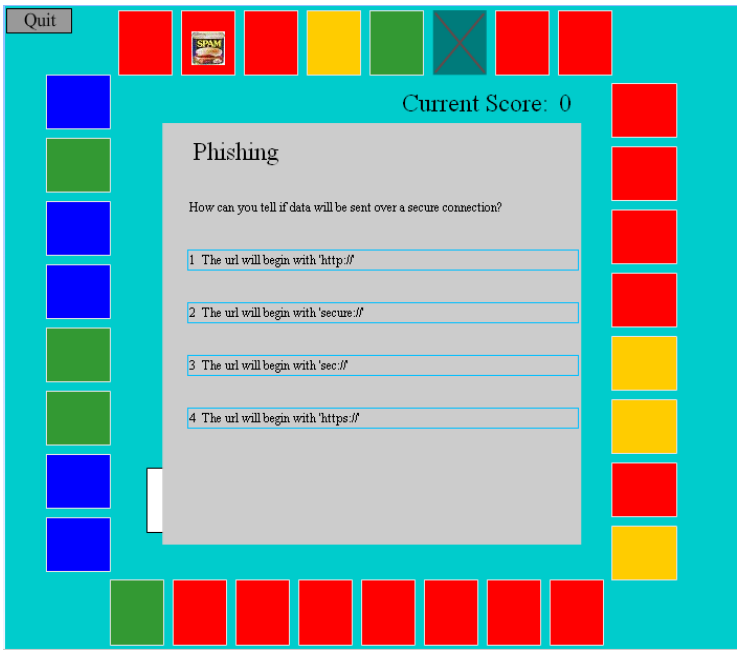

Figure 2 - Question Interface

USER EVALUATION

In conducting an evaluation, the intention was to recruit users with varying levels of existing knowledge in the area. Although the solution assumed very little knowledge in the subject area, ideally it would be beneficial to the majority of users and so it was vital to ensure that the test participants represented a range of user ability. 35 requests for user testing were sent, with 21 users ultimately carrying out the test. 14 of the participants were male, with 7 female. In relation to age, 2 were 18 or under, 12 were 19-25, 3 were 26-35, 1 was 36-45 and 3 were aged 45+.

The solution was tested by asking the users three preliminary questions to find the length of time they spend on the Internet every week and their current knowledge in the subject area. They were then asked read through the online material once, and then play through the game whilst referring to the literature if necessary. They then resumed the questionnaire and were asked to provide their score, overall feelings on the game and literature and their recommendations for future development which was vital with this being a prototype.

Figure 3 shows the relation between time spent online and the achieved score. It would be expected that the longer someone spends on the Internet, the better score they would achieve. As seen below this seemed to be generally the case. As the solution is aimed at every day Internet users, the users at the lower end of the Internet usage were not expected to get poor scores as it was ensured that the material was aimed for a range of users. This seems to be shown below, with the lowest score achieved being 450 which is approximately 56% from someone who spends very little time on the Internet.

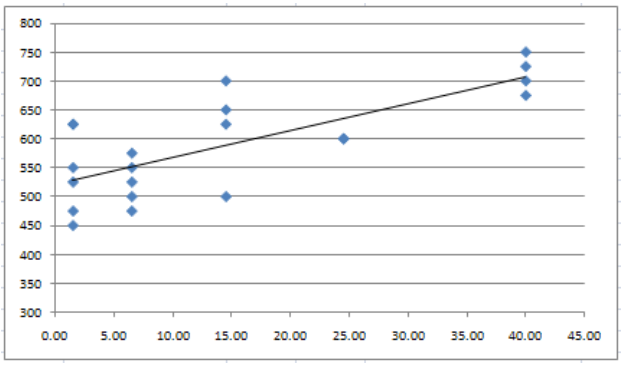

Figure 3 - The relationship between time spent on the Internet and score

Following their evaluation of the game, participants were asked to indicate whether they felt they had learned something as a result. In the vast majority of cases (86%) the users reported that their awareness of social engineering had improved, with the underlying responses recorded as follows:

- 29% felt more aware of the dangers to the point that they felt comfortable to deal with the problem;
- 38% felt more aware of the dangers and wanted to find out more information;
- 19% felt more aware but did not want to look at anything else;
- 14% did not feel more aware and felt that nothing was new to them.

The testing results suggested that the prototype was successful as an awareness-raising tool. In addition, 17 out of 21 of the test participants found the level of website literature suitable, with 18 of them satisfied with the question levels in the game.

Having played the game, participants were asked about factors that it might be useful to see addressed as part of future development. Figure 4 summarises the feedback in this respect. Improved graphics was the most popular option. There are various ways in which this could be developed in the future, including a more aesthetically pleasing board layout rather than the coloured squares in the prototype. Indeed, further development work since the user evaluation has already begun to revise and enhance this aspect, and an example of the revised main game board is shown in Figure 5 (noting that the SP shown in the shield refers to 'Security Pursuit', the working title of the game).

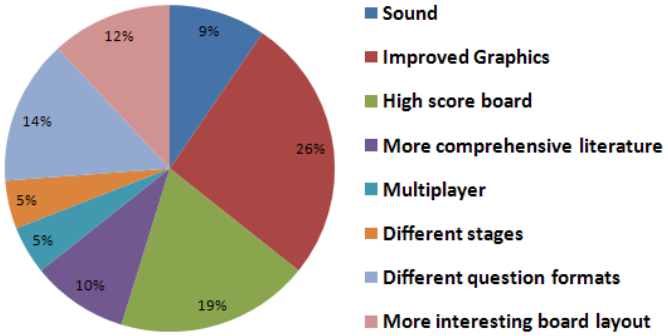

Figure 4 - Features desired in future developments

The second most popular feature was a high score board, which as well as adding a user requested element to the game, may also be a way of retaining the users attention, with a goal for themselves of getting on the high score board they are less likely to become bored. It may also tempt the user to replay the game.

Different question formats was the third most popular feature. This could include things such as displaying four emails to the user, and have them select the email that is a social engineering attack. An alternative to this could be displaying a single email and have the user select the 'hotspots' that would suggest that it is a social engineering attack.

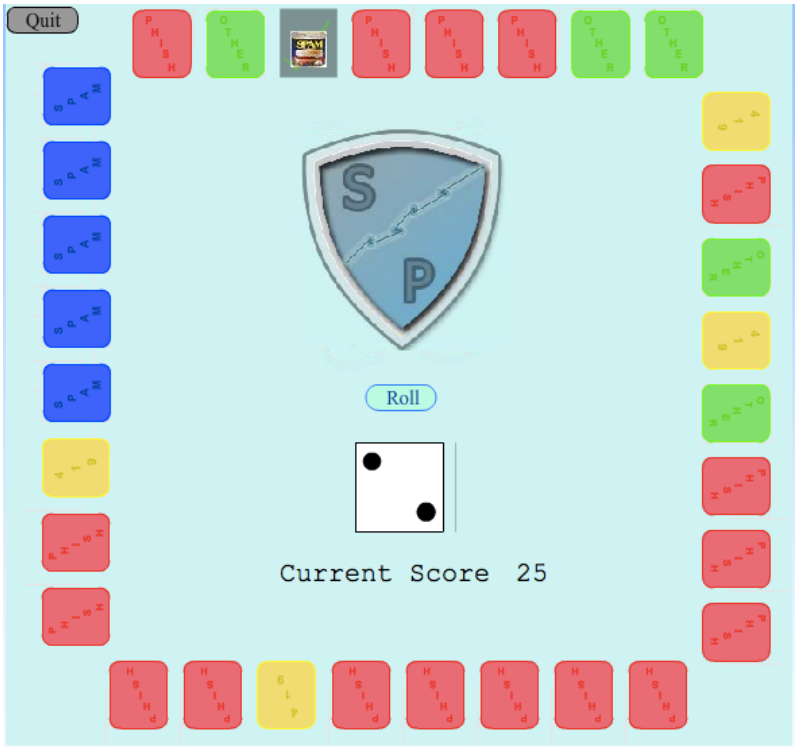

Figure 5- The revised main game board

CONCLUSION

User awareness has a fundamental role to play in maintaining the security of systems and data. Providing support in an engaging and enjoyable manner increases the chances of users taking part and the key information being retained.

The board game approach presented in this paper was considered to meet the criteria of being interactive, and combining the game with reference literature was thought to make the digestion of the latter more enjoyable than simply reading static text. Whilst it was accepted that only offering multiple-choice questions was not ideal, it was a realistic starting point for an initial version of the game.

It can be seen that with the prototype showing potential, if the additional developments are implemented in a future development, participation should increase and ideally so will the awareness levels of those who play.

REFERENCES

APWG. 2009. Phishing Activity Trends Report, 1st Half 2009, Anti-Phishing Working Group, January-June 2009, http://www.apwg.org/reports/apwg_report_h1_2009.pdf (accessed 30 September 2009).

Bennet et al. Object Oriented Analysis and Design. 2nd Ed. London. McGraw-Hill.

BERR. 2008. 2008 Information Security Breaches Survey – Technical Report, Department for Business, Enterprise and Regulatory Reform, April 2008, URN 08/788.

ENISA. 2008. Social Engineering: Exploiting the Weakest Links. Whitepaper, European Network and Information Security Agency, October 2008. http://www.enisa.europa.eu/act/ar/deliverables/2008/social-engineering (accessed 30 September 2009).

Gartner. 2007. Gartner Survey Shows Phishing Attacks Escalated in 2007. Press release, 17 December 2007. http://www.gartner.com/it/page.jsp?id=565125 (accessed 30 September 2009).

SAI Global. 2008. SAI Global Information Security Awareness Survey 2008. http://www.saiglobal.com.

Sheng, S., Magnien, B,, Kumaraguru, P., Acquisti, A., Cranor, L., Hong, J. and Nunge. E. 2007. "Anti-Phishing Phil: The Design and Evaluation of a Game That Teaches People Not to Fall for Phish", in Proceedings of the 2007 Symposium On Usable Privacy and Security, Pittsburgh, PA, 18-20 July 2007.

COPYRIGHT

Michael Newbould & Stephen Furnell ©2009. The author/s assign the Security Research Centre (SECAU) & Edith Cowan University a non-exclusive license to use this document for personal use provided that the article is used in full and this copyright statement is reproduced. The authors also grant a non-exclusive license to SECAU & ECU to publish this document in full in the Conference Proceedings. Such documents may be published on the World Wide Web, CD-ROM, in printed form, and on mirror sites on the World Wide Web. Any other usage is prohibited without the express permission of the authors