Education in the 'Virtual' Community: Can beating Malware Man teach users about Social Networking Security?

A.A. Sercombe and M. Papadaki

Centre for Security, Communications and Network Research,
Plymouth University, United Kingdom
e-mail: info@cscan.org

Abstract

Social Networks have become part of daily life for millions of people and by their very nature they encourage information sharing. 2011 was a year that saw numerous targeted "Spear Phishing" attacks in which it was clear that attackers gained knowledge about victims prior to carrying out their attacks. There is evidence that social media has been utilised as the source for this information so therefore it is more important than ever that users are educated against the risks.

This paper starts by looking at the current threats and awareness strategies. It then describes the design and evaluation of an online game to help educate users. The game has a central 'Malware Man' character and a firewall which burns him if the player answers correctly. The success of the game was evaluated using an experiment with a group of participants who had played the game, and a control group who had not. 101 users participated in the study. The results suggest that the game was successful in educating users as the average percentage of correct answers was 77% for those who had played the game, compared to 55% for those who had not.

Keywords

Social Networking, Social Networks, Phishing, Spear Phishing, Education, Awareness, Game, Interactive

1 Introduction

Social Networks are defined as 'networks of social interactions and personal relationships' (Oxford Dictionary, 2011). They are used to build online communities of people who share associations with one another (Shin, 2010). Facebook alone, reports that it has over 800 million active users, of which more than 50% logon every day (Facebook, 2012). These statistics indicate that there is a large amount of data to mine and a plentiful supply of users that could be targeted. It is clear that social media is a very lucrative target and information source for attackers.

These threats do not only affect individuals, but also pose a risk to organisations, governments and infrastructure. 2011 has seen a decrease in the amount of spam detected, but at the same time, an increase in the number of targeted attacks. It has

been proposed that this may be because attackers are moving away from spam and are choosing to use social networks to mine information so that they can perform more targeted attacks (Symantec, 2011).

A security intelligence company called Stratfor was the victim of a targeted attack in the last week of 2011. At around the same time they released an announcement on Facebook stating that they had evidence that users or employees who posted messages of support on social networking sites were being specifically targeted (BBC, 2011). This is further evidence that information on social media sites is being used by attackers as a standard information gathering tool and that it can also be used to target individuals.

2 Awareness Strategies

There are a number of different strategies used to raise awareness about security threats, and there has been considerable research in this area. The U.K. government, law enforcement and a number of large organisations sponsor a Get Safe Online initiative (www.getsafeonline.org) (Furnell, Bryant & Phippen, 2007). The web site offers videos, guides, reports and help for users and small businesses to raise their security awareness. Globally there are numerous initiatives, for example the European Network and Information Security Agency (ENISA), which provides an awareness raising program of workshops, conferences and literature.

In general, training materials are effective when users actually read them (Sheng et al., 2007). This is easier said than done in some contexts. For example, social networking users cannot be forced to read the material like in an organisational context.

An alternative is defined as ‘embedded training’ whereby users are taught during their normal use and techniques, like role playing can be employed. A game called ‘Anti-phishing Phil’ (Sheng et al., 2007) was developed to complement the research in this area and the evaluation of it has shown it to be effective in educating users about Phishing attacks. The limitation of this game is that it is only focusing on one area of awareness. The danger might be that users have a false sense of security because they have 'educated' themselves in this one area but may have missed other threats. To complement the existing research that has been carried out, this project will attempt to educate social networking users about security threats whilst in the context of a game. The aim is to make the game fun to ensure that users want to play it and also to ensure that it educates them. Games like Anti-Phishing Phil have tended to focus on a particular threat whereas this game will aim to cover a range of threats and will be a more general security awareness tool.

3 Malware Man Design

A number of requirements were collated as a result of learning and education research and a literature review. The key requirements for the education game are listed below:

3.1 Requirements

3.1.1 Non-functional

- The game must captivate player attention (Dondlinger, 2007).
- The game design should promote and foster learning (Dondlinger, 2007).
- A narrative context should be used to ensure that the game is engaging and fun (Sheng et al, 2007).
- The game must have a strong character and story to help motivate players (Sheng et al, 2007).
- There should be an emphasis on skill as there must be a challenge to keep player attention.

3.1.2 Functional Requirements

- The game should be dynamic and easily configurable for different types of Social Networks.
- The game should also be customisable so that it is relevant for different types of users.
- It is important that the game is available to as wide a group of users as possible so it should be as platform independent as possible.

3.2 Design

The game was developed using Adobe Flash Builder 4.5 using the Adobe Flex development language to build a .swf file that can be played using Adobe's Flash Player. This ensures that the game will run on any browser as long as it has Flash Player 10 or above installed.

There are three game states; 'Start', 'InGame' and 'End'. If the user answers correctly, a flickering animated firewall increases in size and a speech bubble appears giving the impression that Malware Man is being hurt.

Help information appears providing the user more information about the question and the correct answer after they have submitted their answer. If the user answers correctly then the text will be coloured green.

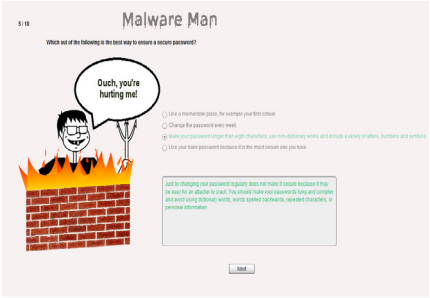

Figure 1: Game Image (Malware Man image sourced from LakeSuperiorityComplex (2011).

If the user answers incorrectly then the firewall stays the same size, and the wrong answer and hint text are coloured red. The right answer is coloured green, so that the user can immediately see where they went wrong.

The design of the questions is centred around the main threats briefly outlined earlier in this paper. The questions were all multiple choice with four possible answers. Some questions included images from social networks, for example a wall posting from a Facebook feed to make the question more relevant to the user. Three sets of ten questions were created for three different versions of the game.

4 Evaluation Design

A user study was used to evaluate how successful the game was in educating users. The study consisted of a group of users who had played the game and a control group who had not. Both groups were given the same survey to complete. The survey included social networking security questions similar to that used in the game and the hypothesis was that the users that had played the game would answer more questions correctly. The questions were multiple choice and reflected the areas that were covered within the game. The research is mainly quantitative in nature but there was also an informal feedback field in the survey for participants to give some qualitative feedback on the game.

The two sample groups included Plymouth University Masters and Undergraduate students and UK Met Office employees. All participants were over 18 years old and the study did not include vulnerable adults. An invitation email and a consent page outlined the aims of the research, contact details, a clear description of the right to withdraw at anytime and a reinforcement that participation is voluntary.

5 Results

104 participants took part in the study, of which three results were discarded due to all blank answers to the questions. The overall percentages are 32% female, 65%

male and 3% undisclosed. 51% of participants were aged between 26-35 and 32% were between 36-45. The other 17% were either 18-25, 46-55 or 56-65.

Figure 2 below shows that that the % of Correct answers is significantly higher for those users that played the game compared to those who had not. The results indicate that the overall percentage of correct answers for those users who played the game was 77%, as opposed to 55% for those who had not played. The first 8 questions in the survey were the same for all users so these are split out in the results. The other questions were Facebook or Twitter specific and only appeared if users played those specific versions of the game but also provided very similar results.

	Correct Answers	Incorrect Answers	Un-answered	Total	% Correct out of Total	% Incorrect out of Total
No Game - 1st 8 Questions	215	177	0	392	54.847	45.153
Game - 1st 8 Questions	322	92	2	416	77.404	22.115
No Game - All Questions	276	239	73	588	46.939	40.646
Game - All Questions	439	116	69	624	70.353	18.590

Figure 2: Table of overall Results

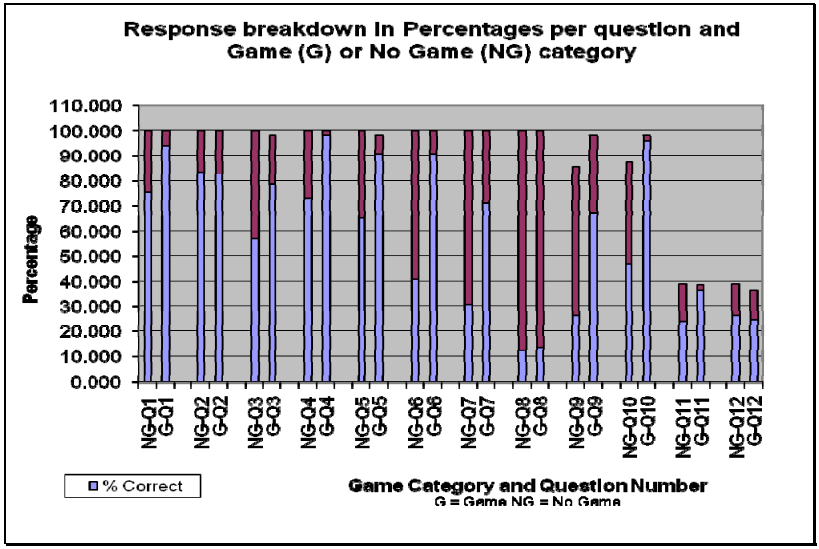

Figure 3: Graph showing a breakdown of the results

Figure 3 shows a breakdown of the results for each question for users who had played the game compared to those who had not. There was one question out of the eight that all answered that was statistics based (Q8 in the graph above). The question was ' During a 3 month period in 2010, what percentage of all malicious URLs observed on social networking sites made use of URL shortening? (According to Symantec threat report 2010).' Before analysing the results, it was thought that as the users had seen these statistics in a similar question when they played the game, they should do better than those who had not played. In actual fact only 13.5% answered correctly compared to 12.3% who had not played. This is interesting as it may suggest that more descriptive questions are more effective in embedding learning. The idea was that the users would be shocked by the percentage and then be more aware of the risk. They may have remembered the principle without the actual percentage and it is not possible to draw conclusions from one question but may warrant further investigation.

Another question where there is a similar percentage for those who played or did not play is question 2. This question was ' Shortened web addresses are more secure because they are harder for hackers to amend?'. A high percentage of both groups answered correctly so this question may have been more obvious for both groups. It was also a true or false question so there is a higher chance that they may have guessed the correct answer.

The informal feedback on the game showed that participants found the game to be generally fun and informative, but there were some concerns over the clarity of the colours for users with colour blindness. One participant suggested that a leader board may have added to the experience so they could see how they performed compared to other users.

6 Conclusions and Future Work

This paper has provided an overview of the current social networking threats and awareness campaigns and has then presented the design and evaluation of the Malware Man Game.

The results suggest that the game was successful in educating users as there was a large difference between the number of correct answers for those that had played the game, compared to those who had not. The sample size was not sufficient to be conclusive and the participants belonged to a specific demographic.

Future research could include looking at different cultures and demographics of users, as well as using a larger sample size. It could also include extensions to the game for different levels and could give forms of reward to see if this improves the user experience.

Trialing the game against other forms of online educational material and carrying out a study to determine how well the game performed comparatively would give a better understanding of how effective the game is in educating users in comparison

to other techniques. It would also be worth investigating further whether different types of questions may be more effective than others as a result of this research.

7 References

BBC, 27/11/2011, *'Anonymous' hack victims face repeat attacks*, BBC. Available from: <http://www.bbc.co.uk/news/technology-16338680>.[27/12/2011].

Dondlinger, MJ 2007, 'Educational video game design: A review of the literature', *Journal of Applied Educational Technology*, vol. 4, no. 1, pp. 21-31.

Facebook, *Statistics-Facebook*, Facebook. Available from: <https://www.facebook.com/press/info.php?statistics>. [05/01/2011].

Furnell, SM, Bryant, P & Phippen, AD 2007, 'Assessing the security perceptions of personal Internet users', *Computers & Security*, vol. 26, no. 5, pp. 410-417.

Hogben, G 2007, 'Security issues and recommendations for online social networks', *Position Paper ENISA European Network and Information Security Agency*, vol. 80211, no. 1.

Jagatic, TN, Johnson, NA, Jakobsson, M & Menczer, F 2007, 'Social phishing', *Communications of the ACM*, vol. 50, no. 10, pp. 94-100.

LakeSuperiorityComplex 2011, *Evil Nerd* (Image). Available from: <http://lakesuperioritycomplex.wordpress.com/2010/06/29/therewoman/>.[01/04/11]
OxfordDictionary 2011, *Oxford Dictionaries - Definition of Social Network* in Oxford Dictionaries, Oxford University Press, [01/06/2011].
Sheng, S, Magnien, B, Kumaraguru, P, Acquisti, A, Cranor, LF, Hong, J & Nunge, E 2007, 'Anti-Phishing Phil: the design and evaluation of a game that teaches people not to fall for phish', in, ACM, pp. 88-99.

Shin, D-H 2010, 'The effects of trust, security and privacy in social networking: A security-based approach to understand the pattern of adoption', *Interacting with Computers*, vol. 22, no. 5, pp. 428-438.

Symantec, CW- 2010, 'The Risks of Social Networking', *Symantec - Security Response*[12/05/2011].

Symantec, PW- 2011, *Symantec Intelligence Report: November 2011*, Symantec, [20/12/2011].