A Game Storyboard Design for Avoiding Phishing Attacks

Nalin A.G. Arachchilage*
University of British Columbia
2332 Main Mall
Vancouver, BC Canada
nalin@ece.ubc.ca

Ivan Flechais†
University of Oxford
Wolfson Building, Parks Road
Oxford, UK, OX1 3QD
ivan.flechais@cs.ox.ac.uk

Konstantin Beznosov‡
University of British Columbia
2332 Main Mall
Vancouver, BC Canada
beznosov@ece.ubc.ca

1. INTRODUCTION

Security exploits can include cyber threats such as computer programs that can disturb the normal behaviour of computer systems (viruses), unsolicited e-mail (spam), malicious software (malware), monitoring software (spyware), attempting to make computer resources unavailable to their intended users (Distributed Denial-of-Service or DDoS attack), the social engineering, and online identity theft (phishing). One such cyber threat, which is particularly dangerous to computer users is phishing [2]. Phishing is well known as online identity theft, which aims to steal sensitive information such as username, password and online banking details from its victims. Automated anti-phishing tools have been developed and used to alert users of potentially fraudulent emails and websites. However, these tools are not entirely reliable in detecting phishing attacks [6] [1]. Even the best anti-phishing tools missed over 20 percent of phishing websites [8]. Because the "human in the loop" is the weakest link in information security [5] [1]. It is not possible to completely avoid the end-user, for example in personal computer use, one mitigating approach for computer and information security is to educate the end-user in security prevention [1] [7] [6] [8] [3]. The aim of this research study focuses on storyboarding a game design for mobile platforms to educate individuals about phishing attacks. Therefore, the study asks how does one identify which issues the game storyboard needs to be addressed? Garera et al. [4] strongly argue it is often possible to differentiate phishing websites from legitimate ones by carefully looking at the URL. Therefore, this mobile game storyboard designed to teach people to identify legitimate URLs from mimic ones.

2. GAME DESIGN ISSUES

To answer these issues, the elements of a game design framework were incorporated into the mobile game storyboard design context. The game design framework (Figure 1) describes individual computer users' behaviour in avoiding the threat of malicious information technologies such as phishing attacks [1]. The model examined how individuals avoid phishing threats by using given anti-phishing game based education.

Consistent with the game design framework (Figure. 1), the users' phishing threat avoidance behaviour is determined by avoidance motivation, which, in turn, is affected by perceived threat. Perceived threat is influenced by perceived severity and susceptibility as well as their combination. Users' avoidance motivation is also determined by the three constructs such as safeguard effectiveness, safeguard cost, and

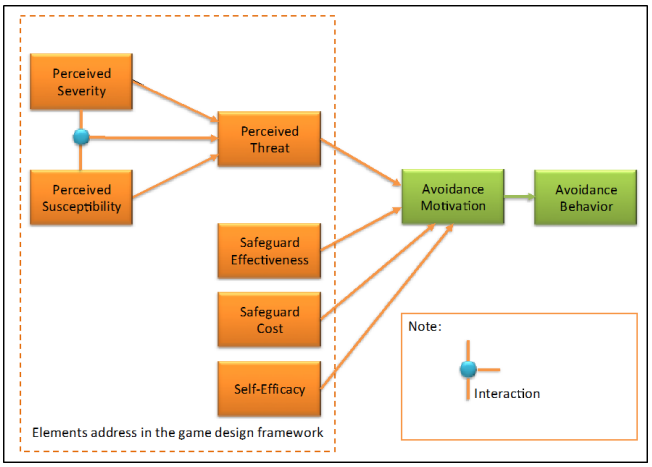

Figure 1: The game design framework [1]

self-efficacy. In addition, the game design framework posits that perceived threat is influenced by the combination of perceived severity and susceptibility. Whilst the game design framework informs the issues that the game design needs to address, it should also indicate how to structure this information and present it in a game context. Therefore, the game design based on a story attempts to develop threat perceptions, making individuals more motivated to avoid phishing attacks and use safeguarding measures. Finally, the elements of the game design framework were incorporated into mobile game storyboard design to enhance individuals' phishing threats avoidance behavior through their motivation to protect themselves from phishing attacks.

3. STORY AND MECHANISM

Storytelling techniques are used to grab attention, which can also help to focus on interesting aspects of reality. Stories can be based on personal experiences or famous tales or they could also be aimed at building a storyline that associates content units, inspires, or reinforces.

The game is based on a scenario of a character of a small fish and 'his' teacher who live in a big pond. The more appropriate, realistic and content relevant the story, the better the chances that it will trigger users. The main character of the game is the small fish, who wants to eat worms to become a big fish. The game player roll plays as a small fish. However, he should be careful of phishers those who try to trick him with fake worms. This represents phishing attacks

by developing threat perception in the game storyboard design. Each worm is associated with a website address (URL), which appears in a dialog box. The game was designed with a total of 10 URLs to randomly display including five good worms and five bad worms. The small fish's job is to eat all the real worms which associate legitimate website addresses and reject fake worms which associate with fake website addresses before the time is up. This attempts to develop the severity and susceptibility of the phishing threat in the game storyboard design. The other character is the small fish's teacher, who is a matured and experienced fish in the pond. If the worm associated with the URL is suspicious and if it is difficult to identify, the small fish can go to 'his' teacher and request help. The teacher could help him by giving some tips on how to identify bad worms. For example, "website addresses associate with numbers in the front are generally scams," or "a company name followed by a hyphen in a URL is generally a scam". Whenever the small fish requests help from the teacher, the score will be reduced by certain amount (in this case by 100 seconds) as a payback for safeguard measure. This attempts to address the safeguard effectiveness and the cost needs to pay for the safeguard in the game storyboard design. The game storyboard design consists of total 10 URLs to randomly display worms including five good worms (associated with legitimate URLs) and five fake worms (associated with phishing URLs). If the user correctly identified all good worms while avoiding all fake worms by looking at URLs, then he will gain 10 points (in this case each attempt possible to score 1 point). If the user falsely identified good worms or fake worms, each attempt loses one life out of total lives remaining to complete the game. If the user requested help from the big fish (in this case small fish's teacher) each attempt loses 100 seconds out of total remaining time to complete the game, which is 600 seconds. Therefore, self-efficacy of preventing from phishing attacks will be addressed in the game storyboard design when the user comes across throughout the game.

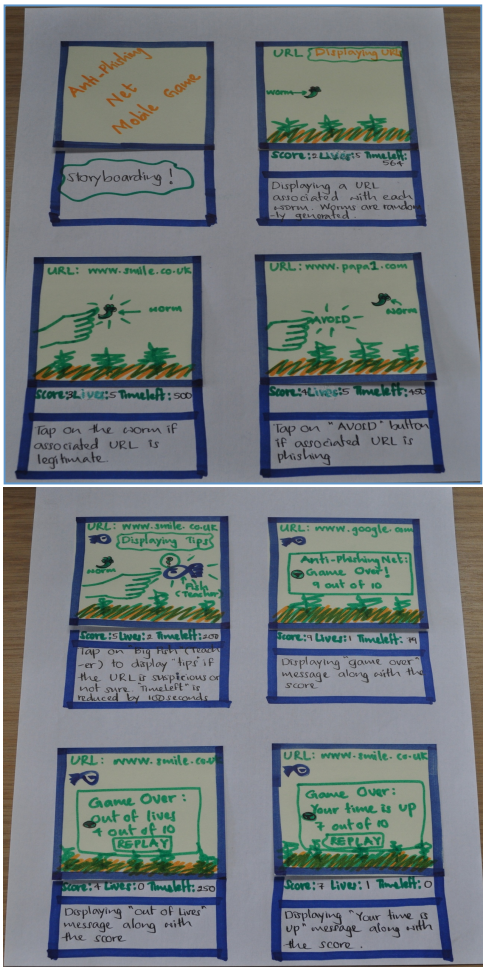

Figure 2: The game storyboard design

4. STORYBOARD DESIGN

Quick and dirty paper prototypes are considered as more powerful to use for designing storyboard. Therefore, the game was initially sketched in a storyboard using ink pen, post-it notes, and papers based on the above mentioned story and which is shown in Figure 2 [7].

5. CONCLUSION

This research focuses on designing a game storyboard to educate computer users to thwart phishing attacks. It asks how does one identify which issues the game storyboard needs to be addressed? The elements of a game design framework were incorporated into the mobile game storyboard design context. The objective of our proposed game storyboard design was to teach user how to identify phishing website addresses (URLs). The overall game storyboard design was targeted to enhance avoidance behavior through motivation to protect computer users from phishing attacks.

6. REFERENCES

[1] N. A. G. Arachchilage and S. Love. A game design framework for avoiding phishing attacks. *Computers in Human Behavior*, 29(3):706–714, 2013.

[2] R. Dhamija, J. D. Tygar, and M. Hearst. Why phishing works. In *Proceedings of the SIGCHI conference on Human Factors in computing systems*, pages 581–590. ACM, 2006.

[3] J. S. Downs, M. Holbrook, and L. F. Cranor. Behavioral response to phishing risk. In *Proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit*, pages 37–44. ACM, 2007.

[4] S. Garera, N. Provos, M. Chew, and A. D. Rubin. A framework for detection and measurement of phishing attacks. In *Proceedings of the 2007 ACM workshop on Recurring malcode*, pages 1–8. ACM, 2007.

[5] S. Purkait. Phishing counter measures and their effectiveness–literature review. *Information Management & Computer Security*, 20(5):382–420, 2012.

[6] S. Sheng, B. Magnien, P. Kumaraguru, A. Acquisti, L. F. Cranor, J. Hong, and E. Nunge. Anti-phishing phil: the design and evaluation of a game that teaches people not to fall for phish. In *Proceedings of the 3rd symposium on Usable privacy and security*, pages 88–99. ACM, 2007.

[7] K. N. Truong, G. R. Hayes, and G. D. Abowd. Storyboarding: an empirical determination of best practices and effective guidelines. In *Proceedings of the 6th conference on Designing Interactive systems*, pages 12–21. ACM, 2006.

[8] Y. Zhang, J. I. Hong, and L. F. Cranor. Cantina: a content-based approach to detecting phishing web sites. In *Proceedings of the 16th international conference on World Wide Web*, pages 639–648. ACM, 2007.