Designing a Mobile Game to Teach Conceptual Knowledge of Avoiding "Phishing Attacks"

Nalin Asanka Gamagedara Arachchilage, Steve Love, Michael Scott
School of Information Systems, Computing and Mathematics
Brunel University
Uxbridge, Middlesex, UK

Abstract

Phishing is a form of online identity theft, which attempts to appropriate confidential and sensitive information such as usernames and passwords from its victims. To facilitate cyberspace as a secure environment, phishing education needs to be made accessible to home computer users and mobile games enable embedded learning in a natural environment. Previously, we have introduced a mobile game design that aimed to enhance avoidance motivation and behavior to protect against phishing threats. This paper focuses on a design that develops the conceptual knowledge that is necessary to combat phishing threats, home computer teaching users about phishing emails and web addresses. The prototype game design is presented on Google App Inventor Emulator.

1. Introduction

Security exploits can include IT threats such as viruses, malicious software (malware), unsolicited e-mail (spam), and monitoring software (spyware). Phishing, however, is a form of *semantic attack* [1, 8] that leverages human vulnerabilities, rather than exploiting technical pitfalls. Attackers will attempt to trick Internet users into following malformed URLs (Uniform Resource Locators) that mimic legitimate versions as closely as possible. These will typically lead to fraudulent websites that share the same look-and-feel as the real version. Users may then unintentionally provide private information such as usernames, passwords or bank details to a third party.

This research comprehends the need of which the human aspect of security can be influenced to avoid malicious IT threats in the context of home computer use. These users are susceptible to phishing threats due to the rapid growth of Internet technology [9]. It is so ubiquitous today that it provides the baseline for modern living, enabling ordinary people to socialize, shop, and be entertained all through their home computers. As people's reliance on the Internet grows, the possibility of hacking, attacking and other security breaches increases day by day [5]. Therefore, home computer users make a significant contribution in helping to make cyberspace a safer place for everyone and the message "security starts at home" should be spread to all home computer users [2].

In the past, phishing attacks have been distributed through scam emails [10, 17]. For example, urging people to participate in a survey or verify their bank account information. Now it has become a persistent threat as people consume and distribute a significant amount of information through links in social media. This includes internet enabled services such as Facebook, Hi5, Skype, Twitter, Orkut, Google+, and even more professional social networking website such as LinkedIn.

In addition, as organizations have become increasingly 'virtual' there has been a technological move from work to the domestic environment [7]. Employees have freedom to work at home or bring unfinished work home due to the pervasiveness of Internet technology. This increases the opportunity for home computer users to open a "back door" to vulnerable IT threats. These home computer users are unlikely to have a sufficient IT infrastructure or technology to protect themselves from malicious IT attacks, or may not have a proper standard or strict IT security policies in place. For example, most home computer users are not IT professionals and lack the necessary computer literacy to establish a secure home computing system. Home computer users also tend to display unsafe computer behavior that is particularly vulnerable to IT threats. For example, browsing unsafe websites, downloading suspicious software, sharing passwords among family and peers, and using unprotected home wireless networks [5].

As phishing attacks become increasingly sophisticated, it becomes more challenging to protect against them [3, 13] and without an appropriate level of security awareness, some home computer users are becoming vulnerable to these new threats [12, 14]. A number of automated software tools have been developed to alert users of potentially fraudulent emails and websites [13]. Ye and Sean

[21] and Dhamija and Tygar [15] have developed a prototype called "trusted paths" for the Mozilla web browser that is designed to help users verify that their browser has made a secure connection to a trusted website. However, these systems are not totally reliable in detecting phishing attacks [19]. Previous research has revealed that the available anti-phishing tools such as Calling ID Toolbar, Cloudmark Anti-Fraud Toolbar, EarthLink Toolbar, Firefox 2, eBay Toolbar, and Netcraft Anti-Phishing Toolbar are insufficient to combat phishing threats [18]. Even the best toolbars miss over 20% of phishing websites [20]. On the one hand, software application designers and developers, with the help of security expertise, will continue to improve phishing and spam detection. Nonetheless, the human factor risk is high and people are the weakest link in information security [4]. Therefore, it is appropriate to mitigate human factor risks by educating users against phishing threats [16, 18].

In this paper, we present the design of a mobile game that aims to develop conceptual knowledge of phishing URLs. The most significant feature of mobile environment is *mobility* itself such as mobility of the user, mobility of the device, and mobility of the service [11, 22]. It enables users to be in contact while they are outside the reach of traditional communicational spaces. For example, a person can play a game on his mobile device while travelling on the bus or train. The reminder of this paper is organized as follows: section two discusses related work; section three describes the game prototype design we created on Google App Inventor Emulator; and the paper concludes in section four opening future work directions.

2. Related work

All Arachchilage and Cole [11, 12] designed a mobile game design prototype as an educational tool to teach home computer users to protect themselves against phishing attacks. Their research proposed a mobile game design for learning, based on a story, which simplifies and exaggerates real life situations. The research asked the following questions: The first question is how does the system developer identify which issues the game needs to address? Once the developer has identified the salient issues, they are faced with second question, what principles should guide the structure of this information. A theoretical model derived from Technology Threat Avoidance Theory (TTAT) was used to address those mobile game design issues and the mobile game design principles were used as a set of guidelines for structuring and presenting information in the mobile game design context [6, 11]. The objective of their anti-phishing mobile game design was to teach the user how to identify phishing URLs and emails, which is one of many ways to identify a phishing attack. The overall mobile game design was focused to enhance avoidance behavior through motivation of home computer users to thwart phishing threats. The prototype game design was presented on Google App Inventor Emulator.

The proposed mobile game design was focused almost entirely on procedural knowledge. However, some conceptual knowledge about the parts of URL and email might help the user to distinguish phishing URLs and email messages from legitimate ones [19]. Therefore, this research attempts to address this issue in the mobile game design context. For example, when a user correctly identifies a phishing URL, they should be asked which portion of the URL indicates phishing, to determine whether or not they have understood the concept of a phishing URL. Alternatively, when a user is presented with a portion of a phishing email, addressing "Dear Valued Customer" this can also be used to determine whether or not they have understood the concept of phishing email. Therefore, this research attempts to extend Arachchilage and Cole's [11, 12] mobile game design by addressing conceptual knowledge of phishing URLs and emails to thwart phishing attacks.

3. Game prototype design

To explore the viability of using a game to thwart phishing attacks based on conceptual knowledge, a prototype was implemented using Google App Inventor Emulator. We created a story addressing conceptual knowledge of phishing URLs and emails within a game design context.

3.1 Story

The game is based on a scenario of the character of a small fish and a big fish that both live in a big pond. The main character is the small fish, who wants to eat worms to become a big fish. Worms are randomly generated in the game design. The user role-plays as the small fish. However the small fish should be careful of phishers those who try to trick him with fake worms. This represents phishing attacks by developing threat perception. The other character is the small fish's teacher, who is experienced fish in the pond. The proposed mobile game design prototype contains two sections: teaching the concept of phishing URLs and phishing emails. In the mobile game design, the user is presented a combination of phishing and legitimate URLs (in this case 15 URLs) and emails (in this case 15 emails). Both URLs and emails are targeted to teach user conceptual knowledge of phishing attacks.

3.1.1 Concepts of phishing website addresses (URLs)

Each worm is associated with a URL, which appears as a dialog box. The small fish's job is to eat all the real worms which are associated with URLs and avoid fake worms which are associated with fake URLs before the time is up (Fig. 1). This attempts to develop the severity and susceptibility of the phishing threat through the game design. If a phishing URL is correctly identified, then users are prompted to indicate which portion of the URL indicates phishing in order to determine whether or not they have understood the conceptual knowledge of the phishing URL (Fig. 2). At this time the users score will be doubled in order to encourage them to complete the game. Nevertheless, if the phishing URL is incorrectly identified, then users get real time feedback saying why their decision was wrong with an example such as "*Legitimate websites usually do not have numbers at the beginning of their URLs. For example, http://*181.57.97.116*/.www.hsbc.co.uk*". Therefore, this attempts to teach conceptual knowledge of phishing URLs within the game design context.

If the worm associated with the URL is suspicious or if it is difficult to identify, the small fish can go to the 'teacher' and request help. The big fish would then provide some tips on how to recognize bad worms. For example, "website addresses associated 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 demands help from the teacher, the time left will be reduced by certain amount (in this case by 1 minute) 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 design context. The consequences of the player's actions are shown in Table 1.

Table 1. Scoring scheme and consequences of the player's action.

	Good worm (associate with legitimate URL)	**Bad worm (associate with phishing URL)**
Player eats	Correct, gain 15 points (each attempt = 1 point)	False negative, (each attempt loses 1 minute out of 10 minutes)
Player reject	False positive, (each attempt loses 1 minute out of 10 minutes)	Correct, gain 15 points (each attempt = 1 point)

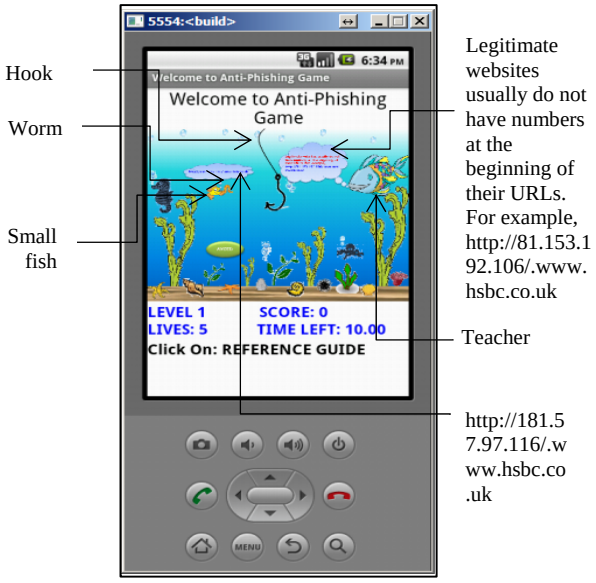

Figure 1. Main Menu of the game prototype design displayed on Google App Inventor Emulator.

Figure 2. Phishing URL dialog box: Learning conceptual knowledge of phishing URL.

3.1.2 Teaching the concept of phishing emails

Each worm is randomly generated with an email icon in the game design, so the small fish needs to eat the worm to open the email (Fig. 3 and Fig. 5). This task is done once the user clicks on the worm. At this point, a portion of an email will appear asking the user to identify whether it is legitimate or phishing email. This represents phishing attacks by developing threat perception. The reason for using a portion of an email, instead of an email, is to determine whether or not the user has understood the conceptual knowledge about phishing emails. The small fish's job is to eat all the real worms by clicking the "ACCEPT" button while avoiding fake worms by clicking the "AVOID" button (Fig. 6). If the user falsely accepted a legitimate or phishing email, they are susceptible to a phishing attack. This causes to lose one life at each attempt in the game

design. At this point, the game design emphasizes both the likelihood of phishing attack and severity caused by the attack. The different sections of an email help user to identify the legitimacy of email [9]. For example, phishing emails often contain generic salutation such as "Dear Valued Customer" or use of a trusted company logo. It could also be a statement urging immediate action or mimicking the email address (Fig.7). Each worm associated with a portion of an email may contain phishing email traps as well as legitimate ones. The phishing email traps covered in the game design include fake links or email addresses, generic salutations, statements urging immediate actions and much more.

If the portion of an email is suspicious and if it is difficult to identify, the small fish can go to 'his' teacher and demand help. The teacher could help him by giving some tips on how to identify phishing emails. For example, "phishing emails often contain a generic salutation" or "emails associated with urgent requests are generally phishing emails". Whenever the small fish demands help from the teacher, the time left will be reduced by certain amount (in this case by 1 minute) 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 design. The small fish's teacher may also help the player throughout the game until it is completed by providing some tips (Fig. 3 and Fig. 4). This can enhance the learnability of the game itself for the user.

The proposed game design is presented in different levels such as beginner, intermediate and advance. When the user moves from the beginner to advanced level, the complexity of the combination of URLs and emails is dramatically increased while considerably decreasing the time period to complete the game. Therefore, self-efficacy of preventing from phishing attacks will be addressed in the game design. Furthermore, a reference guide in the game design provides useful information on where the user can learn more about phishing attacks. The reference guide is linked to the education section of the Anti-Phishing Work Group website (APWG - http://education.apwg.org/). The overall game design is used to teach conceptual knowledge of phishing emails and URLs for home computer users to thwart phishing threats.

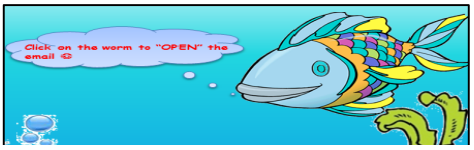

Figure 3. The small fish's teacher provides tips: Click on the worm to "OPEN" the email.

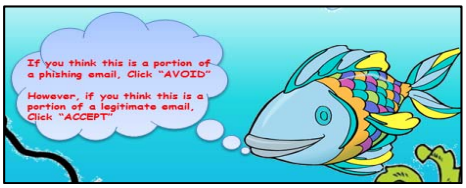

Figure 4. The small fish's teacher provides tips: If you think this is a portion of a phishing email, Click "AVOID". However, if you think this is a portion of a legitimate email, Click "ACCEPT".

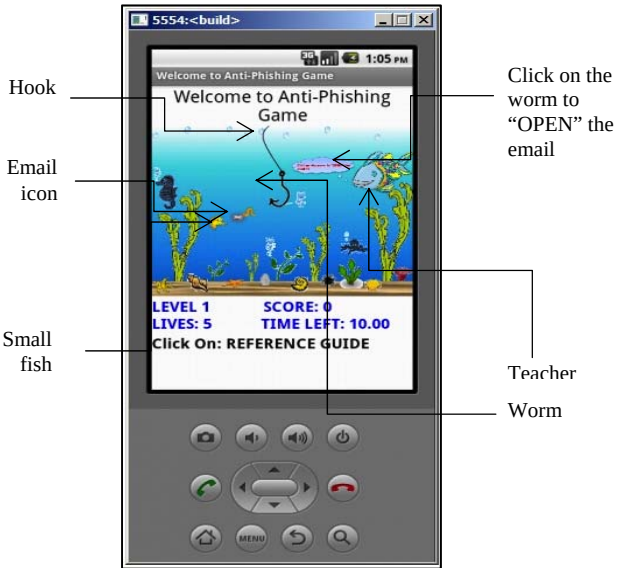

Figure 5. The small fish is waiting for open the email.

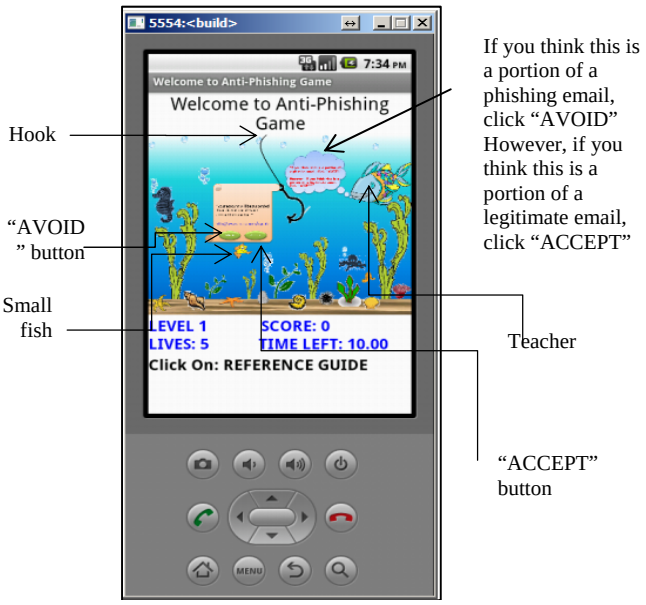

Figure 6. Learning the concepts of phishing emails

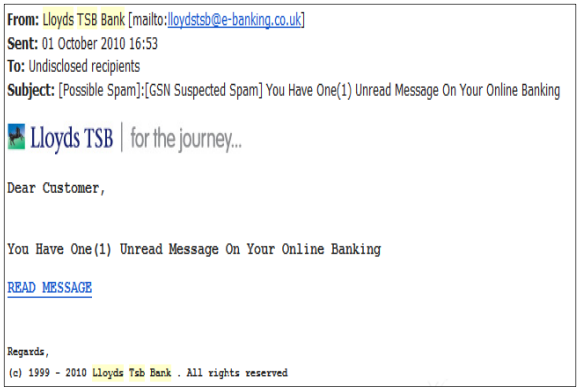

Figure 7. Different sections of a phishing email: mimicked email address, salutation, logo, urging message.

4. Conclusion

Author This research focused on designing a mobile game as an educational tool for home computer users to develop the conceptual knowledge behind phishing attacks. Previous research resulted in a mobile game to educate home computer users about phishing attacks, but it was aimed almost entirely on procedural knowledge. Conceptual knowledge helps users avoid phishing attacks more robustly, due to the necessity to teach users to identify phishing concepts in order to avoid evolving threats on new platforms, such as social media. We believe that by providing this type of education and training for home computer users, it could make a considerable contribution to enabling cyberspace to be a more secure environment.

5. References

[1] B. Schneier, “Semantic Attacks, The Third Wave of Network Attacks”, Crypto-Gram Newsletter, October 2000, Retrieved from http://www.schneier.com/crypto-gram-0010.html.(Accessed date: 02 April 2011.)

[2] B. Y. Ng and M. A. Rahim, “A Socio-Behavioral Study of Home Computer Users' Intention to Practice Security”, The Ninth Pacific Asia Conference on Information Systems, Bangkok, Thailand, 2005.

[3] C. E. Drake, J. J. Oliver and E. J. Koontz, “Mail Frontier Anatomy of a Phishing Email”, February 2006, Retrieved from http://www.mailfrontier.com/docs/MF_Phish_Anatomy.pdf.(Accessed date: 03 April 2011.)

[4] CNN. com, “A convicted hacker debunks some myths”, 2005, http://www.cnn.com/2005/TECH/internet/10/07/kevin.mitnick.cnna/index.html.(Accessed date: 04 April 2011.)

[5] H. Liang and Y. Xue, “Avoidance of Information Technology Threats: A Theoretical Perspective”, MIS Quarterly, vol. 33 (1), pp. 71-90, 2009.

[6] H. Liang and Y. Xue, “Understanding Security Behaviours in Personal Computer Usage: A Threat Avoidance Perspective”, Journal of the Association for Information Systems, vol. 11 (7), pp. 394-413, July 2010.

[7] J. O'Brien, T. Rodden, M. Rouncefield and J. Hughes, “At Home with the Technology: An Ethnographic Study of a Set-Top-Box Trial”, ACM Transactions on Computer-Human Interaction, vol. 6 (3), pp.282-308, 1999.

[8] J. S. Downs, M. Holbrook and L. F. Cranor, “Behavioural response to phishing risk”, Proceedings of the anti-phishing working groups - 2nd annual eCrime researchers summit, pp.37-44, October 2007, Pittsburgh, Pennsylvania, Retrieved from doi>10.1145/1299015.1299019.(Accessed date: 25 March 2011)

[9] K. Ponnurangam, Y. Rhee, S. Sheng, S. Hasan, A. Acquisti, L. F. Cranor and J. Hong, "Getting Users to Pay Attention to Anti-Phishing Education: Evaluation of Retention and Transfer", APWG eCrime Researchers Summit, October,4-5, Pittsburgh, PA, USA, 2007.

[10] L. James, “Phishing Exposed”, Syngress, Canada, 2005.

[11] N.A.G. Arachchilage and M. Cole, "Design a mobile game for home computer users to prevent from “phishing attacks”," Information Society (i-Society), 2011 International Conference on , vol., no., pp.485-489, 27-29 June 2011 URL:http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=5978543&isnumber=5978433. (Accessed Date: 22 December 2011)

[12] N.A.G. Arachchilage and M. Cole, "Designing a mobile game for home computer users to protect against “phishing attacks”," Intenatioal Journal for e-Learning Security (IJeLS), Volume 1, Issue 1/2, March/June 2011.

[13] P. Kumaraguru, Y. Rhee, A. Acquisti, L. F. Cranor, J. Hong and E. Nunge, “Protecting people from phishing: the design and evaluation of an embedded training email system”, Proceedings of the SIGCHI conference on Human Factors in Computing Systems, San Jose, California, USA, April - May 2007.

[14] P. Michael, The Magazine for the IT Professional, British Computer Society, The Charted Institute for IT, March 2011.

[15] Dhamija, R. and Tygar, J. D. 2005. The battle against phishing: Dynamic Security Skins. In Proceedings of the 2005 Symposiumon Usable Privacy and Security (Pittsburgh, Pennsylvania, July 06 - 08, 2005). SOUPS '05, vol. 93. ACM Press, New York,NY, 77-88. DOI= http://doi.acm.org/10.1145/1073001.1073009. (Accessed Date: 20 March 2011)

[16] R. G. Brody, E. Mulig and V. Kimball, "Phishing, pharming and identity theft", Journal of Academy of Accounting and Financial Studies, vol. 11, pp. 43-56, 2007.

[17] R. Richmond, “Hackers set up attacks on home PCs, Financial Firms: study”, September 2006, Retrieved from http://www.marketwatch.com/News/Story/Story.aspx?dist=newsfinder&siteid=google&guid=%7B92615073-95B6-452EA3B9

569BEACF91E8%7D&keyword=.(Accessed date: 27 March 2011.)

[18] S. A. Robila, J. W. Ragucci, “Don't be a phish: steps in user education”, Proceedings of the 11th annual SIGCSE conference on Innovation and technology in computer science education, 26 – 28 June 2006, Bologna, Italy, Retrieved from doi>10.1145/1140124.1140187.(Accessed date: 29 March 2011.)

[19] 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”, Proceedings of the 3rd symposium on Usable privacy and security, Pittsburgh, Pennsylvania, July 2007.

[20] Y. Zhang, S. Egelman, L. Cranor and J. Hong, Phinding Phish: Evaluating Anti-Phishing Tools. In Proceedings of the 14th Annual Network and Distributed System Security Symposium (NDSS 2007), San Diego, CA, 28 February -2 March, 2007.

[21] Z. Ye and S. Sean, Trusted Paths for Browsers, Proceedings of the 11th USENIX Security Symposium, USENIX Association. Berkeley, CA, USA, pp. 263 – 279, 2002.

[22] D. Parsons, H. Ryu and M. Cranshaw, "A Study of Design Requirements for Mobile Learning Environments", Proceedings of the Sixth IEEE International Conference on Advanced Learning Technologies, pp. 96-100, 2006

