Security Awareness Training: A Review

Melad Mohamed Al-Daeef, Nurlida Basir, Madihah Mohd Saudi

***Abstract*—Phishing is a type of social engineering cybercrimes in which, phishers try to steal users' information. Human unawareness and inattention factors are usually exploited by phishers to bypass anti-phishing systems. This impose on anti-phishing solutions to target the vulnerabilities at both of technical and non-technical layers of phishing problem. This paper reviews users' training approach as a non-technical solution to mitigate security threats in general and phishing problem in particular. Security training methods should be designed to attract users' attention in order to enhance their awareness and make them retain acquired knowledge for longer time. Training activities therefore, must consider knowledge acquisition, knowledge retention, and knowledge transfer aspects. Training in addition, should be embedded into something that users are familiar with and continually practice to make training as ongoing activity. Security training as a non-technical solution must be highly considered to complement the performance of anti-phishing technical tools and thus, improve their results.**

***Index Terms*—Phishing, user awareness, user training, embedded training.**

I. Introduction

Through the Internet, users can do a wide range of online transactions. These transactions are unfortunately at the risk of phishing which is a type of social engineering cybercrimes in which, phishers try to steal identity information. Phishing attacks are usually start by sending fake emails that contain misleading URLs that take to phishing websites. The number of phishing websites observed by Anti-Phishing Working Group APWG was increased 250% in the 1st quarter of 2016 over what was seen in the 4th quarter of 2015 [1]. Phishers are usually target anti-phishing systems through unawareness and inattention factors of Internet users. This nature of attack makes phishing a dual-layer problem that require effective solutions at both of technical and non-technical (human) layers.

Anti-phishing solutions are generally classified in two categories, technical solutions that implemented to deal with the vulnerabilities of information systems, and non-technical solutions that focus on human vulnerabilities. Researchers in many studies claim that, technical solutions alone are not enough to stop phishing attacks and they should be complemented by effective non-technical ones [2],[3],[4],[5]. Users' training approach as a non-technical solution can be relied upon to enhance users' awareness about phishing phenomenon and thus, improve the performance of the technical solutions [6],[7].

By using embedded training concept, users can acquire more knowledge, retain this knowledge for longer time, and they can transfer this knowledge into other security fields [8],[9],[10]. This study reviews users' training methods as a non-technical anti-phishing solution and highlights the advantages and limitations of reviewed training methods. It also highlights the points where anti-phishing training methods need to be improved to complement technical solutions.

The rest of this paper is organized as follows; section II discusses the phishing attacks types to show the techniques that used by phishers to steal users' identity information. Section III highlights the reasons behind the success of most phishing scenarios. Section IV shows commonly implemented strategies to defense against phishing attacks. Different definitions of security awareness are presented in section V. The importance of security awareness training and knowledge delivery methods are discussed in section VI. Conclusion paragraph of this paper has presented in section VII.

II. Types of Phishing Attacks

Phishing is a type of cybercrimes that takes many forms to get victims lured and reveal their personal information. In addition of utilizing the vulnerabilities of anti-phishing systems, phishers also exploit users' unawareness and inattention factors.

In *deceptive* form of phishing, phishers utilize the social engineering scheme where victims are usually sent simulated emails that include fake links (URLs) to take them to phishing websites. Email-based phishing trick is also used by phishers to perform *spear phishing* attacks to lure a specific group of users at a particular targeted organizations [11],[12]. *Malware-based*, also known as *exploit-based* is another form of phishing in which, more technically sophisticated tricks are used to exploit the security holes found in Internet browsers and install malicious codes or malwares on users' PCs when they click on the URLs in phishing emails [13]. *Search Engine Phishing* is another form of attacks in which, users are attracted by promoted fake products and e-service at good prices. When they carry out buying transaction, error messages are displayed to inform them that, a problem has occurred and the transaction was unsuccessful. Phishers do not have to contact targeted victims in this form of attack, the victims instead search for phishing websites that highly indexed by

Manuscript received July 02, 2016; revised July 17, 2016.

Melad Mohamed Al Daeef is a PhD Student at the Faculty of Science and Technology, Universiti Sains Islam Malaysia (USIM), Bandar Baru Nilai 71800, Negeri Sembilan Darul Khusus, Malaysia Hand phone: 0060-18250-3435; e-mail: meladmohalda@gmail.com

Dr. Nurlida Basir is a lecturer at the Faculty of Science and Technology, Universiti Sains Islam Malaysia (USIM), Bandar Baru Nilai 71800, Negeri Sembilan Darul Khusus, Malaysia e-mail: nurlida@usim.edu.my

Assoc. prof. Dr. Madihah Mohd Saudi is a lecturer at the Faculty of Science and Technology, Universiti Sains Islam Malaysia (USIM), Bandar Baru Nilai 71800, Negeri Sembilan Darul Khusus, Malaysia e-mail: madihah@usim.edu.my

ISBN: 978-988-14047-4-9
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

search engines based on some keywords [14]. VOIP, SMS, IM, Wi-phishing, and multiplayer games are also utilized as communication channels to perform phishing attacks [15].

III. Why phishing attacks success

To mitigate the bad impact of phishing, it is an important matter to highlight the reasons behind its success although the considerable defense efforts. The main reasons behind the success of phishing attacks are discussed here.

A. Anti-phishing methods such as blacklists, whitelists, and heuristics that commonly used to build anti-phishing systems still have their associated limitations that certainly impact the performance of anti-phishing systems [2],[11]. Hybrid anti-phishing systems such as client-side toolbars that combine two or more of such methods can mitigate this bad effect [16]. Phishers however still able to bypass hybrid systems by using more sophisticated techniques.

B. Emails and websites are usually classified as legitimate or phishing based on different categories of classification features that extracted from questioned emails or websites. Classification features however, might be employed even they are not enough informative or discriminative. Implementing of such imperfect features will eventually impact the quality of classification results [17]. Researchers in [18] for example, have attempted to evaluate the effectiveness of phishing classification features before they are being employed.

C. Users' inattention is another factor behind the success of many of phishing attacks. Many of anti-phishing toolbars that work at users' side are designed to warn them when an attack is detected. Such toolbars in most cases employ passive warning principles such as colored icons or tabs to indicate risk degree. Internet users do not pay enough attention to such passive warnings [7],[19],[20].

D. The lake of users' awareness about phishing is a dangerous point from which phishers target anti-phishing software systems [2],[21]. Unskilled users may do not know how phishing attacks may occur, or even they do not know about the existence of phishing at all. Unaware users do not care about the legitimacy of emails and visited websites, thus they can be easily deceived than aware users [22].

E. Phishers usually play on users' psyche factors to instill some type of urgency and fear in their minds. They always try to urge the victims to shortly update their accounts before they being suspended or terminated [23],[24].

IV. Phishing Defense Strategies

Phishing is a complicated threat that not only threatens Internet users; it threatens financial and business organizations as well. *Detective*, *preventive*, and *corrective* or *response* are the main three categories of anti-phishing solutions [25]. American Bankers Association [12] recommends to develop three anti-phishing defense strategies as following:

A. *Detective Strategies,* they refer to technical and non-technical solutions that aim to discover phishing activities before their occurrences.

B. *Preventive Strategies,* they can mean different things;
- They might refer to the techniques of reducing the possibility of users being victimized. Enhancing users' awareness can be implemented as a preventive strategy.
- Prevention might also refer to the actions of preventing phishers from launching their attacks, and hence reduce the frequency of phishing activities. In this context, law suits and penalties against attackers can be applied.

C. *Response Strategies.* Financial and business organizations should assess phishing risk and formulate well planned and executable response actions against detected phishing activities. Such actions may include reporting or taking down phishing websites and the coordination actions with law enforcement authorities.

V. Security awareness definition

Awareness is a crucial part of any information security program either at personal or organizational level. Individuals' lack of awareness may include but not limited to; browsing and hence disclosing personal information to untrusted sites, installing dangerous applications, and sharing personal information with others [26]. Security awareness programs must be formulated to influence users' behavior and understanding levels [27],[28],[29]. Security awareness has therefore received many definitions that have inferred from its required characteristics.

According to Information Security Forum (ISF) [30], "security awareness is a continual process of learning by which, trainees realize the importance of information security issues, the security level required by the organization, and individuals' security duties". In [31], security awareness defined as "a state where users in an organization are aware of and ideally committed to their security mission". Researchers in [28] have stated that, security awareness consists of two important portions; *first*, suitable and appropriate knowledge must be accurately and timely delivered to individuals; *second*, delivered knowledge should impact individuals' behavior. If one of these two portions absent, the other one therefore becomes ineffective. In [28], researchers have concisely defined security awareness as "the effort to impart the knowledge about information security to the degree that influence users' behavior, thus they conform to applied security policies".

Previous definitions have highlighted three key components of security awareness, they are; *ongoing* or *continual process*, *knowledge delivery method*, and *individuals' behavior impact*. These definitions however, have excluded an important component of knowledge acquiring process, it is the *gradualism* concept. Based on the Adaptive Control of Thought-Rational (ACT-R) theory [32], the knowledge and values are gradually acquired and learned through practice and experience. Human brain keeps statistics on the frequency, recency, and utility of knowledge components [33]. Based on that, information security awareness has defined in this paper as *the security knowledge that has been gradually acquired through a continuous and updated catchy training manner to influence trainees' behavior.*

VI. Security awareness training

ISBN: 978-988-14047-4-9
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

Aside from implemented awareness training method, the main goal of security training programs is to raise trainees' awareness level and thus, influence their security behavior. Information security was traditionally seen as a kind of service that to be provided rather than to be influenced, this have made researchers always focus only on the technical aspects of information security [34]. Although International Organization for Standardization (ISO) standard has differentiated between training and education, these two terms are interchangeably used in this paper.

A. The Importance of Security Awareness Training

Despite of claims that training approach about security does not work, there is however an evidence that, well-designed user training methods can effectively enhance awareness and security behavior [35],[36]. Users' technology-related mistakes cannot be solved by only adding more technologies, awareness training programs can be the perfect choice to alleviate the limitations of technical-based security solutions [24],[37],[38],[39]. Many researchers believe in that, security is usually seen as a secondary goal by users [34], they therefore need to be properly trained to be more aware and know how to recognize and react against the different forms of fraudulent activities [24]. Many studies such as [40] and [41] have been conducted to test the efficiency of security training approach. Although [40] experiment for example did not improve participants' ability to differentiate between phishing and legitimate emails, it however has made them more suspicious (i.e. more aware).

In [38] for example, A Security Education, Training and Awareness (SETA) was defined as an educational program that aim to reduce security breaches that caused because of the lack of employees' security awareness. SETA was designed to educate employees how to focus on security issues to protect themselves and their organization's data and network. SETA program integrates security in all tasks that employees do; from locking computer screens when they move away from their desks; to report unusual activities regarding to emails, files and staff. [39] is another study in which, researchers have proposed a framework that consider awareness training as the main proactive prevention step against Ransomware attacks. In Ransomware form of malware attacks, Internet users are victimized by hijacking and encrypting their files, and they can exchange the decryption key with attackers after making some kind of payment. The common ways in that Ransomware Trojans are installed are phishing emails and visiting websites that contain malicious programs. Security training in addition, considered as an important protection approach by security standards of International Organization for Standardization (ISO) [42], and National Institute of Standards and Technology (NIST) [43].

B. Embedded Training Concept

Anti-phishing training materials can be delivered to trainees through many channels such as emails, posters, classrooms, and games. Training process becomes more effective if training materials embedded into daily work activities [8],[37],[44]. Embedded training concept is defined as the ability to train work activities and skills by using the associated operational system including software and machine that people normally use [45]. This method provides ongoing real time training experience that motivate trainees to learn without requiring them to proactively seek out the training, or even to allocate a training timetable [9]. Embedded training differs from other traditional training concepts that may conducted in classrooms for example where trainees are provided a small chance to test acquired knowledge [15].

An effective education and training experiment should help trainees to learn new knowledge (knowledge acquisition), practice learned knowledge for a long time period (knowledge retention), and apply this knowledge into other related activities (knowledge transfer) [46]. The benefit of embedded training over other traditional training methods is that, it can help trainees to retain acquired knowledge for a long time, and hence they can transfer this knowledge into other related fields [8],[9],[10].

Results of the study conducted in [8] for example show that, participants in the embedded training condition were better in making decisions than participants who trained in the non-embedded training condition. The study in [47] has also shown that, users were able to retain acquired knowledge for at least one week when they have trained in real world experiment (embedded training).

Another examples of embedded training experiments include; training intervention method in [48] to help users correctly distinguish between phishing and legitimate websites. Training information in [48] are presented to users immediately after they mistakenly try to submit personal information to phishing websites to help them detect phishing websites and also to make training as ongoing process. Researchers in[37] have also used the embedded training concept to teach users what phishing clues to look for during the normal use of email. Since multimedia medium can make a positive effect on information retention, they have used screenshots to present training material to users. PhishGuru [35] is a cartoon system that embedded in users' mail system. Users were sent simulated phishing emails through PhishGuru system to test their vulnerability, once they fall for the attack, they presented then with training materials in a comic script form.

C. Security Training Delivery

The success of security awareness training programs relies significantly on the method by which training material were delivered to trainees [36]. Delivery method should make security as an essential attention within its targeted trainees [49]. This section gives examples of commonly used anti-phishing training methods.

- Classroom setting is one of anti-phishing training methods. Researchers in [50] have demonstrated the efficiency of class discussions and exercises to enhance trainees' awareness and thus ability to identify phishing instances. Traditional class sessions however, become ineffective method due to high cost and consumed if when trainees number is increased [47]. In addition to that, trainees need to touch and feel training materials [49], such characteristics are usually not provided in traditional class sessions.
- Posted articles and tips about phishing is another form of online training methods. Such materials are frequently

ISBN: 978-988-14047-4-9
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

published by governments and other organizations and communities such as Federal Trade Commission [51] and Anti-Phishing Working Group [25]. This method however, can help users only if they have actually read training materials. Users will tend to override such frequently seen information because they wrongly believe that they know how to protect themselves [9],[52].

- Researchers have also tried the contextual (two part) training method or spear phishing experiments as an anti-phishing training method. At the first phase of this method, a group of targeted trainees are sent simulated phishing emails to test their vulnerability. Those trainees are given anti-phishing training materials at the second phase of the experiment. In [53] for example, researchers have obtained the personal information from social networking websites for a group of Indiana University students. Those students were sent fake emails claiming originated by their friends. 72% of them have fell for the attack and revealed their university accounts' information to a simulated university website that was designed to perform the study. Another two part contextual studies were also conducted among the West Point cadets [49], and the employees at New York state office of Cyber Security & Critical Infrastructure Coordination [69]. Contextual experiments show that participants were better in avoiding being victimized by subsequent attacks. However, finding an ethical ways to conduct such training experiments is one of faced challenges, as an example, after the experiment in [53] was conducted, some students called it unethical, inappropriate, and illegal.
- Interactive games method was also used to teach users how to identify phishing emails and websites. Some examples of anti-phishing training games are given in this section.

  Anti-phishing Phil [54] shows how online games can help users identify phishing websites by teaching them where to look for phishing indications in web browsers. It also show users how to correctly arrive to legitimate sites through search engines. The game was evaluated to test users' ability to detect phishing websites before and after training experiment. Both of laboratory and real world experiments have shown that, participants who have played the game were much better in detecting phishing websites than others who had taken another type of training activities such as reading online training materials [47]. Game designers have reported that, False Positive FP (legitimate instances that incorrectly identified as phishing) rate was minimized to 14% from 30%, and False Negative FN (phishing instances that incorrectly identified as legitimate) rate was also minimized to 17% from 34%. Despite of that, 31% of subjects were unable to correctly differentiate between legitimate and phishing sites because they have misinterpret examined URLs [3],[54].

  In [55], an anti-phishing educational mobile game was designed to enhance home computer users' behavior, and educate them how to correctly identify the features of URLs and emails to detect phishing attacks.

  It is believed that, game-based training method can offer an effective alternative to traditional training methods [56] since this method can engage players (trainees) in, and catch their attention to, training experiment. Game-based training method however, lacks the knowledge transfer characteristic and demand players to gain required security knowledge before they start playing the game [57]. This method therefore cannot be relied upon as a good source of required knowledge that enhance individuals' awareness and influence their security-related behavior [28],[57].
- User's knowledge about phishing can be also tested by web-based IQ tests. Mail Frontier [58] for example has set a website containing screenshots of actual phishing and legitimate emails. These screenshots were used to test users' ability to differentiate between phishing and legitimate emails. Some of web-based IQ experiments show that, the awareness of users was eventually increased after taking the test. Researchers in [40] for example, have however concluded that, IQ test training method affects users' judgment ability and thus, increase their fear not awareness level. This conclusion was drawn based on results of testing 40 subjects who were asked to answer some questions from existing phishing IQ tests. For most participants, the number of times legitimate instances were incorrectly identified as phishing was increased from the first to the second test; subjects were more suspicious about all instances that shown in the second test.
- Sending training materials through emails is another training method to deliver useful information about phishing, social engineering, password management, and information security incidents. Such emails can effectively increase recipients' security knowledge and awareness. In general, system administrators, ISPs, or training companies are expected to generate and deliver such emails to targeted trainees. This method however, has been called as a non-embedded training method and there are some challenges that diminish its efficiency. Not all recipients for example have the ability to understand the content of such emails. In addition, as a one way communication channel, this method may not catch recipients' attention [57], many of them may discard such frequently received emails and they wrongly believe they know how to protect themselves [9],[52].

VII. Conclusion

Security awareness training is a usually overlooked factor in most of implemented information security programs. Training is a promising approach to enhance users' awareness and thus minimize the bad effect of their mistakes and misbehaviors that cannot be solved by only considering technical aspects of solutions. To be more effective, the main goal of any security training program must make users retain acquired knowledge for a long period of time, and thus make them able to transfer (use) this knowledge into other security fields. The proposed users' training methods are vary in their efficiency and implementation procedures. Some of them are designed based on embedded training concept whereas others are not. Researchers in many studies have provided strong evidence that, users can make better decisions if they have trained using an embedded training concept.

ISBN: 978-988-14047-4-9
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

This paper has highlighted the importance of awareness training approach by reviewing some of training methods that implemented in security in general, and in phishing field in particular. This paper has also introduced a new security awareness definition in which, an important component that related to knowledge acquisition process was added. This component is the gradualism concept which was overlooked by, at least, other reviewed security awareness definitions.

Due to the important role of the awareness training approach in information security field, future studies therefore, should find reliable ways in that, technical solutions are supported by training security training methods. This for example can improve users' ability to detect phishing instances before they are being victimized. Any suggested solution should be able to make users retain acquired knowledge for a long period of time, and also make them able to transfer or use this knowledge to combat other forms of Internet security threats. This can be achieved by implementing ongoing training process that tied together with users' normal work activities.

REFERENCES

[1] APWG, *Anti-Phishing Working Group, Phishing Activity Trends Report, 1th Quarter 2016.* http://docs.apwg.org/reports/apwg_trends_report_q1_2016.pdf.

[2] Wilson, C. and D. Argles. *The fight against phishing: Technology, the end user and legislation*. in *Information Society (i-Society), 2011 International Conference on*. 2011: IEEE.

[3] Kirlappos, I. and M.A. Sasse, *Security education against phishing: A modest proposal for a major rethink.* IEEE Security and Privacy Magazine, 2012. **10**(2): p. 24-32.

[4] Abawajy, J.H., K. Thatcher, and T.-h. Kim. *Investigation of stakeholders commitment to information security awareness programs*. in *Information Security and Assurance, 2008. ISA 2008. International Conference on*. 2008: IEEE.

[5] Aloul, F.A., *The Need for Effective Information Security Awareness.* Journal of Advances in Information Technology, 2012. **3**(3): p. 176-183.

[6] Mohebzada, J., et al. *Phishing in a university community: Two large scale phishing experiments*. in *Innovations in Information Technology (IIT), 2012 International Conference on*. 2012: IEEE.

[7] Ramanathan, V. and H. Wechsler, *phishGILLNET—phishing detection methodology using probabilistic latent semantic analysis, AdaBoost, and co-training.* EURASIP Journal on Information Security, 2012. **2012**(1): p. 1-22.

[8] Kumaraguru, P., et al. *Getting users to pay attention to anti-phishing education: evaluation of retention and transfer*. in *Proceedings of the anti-phishing working groups 2nd annual eCrime researchers summit*. 2007: ACM.

[9] Kumaraguru, P., et al., *Teaching Johnny not to fall for phish.* ACM Transactions on Internet Technology (TOIT), 2010. **10**(2): p. 7.

[10] Alnajim, A. and M. Munro. *An Evaluation of Users' Anti-Phishing Knowledge Retention*. in *Information Management and Engineering, 2009. ICIME'09. International Conference on*. 2009: IEEE.

[11] Almomani, A., et al., *A survey of phishing email filtering techniques.* Communications Surveys & Tutorials, IEEE, 2013. **15**(4): p. 2070-2090.

[12] American-Bankers-Associaion, *works on fraud: phishing prevention and resolution. Available at:* http://www.angelinabank.com/phishing063005.pdf. 2005.

[13] Kirda, E. and C. Kruegel. *Protecting users against phishing attacks*. in *The Computer Journal*. 2005: Citeseer.

[14] Devmane, M. and N. Rana, *Security Issues of Online Social Networks*, in *Advances in Computing, Communication, and Control*. 2013, Springer. p. 740-746.

[15] Hong, J., *The state of phishing attacks.* Communications of the ACM, 2012. **55**(1): p. 74-81.

[16] Abbasi, A. and H. Chen, *A Comparison of Tools for Detecting Fake Websites.* IEEE Computer, 2009. **42**(10): p. 78-86.

[17] Xiang, G., et al., *Cantina+: A feature-rich machine learning framework for detecting phishing web sites.* ACM Transactions on Information and System Security (TISSEC), 2011. **14**(2): p. 21.

[18] Al-Daeef, M.M., N. Basir, and M.M. Saudi. *A Method to Measure the Efficiency of Phishing Emails Detection Features*. in *Information Science and Applications (ICISA), 2014 International Conference on*. 2014: IEEE.

[19] Wu, M., R.C. Miller, and S.L. Garfinkel. *Do security toolbars actually prevent phishing attacks?* in *Proceedings of the SIGCHI conference on Human Factors in computing systems*. 2006: ACM.

[20] Dhamija, R. and J.D. Tygar. *The battle against phishing: Dynamic security skins*. in *Proceedings of the 2005 symposium on Usable privacy and security*. 2005: ACM.

[21] Khonji, M., Y. Iraqi, and A. Jones, *Phishing detection: a literature survey.* Communications Surveys & Tutorials, IEEE, 2013. **15**(4): p. 2091-2121.

[22] Dhamija, R., J.D. Tygar, and M. Hearst. *Why phishing works*. in *Proceedings of the SIGCHI conference on Human Factors in computing systems*. 2006: ACM.

[23] Yu, W.D., S. Nargundkar, and N. Tiruthani. *A phishing vulnerability analysis of web based systems*. in *Computers and Communications, 2008. ISCC 2008. IEEE Symposium on*. 2008: IEEE.

[24] Butler, R., *Investigation of phishing to develop guidelines to protect the Internet consumer's identity against attacks by phishers.* South African Journal of Information Management, 2005. **7**(3).

[25] Anti-Phishing-Working-Group, *APWG.* http://www.antiphishing.org/.

[26] Liang, H. and Y. Xue, *Understanding security behaviors in personal computer usage: A threat avoidance perspective.* Journal of the Association for Information Systems, 2010. **11**(7): p. 394-413.

[27] Wilson, M. and J. Hash, *Building an information technology security awareness and training program.* NIST Special publication, 2003. **800**: p. 50.

[28] Wolf, M., D. Haworth, and L. Pietron, *Measuring an information security awareness program.* Review of Business Information Systems (RBIS), 2011. **15**(3): p. 9-22.

[29] Okenyi, P.O. and T.J. Owens, *On the anatomy of human hacking.* Information Systems Security, 2007. **16**(6): p. 302-314.

[30] *Information Security Forum (ISF).: The Standard of Good Practice for Information Security, Security Standard.* 2007.

[31] Siponen, M.T., *A conceptual foundation for organizational information security awareness.* Information Management & Computer Security, 2000. **8**(1): p. 31-41.

[32] Anderson, J.R. and C. Schunn, *Implications of the ACT-R learning theory: No magic bullets.* Advances in instructional psychology, Educational design and cognitive science, 2000: p. 1-33.

[33] Anderson, J.R., M. Matessa, and C. Lebiere, *ACT-R: A theory of higher level cognition and its relation to visual attention.* Human-Computer Interaction, 1997. **12**(4): p. 439-462.

[34] Stephanou, A. and R. Dagada, *THE IMPACT OF INFORMATION SECURITY AWARENESS TRAINING ON INFORMATION SECURITY BEHAVIOUR: THE CASE FOR FURTHER RESEARCH.*

[35] Kumaraguru, P., et al., *School of Phish: A Real-Word Evaluation of Anti-Phishing Training (CMU-CyLab-09-002).* 2009.

[36] Abawajy, J. and T.-h. Kim, *Performance analysis of cyber security awareness delivery methods*, in *Security technology, disaster recovery and business continuity*. 2010, Springer. p. 142-148.

[37] Kumaraguru, P., et al. *Protecting people from phishing: the design and evaluation of an embedded training email system*. in *Proceedings of the SIGCHI conference on Human factors in computing systems*. 2007: ACM.

[38] Hight, S.D., *The importance of a security, education, training and awareness program, November 2005*.

[39] Luo, X. and Q. Liao, *Awareness education as the key to Ransomware prevention.* Information Systems Security, 2007. **16**(4): p. 195-202.

[40] Anandpara, V., et al., *Phishing IQ tests measure fear, not ability*, in *Financial Cryptography and Data Security*. 2007, Springer. p. 362-366.

[41] Jackson, C., et al., *An evaluation of extended validation and picture-in-picture phishing attacks*, in *Financial Cryptography and Data Security*. 2007, Springer. p. 281-293.

[42] *ISO/IEC . ISO/IEC 27001:2005 - . Tech. rep., International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).* 2005.

[43] NIST, *Nist special publication 800-12, An introduction to computer security: the NIST handbook*. 1995: DIANE Publishing.

[44] Anderson, J.R., L.M. Reder, and H.A. Simon, *Situated learning and education.* Educational researcher, 1996. **25**(4): p. 5-11.

[45] Kirkley, J., et al. *Problem-based embedded training: An instructional methodology for embedded training using mixed and virtual reality*

ISBN: 978-988-14047-4-9
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)

technologies. in *Interservice/Industry Training, Simulation, and Education Conference (I/ITSEC)*. 2003.
[46] Schmidt, R.A. and R.A. Bjork, *New conceptualizations of practice: Common principles in three paradigms suggest new concepts for training.* Psychological science, 1992. **3**(4): p. 207-217.
[47] Kumaraguru, P., et al. *Lessons from a real world evaluation of anti-phishing training*. in *eCrime Researchers Summit, 2008*. 2008: IEEE.
[48] Alnajim, A. and M. Munro. *An anti-phishing approach that uses training intervention for phishing websites detection*. in *Information Technology: New Generations, 2009. ITNG'09. Sixth International Conference on*. 2009: IEEE.
[49] Ferguson, A.J., *Fostering e-mail security awareness: The West Point carronade.* EDUCASE Quarterly, 2005. **28**(1): p. 54-57.
[50] Robila, S.A. and J.W. Ragucci, *Don't be a phish: steps in user education.* ACM SIGCSE Bulletin, 2006. **38**(3): p. 237-241.
[51] *Federal Trade Commission. "Phishing" http://www.consumer.ftc.gov/articles/0003-phishing Accessed 09/01/2015.* .
[52] Alnajim, A. and M. Munro. *An evaluation of users' tips effectiveness for Phishing websites detection*. in *Digital Information Management, 2008. ICDIM 2008. Third International Conference on*. 2008: IEEE.
[53] Jagatic, T.N., et al., *Social phishing.* Communications of the ACM, 2007. **50**(10): p. 94-100.
[54] Sheng, S., et al. *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*. 2007: ACM.
[55] Arachchilage, N.A.G. and M. Cole. *Design a mobile game for home computer users to prevent from "phishing attacks"*. in *Information Society (i-Society), 2011 International Conference on*. 2011: IEEE.
[56] Cone, B.D., et al., *Cyber Security Training and Awareness Through Game Play*. 2006: Springer.
[57] Khan, B., et al., *Effectiveness of information security awareness methods based on psychological theories.* African Journal of Business Management, 2011. **5**(26): p. 10862-10868.
[58] Mail-Frontier, *Phishing IQ. http://survey.mailfrontier.com/survey/quiztest.html*.

ISBN: 978-988-14047-4-9
ISSN: 2078-0958 (Print); ISSN: 2078-0966 (Online)