An Enterprise Anti-phishing Framework

Edwin Frauenstein, Rossouw Solms

Proceedings of the 7th World Conference on Information Security Education
9-10 June 2011, Lucerne, Switzerland

An Enterprise Anti-Phishing Framework

Edwin Donald Frauenstein[1] and Rossouw von Solms[2]

[1]Walter Sisulu University, School of Computing, East London, South Africa
[2]Nelson Mandela Metropolitan University, School of ICT, Port Elizabeth, South Africa
{efrauenstein@wsu.ac.za[1], rossouw@nmmu.ac.za[2]}

Abstract. The objective of this paper is to report back on an organizational framework, which consisted of human, organization and technology (HOT) dimensions in holistically addressing aspects associated with phishing. Most anti-phishing literature studied either focused on technical controls or education in isolation however; education is core to all aspects in the above-mentioned framework. It is evident, from literature, that little work has been conducted on anti-phishing preventative measures in the context of organizations but rather from a personal user-level. In the framework, the emphasis is placed on the human factors in addressing phishing attacks.

Keywords: Information Security, social engineering, human factors, phishing, email scams, spam, spoofed-websites

1 Introduction

It is evident that as more organizations provide greater online access to their customers, phishers are successfully using social engineering techniques and technology advantageously to steal personal information and conduct identity theft on a global scale [20]. Organizations financial information is at risk, because most information-workers are vulnerable to social engineering techniques as the organizations possess financial information [29]. Fraudulent emails, such as phishing, can harm their victims as well as organizations resulting in financial losses, damaged reputation [27] and identity theft. Given a predicted increase in the tools available to fight phishing, it is expected that future attacks will continue to be more refined in targeting users i.e. spear phishing [24] incorporating greater elements of context to become more effective and thus more dangerous for society. Hence, by understanding the tools and technologies that phishers use, organizations, users and their customers can take a proactive approach in defending themselves against future phishing attacks [20]. Although this paper presents a holistic framework which requires all dimensions to be of key importance however, education is indeed a major component of protection against phishing. Thus, the objective of this paper is to emphasis how education, awareness and training are required to effectively strengthen the dependencies between the dimensions in the framework. The rest of the paper is

structured as follows: In Section 2, we give a background of phishing and explain its effectiveness. In Section 3, we illustrate the need for a holistic framework. In Section 4, we demonstrate the anti-phishing framework focusing on human factors. Finally, conclusions are drawn in Section 5.

2 Phishing Explained

"Phishing" is a hacker's term that originated from fraudsters whom are "fishing" for confidential information, mostly conducted through using fake emails and spoofed websites acting as the "bait", and the victim's accounts as the netted "phish" [27]. Phishing is a component of social engineering through which an individual attempts to solicit and steal confidential information from a user or employee by masquerading as a legitimate entity, usually from well-known financial or e-commerce institutions [27] as the primary of objective is to fraudulently obtain money. PayPal™, eBay™, American Online™, ABSA™, Standard Bank™, Google™, Microsoft and the South African Revenue Services are a few popular cases of organizations, and its clients, that have financially been affected through phishing attacks. Although most cases are financial related, phishing includes unauthorized access to all types of data e.g. social security number. Besides email, there are a number of other phishing variations such as spear phishing, wi-phishing, vishing, baiting, whaling and pharming. Phishing techniques have become more sophisticated [27], making use of a range of modern technologies such as: Internet Relay Chat (IRC), instant messengers (IM's), social networking sites (e.g. Facebook, MySpace) [10],[17],[19] and Trojan horse [6],[27]. The effectiveness of using social engineering techniques do not require much prior technical knowledge or education into hacking information systems; instead human emotion, deceit and manipulation are tools used to trick victims into giving up their personal information.

From the description of phishing above, typically five main processes are used to carry out a phishing attack:

Planning: Phisher determines who and how to attack and the information to be obtained from the victim. According to Orgill [21], social engineering attacks usually entail two facets namely: the physical aspect (e.g. workplace, online) and the psychological aspect or a combination using both aspects to gain desired information.

Email Design: The illusion based by email appearance (e.g. email address structure, subject header and content), is made to appear more legitimate by using institution logos, terminology etc. to create authenticity in the mind of the victim.

Fabricated Story: Is used to gain the victims attention, supposedly in their best interest, that a problem exists e.g. customer accounts has been hijacked. The email can also perceive to have a friendly tone e.g. thanking you for your co-operation. Using reverse social engineering, before the problem is resolved, the target feels indebted to the attacker.

Threatening Tone or Consequence: The user is lured by the fake warning and enticed to click on a hyperlink which is usually disguised as text or an image e.g. Click here for verification. The tone, together with reverse psychology, is used e.g.

the user fears that if they choose not to verify, consequently result in their account being automatically deleted. Ironically, it is "human nature" not to want any further undesired consequences or hassles e.g. renewing accounts etc.

Spoofed-Website: After the user selects/clicks the hyperlink embedded within the email message, they are directed to a spoofed-website which also appears authentic and legitimate in design, and subsequently the victims personal details are captured unsuspectingly.

3 The Need for a Holistic Anti-Phishing Framework

Organizations are at risk caused through their employees' actions and behavior [28]. If human behavior could be understood, one may suitably address why humans fall for victim to phishing emails [1],[5]. According to Hinson [13], it can be argued that technical flaws themselves are the product of human errors. Even so, companies concerned with information and data security are increasingly dedicating more *technological* resources to evaluate and protect their information systems [13] thus ignoring employees as the source of their most prevalent exposure. It is often easier for attackers to exploit human and social weaknesses of the defences than to defeat the technological countermeasures [18]. This is also evident in anti-phishing literature as most research focused on technical solutions such as: developing browser toolbars/plug-ins [23] preventative measures, characteristics and email structure [6],[20],[22], algorithms for detecting, identifying and measuring phishing emails and sites [8],[11],[32] and evaluating the effectiveness of web browser toolbar warnings/indicators [4],[7],[12],[31]. Many employees cannot identify the difference between a genuine and a spoofed website [4],[21]. Furthermore, many users are too preoccupied with their primary work duties that they hardly remember to pay attention for web browser security indicators [19]. Information security is far more than applying a range of physical and technical controls [13] and technically knowledgeable specialists often make the mistake of believing that technical measures succeed in protecting them and average consumers [14]. Social engineering attacks and lack of compliance of organizational security policies are increasingly cited as security concerns. Technical solutions are only as good as the people that use and operate them because information security is a multi-dimensional issue and only be achieved if a holistic approach is taken [3].

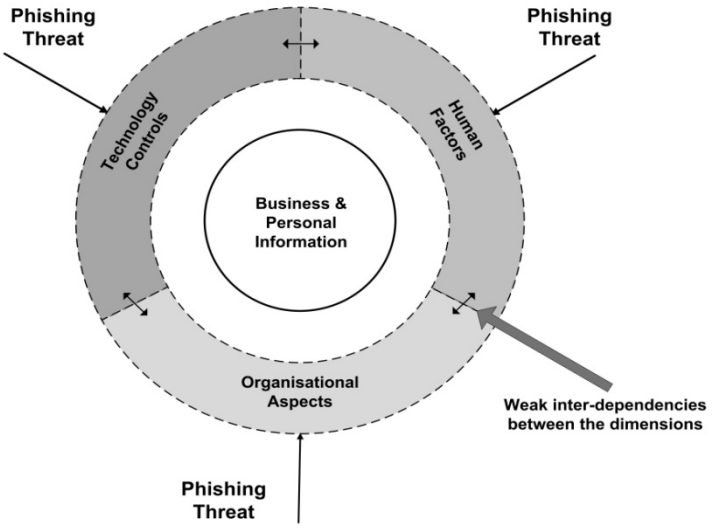

Fig. 1. Organizational dimensions targeted by phishing

Generally information security threats exploit human behavior and thus, in an organizational context, require a framework consisting of human, organizational and technological dimensions (HOT) to address against such threats [9]. Illustrated in Fig 1, HOT dimensions are operating in isolation of one another *(dotted lines)*, caused from limited communication and interaction between each of them thus forming only a 'single layer' oriented defense. As a result, if one of the dimensions is weakened, phishing attacks may proliferate compromising the other dimensions respectively. Ideally, it is suitable to move towards an 'in-depth' defense oriented model (see Fig. 2), thus allowing several barriers to serve a defense.

4 Anti-Phishing Framework: Phishing for a Solution

Technology controls have proven to be inadequate in protecting against phishing especially when applied in isolation of other organizational aspects. While technology is important, organizational and human factors also form a crucial role in achieving information security [1]. Understanding of how different human, organizational, and technological elements interplay could explain how different factors lead to sources of security breaches and vulnerabilities within organizations [15],[30]. Since each dimension has human involvement, even if the organizational dimension is added, protection may not be sufficient as both the organizational and technology dimensions depend on the H dimension. In the organizational dimension, best practices, policies, procedures and international standards (e.g. ISO 27002, King III, COBIT 4.0); fully depend on humans obeying them. Furthermore, they need to be in place to guide the other dimensions. Technology dimensions would typically involve any technical controls such as: anti-phishing browser plug-ins, anti-virus software, spam filters, web

browsers, network firewalls, etc. and is dependent on humans to follow the procedures to ensure the technical controls are functioning and applied correctly. The human dimension calls for effective *awareness*, *education* and *training* to assist in strengthening the 'human firewall' and to ideally cultivate information security behavior in the organization. Of these dimensions, the human dimension is the area that phishing exposes the most and as a result, compromises the technology and organizational dimensions. Thus, there is a need for the education element to be present in *all* of the above-mentioned dimensions to ensure that all HOT dimensions are functioning optimally. In doing so, this should provide for adequate overall risk mitigation against phishing attacks (see Fig.2). Further research will validate these findings through an expert review.

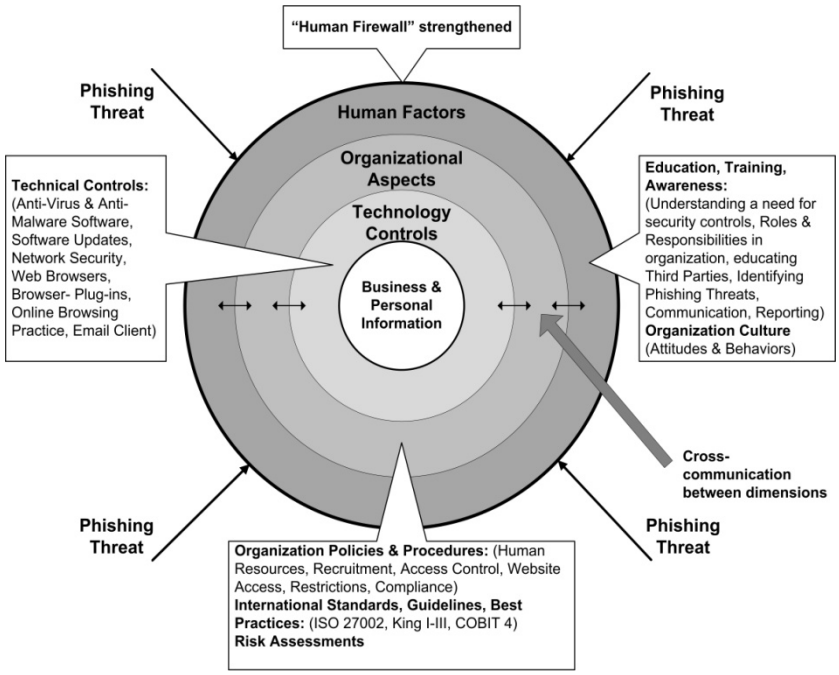

Fig. 2. Aspects in an organization, holistically related to an anti-phishing framework

Illustrated in Fig 2, continual communication *(concentric circles & arrows)* between the HOT dimensions serves a stronger defense. The human dimension is the entry point for phishing attacks and the common link (the glue) which influences all the other dimensions. It requires education to strengthen the interdependencies between the other areas e.g. staff must be knowledgeable enough of policies and technical aspects to ensure that operational procedures are obeyed and implemented correctly. The following section focuses on the components required to address the human factor dimension.

Information Security Management & Culture: Information security management requires, as a minimum, participation by all employees, shareholders, suppliers, third parties, customers or other external parties [25]. It is the responsibility of all employees to protect information thus defending the reputation and financial well-being of the business [2]. Effective interactions and communications are required to reach a mutual understanding about security risks among different stakeholders [30]. An information security culture needs to be adopted to ensure that information security becomes a natural aspect in the daily practice of every employee.

Educate Staff in Recognizing Phishing Emails and other Online Threats: Staff security education and training is one of the most important aspects of an organizations security posture and perhaps the greatest non-technical measure available and cost-effective solution for human factors and security [2]. Security topics and requirements need to be integrated into normal business behaviour, through clear policy and staff education [2]. Through a regular and comprehensive user education programme, staff can resist and be made more aware of the design (e.g. the address bar, SSL icon, web browser warning indicators, fake websites), activities and dangers involved in a phishing attack [14],[16],[26] and to report such attacks. This is substantiated by Ohaya [19] that many users do not have the underlying knowledge of how operating systems, e-mails and websites work as employees cannot tell the difference between a genuine and spoofed-website. In some cases, users frequently ignore phishing warning messages from anti-phishing tools [7],[19],[31]. For effectiveness, the training could have some incentive, fun (e.g. gameplay [26]) or humour to gain participation from staff. An added benefit, through training, allows employees to also learn other current and future threats of information security aspects e.g. scams, viruses instead of phishing attacks alone especially since attack methods are evolving. Third parties may also require education equivalent with full time employees however, effective education may prove difficult in outsourced environments where providers are growing rapidly [2]. It is essential for all employees to be an above-average computer user, especially in using email and internet, as it exposes the user and organisation to other potential threats. This requirement can be enforced in the recruitment policy (*Organisation Aspects*).

Awareness Programmes: According to ISO/IEC 27002 [25], critical success factors, based on experience, have shown that information security awareness is important. Awareness programmes should aim to enhance levels of trust between employer and employee by developing an understanding of the reasons for the security policies and controls that have been applied, as it will help staff be more aware of the issues [3] thus reducing the likelihood of accidental breaches and increase the probability of malicious activity being detected and reported. Staff needs to understand the implications of not obeying such policies.

Staff Lack in Security Behaviour: Unacceptable, non-malicious behaviour by staff should be taken seriously. Organisation policies can ensure that employees cannot plead ignorance to the rules as many insider problems stem from ignorance rather than malicious motivation [2]. However, mere accidents can potentially cause large implications e.g. social networking sites are a playground for social engineers [10] thus, if staff are spending excessive time on social network sites during office hours, this may put the organisations reputation and financial well-being at risk.

Technical staff must be educated in their duties and define proper technical procedures and apply the relevant technological controls to implement those procedures e.g. prevent users from accessing risky sites.

Monitoring: Some organisations emphasise that monitoring can benefit staff where employees are reassured that the organisation is safeguarded against confidential leaks and hence possible damage to its reputation or financial loss.

5 Conclusion

It has been established that HOT dimensions in an organization require strengthening to address phishing [9]. Human factors have been mentioned to be the greatest risk and as such require the most focus. Much research has been placed either on education, training and awareness [14],[16],[21],[26] or technical controls. Although each HOT dimension has its own weaknesses or vulnerabilities, as all encompass some human involvement, education can close the gap between all the dimensions (e.g. should the technical controls fail; humans can be aware and knowledgeable in addressing a phishing attack) thus resulting in a multi-level defense model.

References

1. Beznosov, K. & Beznosova, O.: On the imbalance of the security problem space and its expected consequences. Information Management & Computer Security, pp.420--431.15, Emerald (2007)
2. Cobb, M.: Preventing phishing attacks: Enterprise best practices. SearchSecurity.co.uk. (2010)
3. Colwill, C.:Human factors in information security: The insider threat - Who can you trust these days? Information Security Technical Report, 30**,** pp.1--11. (2010)
4. Dhamija, R., Tygar, J. D. & Hearst, M.: Why phishing works. In: SIGCHI conference on Human Factors in computing systems, pp. 581--590. Montreal,Canada: ACM.(2006)
5. Downs, J. S., Holbrook, M. & Cranor, L. F.: Behavioral response to phishing risk. In: anti-phishing working groups 2nd annual eCrime researchers summit, pp.37--44. Pittsburgh, Pennsylvania: ACM. (2007)
6. Drake, C. E., Oliver, J. J. & Koontz, E. J.: Anatomy of a Phishing Email. Conference on Email and Anti-Spam (CEAS). Citeseer. (2004)
7. Egelman, S., Cranor, L. F. & Hong, J.: You've been warned: an empirical study of the effectiveness of web browser phishing warnings. In:26th annual SIGCHI conference on Human factors in computing systems, pp. 106--1074. Florence, Italy: ACM (2008)
8. Fette, I., Sadeh, N. & Tomasic, A.: Learning to detect phishing emails. In: 16th international conference on World Wide Web, pp. 649--656. Banff, Alberta, Canada: ACM (2007)
9. Frauenstein, E. D. & von Solms, R.: Phishing: How an organisation can protect itself. In: Information Security South Africa, pp. 253--268. 6-8 July 2009 Johannesburg, South Africa (2009)
10. Frauenstein, E. D. & von Solms, R.: The Wild Wide West of Social Networking Sites. South African Information Security Multi-Conference, pp. 74--88. 17-18 May 2010 Port Elizabeth, South Africa (2010)

11. Garera, S., Provos, N., Chew, M. & Rubin, A. D.: A framework for detection and measurement of phishing attacks. In: 2007 ACM workshop on Recurring malcode, pp. 1--8. Alexandria, Virginia, USA: ACM (2007)
12. Herzberg, A. & Jbara, A.: Security and identification indicators for browsers against spoofing and phishing attacks. ACM Trans. Internet Technol., 8**,** pp. 1--36. (2008)
13. Hinson, G.: Human factors in information security. http://www.infosecwriters.com/text_resources/pdf/human_factors.pdf. (2003)
14. Jakobsson, M.: The Human Factor in Phishing. Privacy & Security of Consumer Information. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.68.8721&rep=rep1&type=pdf.(2007)
15. Kraemer, S., Carayon, P. & Clem J.: Human and organizational factors in computer and information security:Pathways to vulnerabilities. Computers & Security, 28, pp. 509--520. (2009)
16. Kumaraguru, P., Sheng, S., Acquisti, A., Cranor, L. F. & Hong, J.: Teaching Johnny not to fall for phish. ACM Transactions on Internet Technology, pp. 1--31. 10, ACM (2010)
17. Leavitt, N.: Instant Messaging: A new target for hackers, pp. 20--33. IEEE Press (2005)
18. Mitnick, K. D., Simon, W. L. & Wozniack, S.: The Art of Deception: Controlling the Human Element of Security, New York, Wiley (2002)
19. Ohaya, C.: Managing phishing threats in an organization. In: 3rd annual conference on Information security curriculum development, pp. 159--161.Kennesaw, Georgia, ACM (2006)
20. Ollman, G.: The Phishing Guide (white paper), http://www.ngssoftware.com/papers/NISR-WP-Phishing.pdf.(2008)
21. Orgill, G. L., Romney, G. W., Bailey, M. G. & Orgill, P. M.: The urgency for effective user privacy-education to counter social engineering attacks on secure computer systems. In: 5th conference on IT education, pp. 177--181. Salt Lake City, UT, USA: ACM (2004)
22. Patel, D. & Luo, X.: Take a close look at phishing. In: 4th annual conference on Information security curriculum development, pp. 1--4. Kennesaw, Georgia:. ACM (2007)
23. Raffetseder, T., Kirda, E. & Kruegel, C.: Building Anti-Phishing Browser Plug-Ins: An Experience Report. In: 3rd International Workshop on Software Engineering for Secure Systems. IEEE Computer Society (2007)
24. Robila, S. A. & Ragucci, J. W.: Don't be a phish: steps in user education. In: 11th annual SIGCSE conference on Innovation and technology in computer science education. pp. 237--241. Bologna, Italy: ACM (2006)
25. SANS, Information technology-Security techniques-Code of practice for information security management. ISO/IEC 27002:2005. Standards South Africa.(2008)
26. Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L. F., Hong, J. & Nunge, E.: Anti-Phishing Phil: the design and evaluation of a game that teaches people not to fall for phish. In: 3rd symposium on Usable privacy and security, pp. 88--99. Pittsburgh, Pennsylvania: ACM (2007)
27. Sophos, Phishing and the threat to corporate networks (white paper).: http://www.sophos.com/whitepapers/sophos-phishing-wpuk.pdf.(2005)
28. Thomson, K.-L., von Solms, R. & Louw, L.: Cultivating an organizational information security culture. Computer Fraud & Security. (2006)
29. von Solms, S. H. & von Solms, R.: Information Security Governance, New York, Springer. (2009)
30. Werlinger, R., Hawkey, K. & Beznosov, K.: Human, Organizational and Technological Challenges of Implementing IT Security in Organizations. In: Human Aspects of Information Security and Assurance, pp. 35--48. Plymouth, England. (2008)

31.Wu, M., Miller, R. C. & Garfinkel, S. L.: Do security toolbars actually prevent phishing attacks? In: SIGCHI conference on Human Factors in computing systems, pp. 601--610. Montreal, Quebec, Canada, ACM (2006)
32.Zhang, Y., Hong, J. I. & Cranor, L. F.: Cantina: a content-based approach to detecting phishing web sites. In: 16th international conference on World Wide Web. pp.639--648. Banff, Alberta, Canada:. ACM (2007)