# Using Theories and Best Practices to Bridge the Phishing Gap

E.D Frauenstein and R. von Solms

Nelson Mandela Metropolitan University, School of ICT, Port Elizabeth, South Africa
e-mail: efrauenstein@wsu.ac.za[1] and rossouw@nmmu.ac.za[2]

## Abstract

Phishing is a mounting security problem that organisations and users continue to face. Organisations generally apply a single-layer level of defence against information security threats, which includes phishing. This single-layer level of defence is certainly not adequate against modern-day phishing attacks. It is essential for organisations to implement a holistic approach, while considering human factors, organisational aspects and technological controls to combat phishing threats. However, in each of these three elements, weaknesses arise as each is linked by means of human involvement. As a result, this approach creates a gap for successful phishing attacks to potentially compromise these elements. This paper suggests possible linkages to cover the 'gaps' between each of these elements. More understanding is necessary on how these linkages can be managed more appropriately. As such, this paper introduces possible theories and best practices which can be used to understand and address each of these linkages and therefore attempts to bridge the phishing gap by strengthening the human element.

## Keywords

Phishing, social engineering, human factors, information security, agency theory, Technology Acceptance Model. COBIT 4.1

## 1. Introduction

We live in the information age where users are able to access and share information freely by using both computers and mobile devices. Although this has been made possible by the Internet, it poses security risks as attempts are made to use this same Internet environment in order to compromise information. Accordingly, there is an urgent need for users and organisations to protect their information resources from agents presenting a security threat. Apart from dedicating resources, organisations typically spend large amounts of money as well to improve their technological defences against general security threats. However, the agents posing these threats are adopting social engineering (SE) techniques in order to bypass the technical measures which organisations are putting in place. SE techniques are often effective because they target human behaviour; something which the majority of researchers believe is a far easier alternative than hacking information systems. Typically, phishing involves a fraudster (referred to as a phisher) who uses SE techniques in the context of an email message in order to steal confidential information from a user by imitating a legitimate entity (Kumaraguru *et al.* 2007). Most of the organisations cited in such phishing emails are well-known financial institutions. Using email is the most effective phishing device because the email message may be created to appear authentic through the use of the corporate logos and terminology distinctive of the institution from which the email is purported to originate. Typically, phishers use a fabricated story to convince their victims either to resolve a particular problem or to claim a substantial prize. The user is usually also required to complete this process by clicking on a hyperlink contained within the email. This hyperlink then typically directs the user to a spoofed website which requires the victim to log in using personal information (e.g. username, password, account number). The user believes that the spoofed website is genuine because it looks almost identical to the legitimate website. However, the user is unaware of the fact that the spoofed website records his/her personal information which will then be used towards the phisher's own ends.

A cyber security study conducted by Deloitte revealed that chief information security officers (CISOs) are of the opinion that phishing and pharming currently pose the highest cyber security threat to their organisations (Deloitte, 2012). Organisations and their customers have lost millions of dollars as a result of phishing. In view of the fact that there are no boundaries to the Internet, phishing may affect all users who are connected to the Internet. The power of phishing lies in its ability to circumvent technological defences because it exploits human behaviour and knowledge. Dhamija *et al.* (2006) believe that users generally have great difficulty in distinguishing between legitimate websites and spoofed websites. However, despite this, organisations continue to focus primarily on securing their computer systems using technological controls and, thus, neglecting the human element. Within an organisational context, Frauenstein and Von Solms (2009) pointed out that there are a number of areas which phishers attack and attempt to exploit. These areas or elements include; human factors, organisational aspects and technological controls (HOT). Ironically, these same areas serve simultaneously as security measures against phishing attacks. In the literature studied, the main areas of HOT are often treated as separate or disjoint entities. Furthermore, these three elements mentioned above are characterised by gaps which arise resulting from human involvement (Frauenstein and Von Solms, 2011). Phishers target these gaps. This paper proposes possible 'linkages' between these elements. By strengthening the human element in each of these elements and the gap between them, an integrated approach can be formed which will ultimately result in a holistic anti-phishing framework.

## 2. Using an Integrated HOT Approach to Address Phishing

Beznosov and Beznosova (2007) state "public research related to computer security has been overwhelmingly focused on technological aspects, leaving human and social elements mostly uncharted". The literature also recognises that technology is not the only way to manage general information security related threats. Subsequently, human factors became another important focus for information security research. Furthermore, to understand why users behave and react in certain ways when presented with difficult situations, human psychology (Jakobsson, 2007; Schneier, 2008; West, 2008), human-computer interaction, user security awareness (Thomson and Von Solms, 1998), attitudes and behaviour (Downs *et al.* 2007), and organisational culture (Cabrera *et al.* 2001; Schlienger and Teufel, 2003; Thomson *et* *al*. 2006) are all distinct areas of interest in the area of human factors. Cabrera *et al.* (2001) emphasise that technology and people are only two of the several subsystems that function within the organisation. They suggest that in order to understand the interconnections between technology and people, a broader scope which describes the relationships between the two and other important subsystems needs to be employed. Besides technology, Werlinger *et al.* (2008) see a need to understand the impact of human and organisational factors. They state that few researchers have provided a comprehensive integrated overview of the challenges faced by security practitioners. Furthermore, they add that "a better understanding of how different human, organisational and technological elements interplay could explain how different factors lead to security breaches and vulnerabilities within an organisation". Besnosov and Beznosova (2007) recommend that future research should focus on examining the *relationship* between organisational processes and behaviour in the effectiveness of security defences. In their research, Cabrera *et al.* (2001) reveal that an integrative model will help both administrators and technology designers to understand and manage the interconnections between technology and the other human and organisational aspects of their business. Furthermore, they state that it is important to pay special attention to the factors that determine the behaviour of people in a particular organisation. Moreover, they maintain that organisational culture needs to be understood as it will describe factors that influence human behaviour. This would seem to support the need to explore the factors that influence these relationships.

In this paper, the 'integrated approach' consists of merging three main elements, namely, human factors, organisational aspects and technological controls (HOT). Since each element has its own inherent weaknesses, even when an element is linked to another element (e.g. H+T), the gap for phishers to exploit is not eliminated. As pointed out by Werlinger *et al.* (2008), these gaps become more apparent if elements are interrelated because of these relationships. Some sources discuss adopting an approach whereby all HOT elements are included and, therefore, some studies have already partly integrated some of the elements. However, it would also seem from the literature studied that there are challenges using this approach. An understanding of how to integrate these elements is necessary, as failure to achieve this could result in one relationship being compromised and thus may have an undesired effect on other elements.

## 3. A Need to Bridge the Phishing Gap

This section aims to further explore the links between HOT elements by using problem-based scenarios. At the same time, this section also points out the gaps between each of these relationships. Understanding which relationships depend on one another will help establish which of the main HOT relationships require strengthening.

Scenario A: John receives an email from his banking institution. The email warns John that the bank's customers may be subject to fraudulent activities. Therefore, he is requested to verify his banking details to validate his account. The email provides a hyperlink which will direct him to the bank's website in order to complete this verification process.

In this scenario, John will have to know how to discern phishing emails from legitimate emails. Accordingly, this knowledge will determine his actions and behaviour in reaction to the email. In this scenario, the technological controls had failed, as the phishing email reached John, consequently exposing the human factor element, and thus making John vulnerable. Alternatively, if John had not received the phishing email, then the technological controls might have performed their role adequately. In this scenario, John could make effective use of technological tools such as an anti-virus program and/or features of the email client. If he could correctly identify the phishing email, then he could use the email client function to mark the email as spam, possibly preventing such emails from reaching him again in the future. John could also identify warnings from his web browser whether he is active on a spoofed-website. In these instances, only a single-layer defence is present, that is, either technological controls or human factors. Therefore, it can be established that in Scenario A, **human** (H) and **technological** (T) elements are linked (HT) and require further strengthening.

Scenario B: John manages to find time during working hours to communicate with his friends on his office computer terminal using social networking websites and other applications. From his computer terminal, he also manages to download software, games, movies, wallpapers and music, as he does not have an Internet connection at home.

Phishers make use of a variety of technologies and techniques to trick their victims and John may not be aware that phishing is not limited to the use of emails. In Scenario B, it would seem that John disregards any security risks he might pose to the organisation from his actions. Through social networking websites, John may have clicked on hyperlinks, supposedly sent from his online friends, thereby downloading a virus or having his account hijacked. John is abusing organisational resources by using its Internet service for his personal interests. He is also abusing organisational time, as he is not carrying out his work-related tasks. John is being paid to perform his duties at work and not for any personal activities. Activities, such as downloading games, could potentially expose the organisation to viruses or Trojans, which may originate from phishers. A control mechanism related to Scenario B, could be organisational policies and procedures that strictly manage the use of technology by employees; for example, an Internet usage policy. Weak policies could result in employees bringing in their own technology from home, further creating new opportunities for phishers and other threats. Policies and procedures can also help ensure that John understands what encompasses acceptable and unacceptable behaviour in the workplace. John should be aware of the risks that security threats pose to him personally, as well as be technically knowledgeable about using websites, hyperlinks, email clients, software and so on. In Scenario B, it is evident that there is a clear gap between John's needs and what the organisation expects and requires from John. In this instance, the main links that can be compromised by John's actions are the **human** (H) and **organisational** (O) elements.

<u>Scenario C:</u> The organisation has very slow Internet connection and sometimes no Internet at all. As a result, staff often blames the organisation for not completing tasks on time. Moreover, the computer hardware and software are outdated and the organisation has no clearly defined policies or procedures describing the acceptable use of software or placing any restrictions on its use. In addition, individuals do not require authorisation to enter the work premises. Although staff security training workshops are offered, staff members do not participate and generally exempt themselves from such training.

In Scenario C, it is evident, that, from a technological perspective, the organisation is not providing a suitable service. It should ensure that technical staff apply technological controls such as network firewalls and anti-virus programs, and ensure that they are updated regularly and managed correctly. The organisation could restrict users (employees) from accessing social networking websites from their workstations during work time or even permanently by implementing technological controls such as firewalls and other authentication measures. The organisation is not implementing good practice in that it does not use technology to carry out business functions correctly, accurately and efficiently. As a result, opportunities may be created for phishers to expose any weaknesses inherent in the systems. Outdated hardware and software, viruses (perhaps originating from phishers) are able to penetrate the organisation's weakened information system and compromise its information and data. Moreover, since this organisation has no access control measures in place, any unauthorised person may enter the premises posing as an employee or customer. This imposter could be a social engineer (i.e. phisher) intent on analysing any physical, technical and behavioural weaknesses in the system. Consequently this information could be used to plot a phishing attack on the organisation. From this scenario it is evident that there is a gap between the **organisational** (O) and **technological** (T) elements.

In all three scenarios the human element was targeted most frequently, even though other controls played a role. Unfortunately, organisations may therefore be of the opinion that, since phishing penetrates technological defences, technology requires the most improvement. However, phishers most frequently exploit human behaviour which is made easier by a lack of knowledge in correct use of technology. Furthermore, humans' lack of compliance with organisational policies and procedures favours phishers. In order, therefore, to be adequately protected against phishing attacks, particularly in an organisational context, a framework is required consisting of all the HOT elements (Frauenstein and Von Solms, 2009). There is a need to close the gap between each of these elements. If this is not done, any of the three HOT elements may subsequently be compromised to the detriment of the organisation. In the literature examined no approach could be found that describes ways to further integrate and improve the relationships between the HOT elements.

# 4. Linking Elements towards a Holistic Framework

The previous section established and described the three main links that should exist between the HOT elements. However, these links are still not tightly bound, thus exposing a gap for phishers to exploit. As such, more understanding is necessary on how the links can be managed more appropriately. This section aims to achieve this by describing theories and best practices in conjunction with those links. An understanding of these theories and best practices will help point out specific areas that influence the respective links, which will contribute to the establishment of an anti-phishing framework.

## 4.1. The Technology Acceptance Model

Many IT professionals reason that the key to the success of information security lies in the way humans use computers and technology. Phishers take advantage of aspects of human behaviour, specifically the way humans interact with computers (Schneier, 2000). Since it is apparent that humans are often unable to use technology optimally, developers are generally automating technology. One of the factors that may cause humans not to use technology correctly is because it is considered technically complex. The Technology Acceptance Model (TAM) is an information systems theory representing individuals' acceptance and usage of technology (Davis, 1989). For this reason, the TAM serves as a suitable model to understand how the **human** (H) and **technology** (T) elements can be further strengthened. According to Swanson (1988), one of the most challenging issues in information systems (IS) research is to understand why people accept or reject computers. If this can be understood, one would be able to predict, explain and increase user acceptance of technology (Davis, 1989). Accordingly, the TAM suggests that when users are presented with a new form of technology, a number of factors influence their decision about *how* and *when* they will use that technology. As discussed by Davis (1989), these two factors are: perceived ease of use (PEOU) and perceived usefulness (PU). Users' negative attitudes and behaviour towards the use of technology may influence its perceived usefulness.

In his study Ohaya (2006) points out the following factors why users are still susceptible to phishing: "lack of knowledge in computer systems; lack of security and security indicators; lack of attention to security indicators; lack of attention to the absence of security indicators and finally sophistication of spoofed websites." In some cases, users ignore phishing warning messages from anti-phishing tools (Dhamija *et al.* 2006; Egelman *et al.* 2008). All of these concerns mentioned points out a lack of knowledge in technology. Technology is frequently used by phishers as a tool to carry out their attacks. In response, users (the victims) should also be able to use technology as a tool to protect themselves against such attacks. Some phishers are very knowledgeable about web development and are able to develop websites that are almost perfect replicas of genuine websites (Jakobsson, 2007). This strongly suggests that users need to be educated, trained and made aware of phishing techniques and to be suspicious of well-designed spoofed websites. Users also require training in using technological tools and its features such as email client, web browser, anti-virus program, system alerts and so on. This can successfully bridge the gap between humans (H) and technology (T).

### 4.2. Agency Theory

Agency theory discusses the agency problem that arises when cooperating parties have different goals and division of labour (Jensen and Meckling, 1976). This relationship is metaphorically described as a contract between two parties, namely, the *principal* who delegates work to the *agent* who performs that work (Jensen and Meckling, 1976). In this study, the research problem is addressed in an organisational context; as such, the principal is seen as the *organisation* and the agent is the *user* or *employee*. Agency theory is regarded here as being an appropriate theory to understand the significant role between **human** (employee) and **organisational** (management) elements. According to Eisenhardt (1989), agency theory is concerned with resolving two problems: The conflicting desires or goals of the principal and agent, and the verification of the agent's activities, which is too difficult or expensive for the principal. Conflict arises when the principal and the agent have different attitudes toward risk. These differing goals may explain why the agent (i.e. employees) disobeys or neglects organisational policies and procedures. The fact that organisations have policies and procedures in place means that there are no written disparities in what the employee should and should not do. However, even if an organisation has such policies and procedures in place, it should not necessarily be taken for granted that employees comply with and support them. Herath and Rao (2009) state that employee negligence and non-compliance with policies cost organisations millions of dollars every year. To address the problems pointed out above, the principal aims to motivate the agent using incentives that recognise the agent's effort, as well as the environmental factors that have an effect on the outcomes (Herath and Rao, 2009).

Schlienger and Teufel (2003) describe that even where employees know of security policies, they may still wilfully ignore such policies because they do not understand *why* they are needed. Therefore, for users to behave appropriately in the organisation they first need to be made aware of and given reasons why security policies and procedures are needed. Furthermore, they need to know and understand how to implement the procedures supporting such policies (Thomson and Von Solms, 1998). If this is not accomplished, users will put organisations' information at risk. Educating employees on why such policies are in place not only increases understanding, but also increases motivation (Siponen, 2000). In terms of such policies, it is also important that employees understand their roles and responsibilities within the organisation (ISO/IEC 27002, 2005, p. 23). Establishing an organisational security culture is another element that cannot be ignored as it has great significance in agency theory. The organisational culture is consequently expressed in terms of the collective values, norms and knowledge of organisations (Schlienger and Teufel, 2003). In turn, those collective norms and values impact on the behaviour of the organisation's employees. If employees do not take the severity of risks posed by phishers seriously, their behaviour will affect other members of a particular organisation. Addressing the agency theory factors requires both parties to understand their roles and responsibilities. In this regard, education is required to help change the behaviour of employees. If this could be achieved, this would satisfy the agency theory problems highlighted earlier, thus closing the gap between the human (H) and the organisational (O) elements.

### 4.3. COBIT 4.1

Linking IT to business is not a new concept; it has previously been recognised as business–IT alignment. This alignment refers to "applying IT in an appropriate and timely way, in harmony with the business strategies, goals and needs" (Luftman, 2004). IT alignment specifically attempts to address the way the organisation should or could be harmonised with IT. For this reason, COBIT 4.1 (2007) serves as a suitable best practice to understand how the link between the **organisational** (O) and **technology** (T) elements can be strengthened. COBIT's objective is the following: "Specifying the decision rights and accountability framework to encourage desirable behaviour in the use of IT." It has been frequently pointed out in this study, that human behaviour is a concern. IT governance implies a system in which all stakeholders, including the board, executive management, customers and staff, have clear accountability for their respective responsibilities in the decision-making processes affecting IT. These stakeholders form part of the organisational dimension. Elements of the COBIT 4.1 domains were selected specifically to deal with phishing threats. COBIT's guidelines of 'ensure systems security', 'monitor and evaluate internal controls' and finally 'ensure regulatory compliance' are considered applicable in addressing this linkage specific to phishing. According to COBIT 4.1, ensuring systems security is in place would satisfy the requirements for IT by maintaining the integrity of information, processing infrastructure and minimising the impact of security vulnerabilities and incidents. This is applicable not only to phishing threats but also to any security threat. Monitoring and evaluating the effectiveness of controls is an important process given the ever-changing nature of technological controls and phishing attacks. As a result, controls may have to be improved accordingly. Top-level management has a vital role to play in ensuring that the organisational IT infrastructure provides a safe, reliable and secure environment in which its employees can perform their duties. It must support information security and ensure that employees are trained to exercise their information security responsibilities. If not, this will potentially create an opportunity for phishers to target weak IT infrastructure either by exploiting technological vulnerabilities, or through employee behaviour.

## 5. Conclusions and Future Work

This paper examined theories and best practices that are relevant to the main relationships that influence each of the HOT elements. This provided guidance for understanding the variables that reveal gaps between each of the elements. It is evident that in all three linkages (HT, HO, and OT), the attitudes and behaviour of users influence the functioning of these linkages. Humans need to be properly educated to minimize any negative attitudes towards technology and to recognise that it is easy to use and useful for its purpose. Moreover, they need to be educated on security threats and their related risks. Humans need to be trained in using technological controls correctly to counter phishing attacks. They also need to be educated in terms of carrying out their roles and responsibilities safely in organisations; this is made possible by organisational policies and procedures. Finally, the organisation should ensure that its IT infrastructure and its associated processes are defined and managed correctly. It can be claimed that; if TAM and the agency dilemma, as described in Agency theory, together with elements of COBIT are satisfactorily introduced and maintained in an organisation, definite strides are being made towards a holistic anti-phishing framework. Accordingly, a security awareness, training and education programme will play an essential role in ensuring that these linkages form a stronger bond with the respective elements. Components of such a programme will be discussed in future work and will be evaluated by means of semi-structured interviews.

## 6. References

Beznosov, K., & Beznosova, O. (2007). On the imbalance of the security problem space and its expected consequences. *Information Management & Computer Security, 15*, pp. 420–431.

Cabrera, Á., Cabrera, E. F., & Barajas, S. (2001). The key role of organizational culture in a multi-system view of technology-driven change. *International Journal of Information Management, 21*, pp. 245–261.

COBIT 4.1. (2007). *COBIT 4.1 Executive Summary*. Illinois, USA: IT Governance Institute.

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. *MIS Quarterly, 13*, pp. 319–340.

Deloitte. (2012). *Deloitte-NASCIO Cybersecurity Study: State governments at risk: a call for collaboration and compliance*. http://www.nascio.org/events/2012Annual/documents/State-Governments-at-Risk.pdf (Accessed 20 November 2012).

Dhamija, R., Tygar, J. D., & Hearst, M. (2006). *Why phishing works*. Proceedings of the SIGCHI conference on Human Factors in computing systems, Montreal, Quebec, Canada: ACM. pp. 581–590.

Downs, J. S., Holbrook, M. B., & Cranor, L. F. (2007). *Behavioral response to phishing risk.* Proceedings of the Anti-Phishing Working Group's 2nd Annual eCrime Researchers Summit, 2007 Pittsburgh, Pennsylvania. 1299019: ACM, pp. 37-44.

Egelman, S., Cranor, L. F., & Hong, J. (2008). *You've been warned: An empirical study of the effectiveness of web browser phishing warnings*. Proceedings of the twenty-sixth annual SIGCHI conference on Human factors in computing systems. Florence, Italy: ACM. pp. 1065-1074.

Eisenhardt, K. M. (1989). Agency theory: An assessment and review. *Academy of Management Review, 14*, pp. 57–74.

Frauenstein, E. D., & Von Solms, R. (2009). Phishing: How an organisation can protect itself. *Information Security South Africa (ISSA)*. Johannesburg, South Africa. pp. 253–268.

Frauenstein, E. D., & Von Solms, R. (2011). An enterprise anti-phishing framework. *Proceedings of the 7th World Conference on Information Security Education (IFIP WISE7 TC11.8),* Lucerne, Switzerland. pp. 80-88.

Herath, T., & Rao, H. R. (2009). Encouraging information security behaviors in organizations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems, 47*, pp. 154–165.

ISO/IEC 27002. (2005). Information Technology: Security techniques – Code of practice for information security management. *ISO/IEC 27002:2005.* Standards South Africa.

Jakobsson, M., Tsow, A., Shah, A., Blevis, E., & Lim, Y. K. (2007). What instills trust? A qualitative study of phishing. *Proceedings of the 11th International Conference on Financial cryptography and 1st International conference on Usable Security.* Scarborough, Trinidad and Tobago: Springer-Verlag.

Jensen, M., & Meckling, W. (1976). Theory of the firm: Managerial behavior, agency costs, and ownership structure. *Journal of Financial Economics, 3*, pp.305–360.

Kumaraguru, P., Rhee, Y., Sheng, S., Hasan, S., Acquisti, A., Cranor, L. F., & Hong, J. (2007). Getting users to pay attention to anti-phishing education: Evaluation of retention and transfer. *Proceedings of the Anti-Phishing Working Group's 2nd Annual eCrime Researchers Summit.* Pittsburgh, Pennsylvania: ACM.

Luftman, J. (2004). *Strategies for information technology governance.* Pennsylvania, USA: Idea Group (IGI Global).

Ohaya, C. (2006). Managing phishing threats in an organization. *Proceedings of the 3rd annual conference on Information security curriculum development*, 2006 Kennesaw, Georgia. 1231083: ACM. pp. 159–161.

Schlienger, T., & Teufel, S. (2003). Information security culture: From analysis to change. *Proceedings of the 3rd Annual Information Security South Africa Conference (ISSA).* Johannesburg, South Africa, pp.183–196.

Schneier, B. (2000). *Semantic attacks: The third wave of network attacks*. http://www.schneier.com/crypto-gram-0010.html#1. (Accessed 14 April 2009).

Schneier, B. (2008). The psychology of security. *Proceedings of the Cryptology in Africa 1st international conference on Progress in cryptology.* Casablanca, Morocco: Springer-Verlag.

Siponen, M. (2000). A conceptual foundation for organizational information security awareness. *Information Management & Computer Security*, *8*(1), pp. 31–41.

Swanson, E. B. (1988). *Information system implementation: Bridging the gap between design and utilization.* Homewood, IL: Irwin.

Thomson, K.-L., Von Solms, R., & Louw, L. (2006). Cultivating an organizational information security culture. *Computer Fraud & Security.*

Thomson, M. E., & Von Solms, R. (1998). Information security awareness: Educating your users effectively. *Information Management & Computer Security*, *6*, pp. 167–173.

Werlinger, R., Hawkey, K., & Beznosov, K. (2008). Human, organizational and technological challenges of implementing it security in organizations. *Human Aspects of Information Security and Assurance (HAISA) 2008*. Plymouth, England. pp. 1-10.

West, R. (2008). The psychology of security. *Commun. ACM, 51*, pp. 34–40.