PHISHING: HOW AN ORGANISATION CAN PROTECT ITSELF

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

[1, 2]Nelson Mandela Metropolitan University, South Africa

[1]efrauenstein@wsu.ac.za, (+27)72 144 2751, East London, 5247

[2]rossouw@nmmu.ac.za, (+27)41 5043669, PO Box 77000, Port Elizabeth, 6000

ABSTRACT

The objective of this paper is to report on research to construct a model, which should provide guidance to an organization on how to address all dimensions associated with phishing and assist in solving the problem holistically. The emphasis will be placed on the human and organizational dimensions. Most research in this area has shown that only certain dimensions used to combat phishing attacks, in an organization, are addressed in isolation and not holistically. Anti-phishing research literature studied has either focused on algorithms for detecting phishing attacks in web browsers (Egelman, 2008; Fette, 2007; Garera, 2007; Patel, 2007) or on evaluating the user interfaces of anti-phishing web browser toolbars (Wu, 2006). From research studied, there has been little work conducted on preventing users from falling for phishing email messages. It has been proven that phishing does indeed pose an ongoing threat to an organization through its employees. Therefore, a suitable solution to this problem should be devised. This paper attempts to present such a holistic solution in the form of a model.

KEY WORDS

Phishing, social engineering, information security model, e-mail scams, spoof-websites

PHISHING: HOW AN ORGANIZATION CAN PROTECT ITSELF

1 INTRODUCTION

Information in the modern electronic world can be viewed as the most important asset in a global market. Individuals, businesses, organizations and governments depend on information to be embedded in secure, private and trustworthy IT infrastructures (http://www.thedacs.com/techs/enhanced_life_cycles/). Individuals within an organizational environment often tend to rely on an organization to take responsibility and have these well defined controls to protect the integrity and availability (ICT Standards Board, 2007) of their personal data from unauthorized access, use, disclosure, disruption, modification or destruction (IBM Business Consulting Services, 2006). However, these controls alone cannot avert information security threats. An alternative technique of gaining unauthorized access of information, apart from the common procedure of hacking, is *Phishing*.

The objective of this paper is to report on research to construct a model, which should provide guidance to an organization on how to include all dimensions associated with phishing and assist in solving the problem holistically. The emphasis will be placed on the human and organizational dimensions. This paper also addresses, from research studied, the problems that phishing poses to individuals and organizations (Orgill, 2004).

2 BACKGROUND TO THE PROBLEM OF PHISHING

There is much evidence in literature that proves that phishing is a growing problem in the current global industry and poses an ongoing threat that may affect every individual in an organization (Ohaya, 2006; Orgill, 2004; Safecode, 2008; Threat Insight Quarterly, 2005). Phishing is a social engineering technique through which an individual attempts to solicit and steal confidential information from a user or employee by masquerading as a legitimate entity (Kumaraguru, 2007). Today, phishing has become much more sophisticated in techniques using technology, advantageously,

as a tool through a combination of spoofed emails, Internet Relay Chat (IRC) and instant messengers (IM's) to lure individuals (Ohaya, 2006).

Since most organizations are conducting business transactions through the Internet, Information Technology is rapidly changing the world through information and communication technology (Alkadi, 2004). Today most communication occurs through electronic mail. According to Badra (2007), there are many various forms of phishing attacks however, common phishing schemes mostly use spoofed e-mails to lure users to fake websites designed to capture their confidential information (Ohaya, 2006). The spoofed- email normally tends to have a slightly threatening message or tone to increase the effectiveness of luring the victim to avoid any further consequence. An example of this technique could be that the user's bank account details would be terminated if they fail to respond to the email. Phishing is not only based on obtaining user account details, but includes access to all personal and financial data. When individuals respond to such messages, they are putting themselves and their respective organizations at risk. This is caused primarily due to a lack of knowledge in information security protocols and carelessness regarding the consequences which may follow.

Recently, social attraction networks (e.g. MySpace, Facebook and Friendster) have gained popularity in phishing attacks (Brown, 2008; Unisys, 2008) and are being used as sources to lure individuals to give out their personal information. The latter substantiates the point that threats are constantly finding new weaknesses in technology and using more sophisticated techniques to gain entry through this modern, technological age (Orgill, 2004). Since people can be considered to be the weakest link in a very technologically secure computing environment (according to current standards), they are consequently targeted by social engineering attacks (Orgill, 2004). Much emphasis is placed on making computer systems more secure (technology aspect) and thus, the human element is often forgotten, ignored or neglected. Each new threat adds to the difficulty of securing an information system. The attacker does not have to have any prior knowledge into hacking systems, but rather understanding the use social engineering techniques. Human emotion and manipulation are used to trick victims into giving up personal information. The social engineer attempts to exploit the natural desires of humans to trust others and strangers, to assist in other's labours and to gain favour in their eyes

(Orgill, 2004). PayPal, eBay, American Online (AOL) and the South African Revenue Services (SARS) (http://www.sars.gov.za/home.asp?pid=42736) are well known examples of organizations that have all claimed victim to having been financially affected by phishing attacks

People and organizations, especially in a South African context, may not be aware of the dangers that phishing poses or how to detect these threats. This is indeed the case, even though much literary sources educate users on how to effectively identify these threats (Fette, 2007; Garera, 2007; Patel, 2007). People seem too dependant on IT systems to manage security concerns. This lack in responsibility exposes this weakest link, the human factor (Orgill, 2004; Patrick, 2005; Robila, 2006).

3 CURRENT PROTECTION MEASURES IN ORGANIZATIONS

Organizations can effectively manage and protect their information from unauthorized access, by following the internationally accepted and recognized Code of Practice for Information Security Management i.e. ISO 27002 (http://www.iso27001security.com/html/27002.html). This international standard is but one 'best practice' approach that provides recommendations of what companies should implement to protect their information assets. The standard also addresses many issues and concerns relating to information security. Applying only an international standard may not be adequate enough as even these generally accepted Information Security (IS) standards and best practices do not effectively address the Social Engineering aspect of Information Security and may leave gaps for phishing attacks. The document does not particularly focus/emphasis on the term "phishing" attacks but does indeed mention that it is currently a problem. It rather gives general guidelines that one shouldn't exchange information with unknown parties or open emails from unknown sources etc. The illusion that emails appear to be from a legitimate source is what allows phishing attacks to be so effective. The email seems relevant in context and seems legitimate, in design, to the individual (Egelman, 2008). The latter is regarded as a spear phishing attack (Microsoft, 2005). Therefore, spear phishing attacks have the potential to pass through strong company regulations and seemingly secure technology controls, relying mostly on the human element for protection (Orgill, 2004).

There are many reasons why individuals fall susceptible to phishing attacks. According to Ohaya (2006) some of the reasons include a lack of knowledge of computer systems, lack of security and security indicators, lack of attention to the security indicators, lack of attention to the absence of security indicators, and the sophistication of spoofed sites seem to be the greatest threat. If the site looks authentic, users have confidence in it as they could not tell the difference between a genuine or spoofed web-site. Ohaya (2006) states further that security managers should take the following steps to protect the organization and employees from phishing attacks:

> 1. "Ensure privacy and security are perceived at a macro level in the organization.
>
> 2. Create security policies, standards, and procedures that are part of an ongoing overall security management framework
>
> 3. Ensure that all employees in the organization have security education, training and awareness about phishing and other threats in addition to following security policies and procedures."

Orgill (2004) substantiates this in stating that employee education should cover the company's strong policy statements, including penalties for non-compliance. In fact, researchers (Ohaya, 2006; Orgill, 2004; Robila, 2006) have shown that user education is the most important aspect of preventing phishing attacks. Kumaraguru (2007) designed and evaluated an embedded training email system that teaches people the dangers of phishing during their normal use of email as he feels that people simply ignore security notices and warnings. Sheng (2007) developed a game that teaches people not to fall for phishing, thus getting them more interested in the fun educational aspect. According to Badra (2007), reducing the phishing threat can be achieved if a given solution could meet the following functions: monitoring potentially malicious activity, authenticating email messages, detecting unauthorized use of trademarks or logos or other proprietary imagery, improving the security patching infrastructure to increase resistance to malware, using personalized information to authenticate an email directly to a user and detecting a fraudulent web site and alerting the user.

According to O'Brien (2000) there are 3 major types of controls that must be developed to ensure the quality and security of information systems

- **Information System controls** (input, processing, output and storage controls)
- **Procedural Controls** (standard procedures, documentation, authorization requirements, auditing)
- **Facility Controls** (physical protection, computer failure controls, network security and biometric controls).

These above-mentioned controls merely focus on the management aspect of the information system in relation to normal everyday conditions of business transactions, specifically the input, processing, output and storage activities in an information system. This approach focuses more on the technological and organizational measures in place rather than an unforeseen human error. It does not encompass provisions for the idiosyncratic nature of the human element, especially within a social context. Phishing has few technical boundaries. Its strength lies in its ability to trick any individual irrespective of experience, knowledge or position in the organization. This method of acquiring sensitive information from the individual could then lead to the entire organization's confidentiality or individual's personal information being put at risk.

While technology is important, organizational and human factors also play a crucial role in achieving information security (Dutta, 2008). These dimensions should play a role in constructing a holistic approach to protect information assets against phishing attacks. The ***technological*** dimensions would typically involve anti-phishing software, spam filters, firewall etc. The ***human*** dimension calls for effective awareness and education to assist in strengthening the 'human firewall' and to ideally cultivate a culture of information security behaviour. On the other hand, sound ***organizational*** measures, e.g. policies and procedures, need to be in place to put everything into perspective. Of these dimensions, the human factor is probably the most important since this is the area that phishing exposes the most. Research suggests that if human behavioural response can be understood, then one may have a solution to the issue of why people fall susceptible to phishing attacks (Downs, 2007). Information

Security should not be regarded as a technical issue but rather a multi-dimensional issue. Therefore is a need for all of these dimensions to be considered. In doing so, this should provide for adequate overall risk mitigation against phishing attacks.

Below are the main components which will be addressed in the model and recommendations for each of these components:

International Standards, Guidelines and Best Practices: As mentioned**,** numerous international standards, best practices and guidelines refer to the effective protection of information assets, e.g. ISO 27002 (http://www.iso27001security.com/html/27002.html), COBIT (COBIT, 2000), the King II Report (King Report, 2001), etc. Such standards, best practices and guidelines should play an integral role in the eventual plan to protect organizational information assets against phishing attacks.

Technology controls: As earlier discussed in this paper, threats are finding new weaknesses in technology. Therefore it is considered a dimension that compromises the integrity of an organization's information security. It is important to address its role in the model. Phishing attacks can breach a weak technological barrier. The "phisher" may rely on the individual or organization to have an outdated or ineffective web browser, outdated anti-virus program due to poor organization policies. The phisher may lure individuals through websites like Facebook, Twitter etc. The use of IRC and Instant messengers are a new breeding ground for phishing attacks. Most organizations should have anti-virus programs installed. However, an effective anti-virus program is only as good as the currency of its virus definition updates that it receives. Besides its primary function of scanning for virus signatures, some anti-virus programs can also detect most phishing websites (http://anti-virus-tools.software.informer.com/). The anti-virus program can also remove key-logger Trojans- a virus designed by 'phishers' to monitor keystrokes from the keyboard.

Organizations use firewalls, in a network environment, to filter incoming emails as well as to block unauthorized entry from outsiders. If properly defined through procedures, the firewall also prevents employees from accessing illegal or unwanted websites, in this regard phishing websites.

(http://www.security-forums.com/viewtopic.php?p=5787&id=db1bca5dcddd4bff05dd056501b7e922).

The internet web browser also forms an important role, in security, in having the built-in capacity to identify spoofed websites. Common web browsers such as Microsoft Internet Explorer 7, Opera 9.5, Firefox 3, and Safari 3.2 etc. can detect most phishing websites. However, each reacts differently to suspicious spoofed-websites in the manner it displays active phishing warnings to the user (Egelman, 2008). This presents a problem in the sense that it may confuse the individual when presented with such a warning. An organizational standard should be set as to identify which browser would best be suited in such a case of an individual falling susceptible to a phishing website.

The operating system (e.g. Windows XP, Windows Vista, etc.) should be regularly updated for software enhancements (updates, patches, hot-fixes etc.) either automatically or by relevant staff. Failure to do so creates an opportunity for viruses to either pose as an application or as a warning notification thus luring the victim to submit confidential information. The latter is another technique of phishing that acquires personal information (http://computing.vassar.edu/safecomputing/security/ospatch.html). Phishing attacks can also be in the form of malicious code-based or Trojan-based attacks, in which malicious software causes data compromises (Badra, 2007)

Technological aspects form an imperative part in the eventual protection model against phishing attacks. Clear guidelines need to be provided as to which controls should be implemented in this regard.

Organizational aspects: Human Resource related aspects play a major role in the recruitment of skilled and trustworthy staff. This can be done through effective screening etc. Newly appointed staff must be made aware of company policies and procedures. This can be defined in a policy document by the organization requiring employees to sign upon appointment. Failure to comply with these procedures should result in penalties by the staff member. Some of these policies may have a relationship with technology aspects e.g. do not install pirated software, individuals must encrypt sensitive files when emailing clients, software

updates must be done regularly by IT staff, downloading of files not relative to organization needs is not permitted etc. The organization needs to adopt an information security culture. The organization needs to realize the importance of strengthening and securing their information, and lead the way in ensuring that future security threats are prevented and controlled. This can be done through effective physical and software procedures. It is critically important that the organization should ensure that proper policies, regarding protection against phishing attacks, are defined and that sound procedures are put in place. Once in place, this will then have an effect on the technological aspects and human aspects.

Human Factors: As mentioned throughout this paper, the weakest target phishing attacks focus on is through the human aspect. Through education, employees can be made more aware of the activities involved in a phishing attack (van der Merwe, 2005) and how it may affect them and the organization. This can be done through regular training workshops. The training needs to have some incentive or humour in gaining effective participation from its employees. The training should also give relevant examples in context of daily issues that plague employees in the organization, specifically in emails from unknown sources. The latter should address how to identify these threats and what procedures to follow. An added benefit, through training, allows employees to also learn of other current and future threats of information security aspects instead of phishing attacks alone. According to van der Merwe (2005), there are five issues that a company or individual should be aware of in phishing: education, preparation, avoidance, intervention and treatment. All of the latter issues have been considered and addressed in the proposed model.

As previously mentioned, three very important dimensions should form part of the protection model against phishing attacks. These are; technological, organizational and human related dimensions. These dimensions should be governed by applicable standards, best practices and guidelines. Below, figure 1, graphically represents the draft model of the above-mentioned dimensions to be considered in protecting company information from phishing attacks.

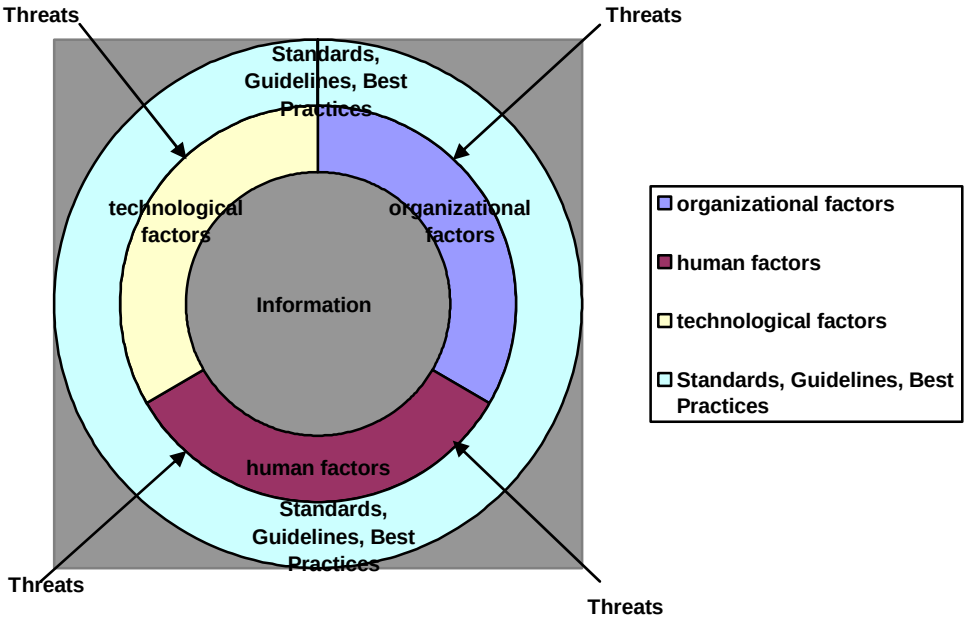

Figure 1: The model highlights major aspects, in an organization, that must be considered to form a complete barrier of defence against phishing attacks

4 CONTRIBUTION OF THE STUDY AND FURTHER RESEARCH

The proposed solution will be refined and tested, using design science, through further literature studies as well as a case study in an organization to determine its effectiveness. Sound methodologies will also be utilized to ensure that the model is developed with rigor to result in a trustworthy artifact. Of the three dimensions, through research studied, the human dimension has been established to be the weakest aspect in which phishing threats breach information security.

The detailed, eventual, model will help make an organization more aware of the dangers of phishing and educate them to prevent phishing attacks by addressing all dimensions required

5 CONCLUSION

As more organizations provide greater online access for their customers, phishers are successfully using more social engineering techniques to steal personal information and conduct identity theft at a global scale. By understanding the tools and technologies that phishers use, organizations and their customers can take a proactive approach in defending themselves against future attacks. To make this possible, it is imperative that organizations and its employees be properly educated about the dangers of phishing thus addressing the human dimension. It must be understood that all dimensions, as a whole, should be considered in the model and not just one in isolation. This will form a complete barrier against phishing attacks. Although a company may have well defined procedures that employees could read and sign every year, it has proven to be insufficient (Gragg, 2002). The latter can be due to large amounts of policy documentation that employees aren't keen to read and consequently merely signing it. Given a predicted increase in tools available to fight phishing, it is expected that future attacks will continue to be more refined in terms of targeting the user and even specificity (Robila, 2006). The latter such case of an employee within the organization attempting to acquire information illegally through another employee. Therefore, the proposed solution to this problem needs to be designed through an effective, rigorous model.

6 REFERENCES

Alkadi, I and Alkadi, G, (2004). '*Information technology in the business world through the years and beyond!'*, Journal of Academy of Business and Economics

Badra, M., E-L Sawda, S., Hajjeh, I, (2007). '*Phishing Attacks and Solutions'*, ACM International conference proceedings of the 3rd International conference on mobile multimedia communications, vol. 329, ICST (Institute for Computer sciences, social-informatics and telecommunications engineering, Nafpaktos, Greece

Brown, G., Howe, T., Ihbe, M., Prakash, A. and Borders, K. (2008). ' *Social Networks and context-aware spam*', Proceedings of the ACM 2008 conference on computer supported cooperative work, ACM, San Diego, CA, USA, pp. 403-412

COBIT (2000), '*Control Objectives for information and related technologies'* (COBIT), 3rd Edition, IT Governance Institute, USA, 2000

Downs, J.S., Holbrook, M. and Cranor, L.F (2007). '*Behavioral response to phishing risk*,' ACM International Conference Proceeding series, vol. 269, ACM, Pittsburgh, Pennsylvania, pp. 37-44

Dutta, A., Roy, R. (2008). '*Dynamics of organizational information security'*, System Dynamics Review, vol.24, Issue 3.,Wiley Interscience, Accessed 14 April 2009, http://www3.interscience.wiley.com/journal/121518999/abstract?CRETRY=1&SRETRY=0

Egelman, S., Cranor, L.F. and Hong, J. (2008). '*You've Been Warned: An Empirical study of the effectiveness of web browser phishing warnings'*, Conference on Human Factors in computing systems-Proceedings of the 26th annual SIGCHI conference on Human factors in computer systems, ACM, Florence, Italy, pp. 1065-1074

Enhancing the development life cycle to produce secure software (2008), Retrieved 28 May 2009 from http://www.thedacs.com/techs/enhanced_life_cycles/

Fette, I., Sadeh, N. and Tomasic, A. (2007). ' *Learning to detect phishing emails'*, Proceedings of the 16th International conference on World Wide Web, ACM, Banff, Alberta, Canada, pp 649-656

Garera, S., Provos, N., Chew, M. and Rubin, A.D (2007). ‘ *A framework for detection and measurement of phishing attacks*’, Proceedings of the ACM workshop on recurring malcode, ACM, Alexandria, Virginia, USA, pp. 1-8

Gragg, D. (2002). ‘*A multi-level defense against social engineering’*, SANS Institute InfoSec Reading Room, Accessed on 3 April 2009, http://www.sans.org/rr/papers/51/920.pdf

How to keep your computer's operating system and programs up-to-date. Retrieved 17 April 2009 from http://computing.vassar.edu/safecomputing/security/ospatch.html

IBM Business Consulting Services (2006). ‘*Federal Information Security Management Act (FISMA) Compliance Solution- Improving management, operational, and technical controls over information, personnel, and physical security and privacy*’, USA, Accessed on 14th April 2009, http://www-03.ibm.com/industries/global/files/FISMA_Cutsheet_PS_0306.pdf

ICT Standards Board (2007). ‘*Network and Information Security Standards Report’*, Issue 6.2, Accessed on 17th April 2009, http://www.cen.eu/CENORM/BusinessDomains/businessdomains/isss/activity/nisfinalreport.pdf

ISO/IEC 27002:2005 Information technology -- Security techniques -- Code of Practice for Information Security Management. Retrieved 14 April 2009 from http://www.iso27001security.com/html/27002.html

King Report (2001). ‘*King Report on Corporate Governance for South Africa 2001’*, Accessed on 17 April 2009, http://general.uj.ac.za/infosci/scipsa/king-report-on-corp-gov.pdf

Kumaraguru, P., Rhee, Y., Acquisti, A., Cranor, L.F., Hong, J. and Nunge, E. (2007). *'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, ACM, San Jose, California, USA, pp. 905-914

Microsoft (2008). '*What is spear phishing?-Help prevent identity theft from new targeted phishing scams'*, Accessed on 10 April 2009, http://www.microsoft.com/canada/athome/security/email/spear_phishing.mspx

O' Brien, J. (2000). *'Introduction to Information Systems-Essentials for the internetworked Enterprise*, ninth international edition, Irwin/McGraw Hill, United States

Ohaya, C. (2006). '*Managing Phishing threats in an organization*', Information Security Curriculum Development Conference, Proceedings of the 3rd annual conference on Information security curriculum development, ACM, Kennesaw, Georgia, pp 159-161

Orgill, G.L., Romney, G.W., Bailey, M.G and Orgill, P.M (2004). '*The Urgency for Effective User Privacy-education to Counter Social Engineering Attacks on Secure Computer Systems*', Information Technology Education (Formerly CITC), ACM, New York, USA, Salt Lake City, UT, USA, pp. 177-181

Patel, D. and Luo, X. (2007). ' *Take a close look at phishing'*, Information Security Curriculum Development Conference'07, Proceedings of the 4th annual conference on Information security curriculum development, ACM, Kennesaw, Georgia, USA

Patrick, A., Marsh, S. and Briggs, P. (2005). '*Designing systems that people will trust*', National Research Council Canada, Accessed on 14th April 2009, http://www.iit-iti.nrc-cnrc.gc.ca/publications/nrc-47438_e.html

Robila, S.A and Ragucci, J.W. (2006). *'Don't be a phish: Steps in user education*', Annual Joint Conference Integrating Technology into Computer Science Education, Proceedings of the 11th annual SIGCSE conference on Innovation and technology in computer science education, ACM, Bologna, Italy, pp. 237-241

Safecode (2008). '*Software Assurance: An Overview of Current Industry Best Practices*', Accessed on 14th April 2009, http://www.safecode.org/publications/SAFECode_BestPractices0208.pdf

Security and Privacy / Anti-virus Tools at Software Informer. Retrieved 17 April 2009 from http://anti-virus-tools.software.informer.com

Sheng, S., Magnien, B., Kumaraguru, P., Acquisti, A., Cranor, L.F., Hong, J. and Nunge, E. (2007). '*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, vol.229, ACM, Pittsburgh, Pennsylvania, pp. 88-99

South African Revenue Services – SARS Phishing Attack. Retrieved 14 April 2009 from http://www.sars.gov.za/home.asp?pid=42736

Threat Insight Quarterly (2005). '*Phishing and other significant threats of 2004'*, Internet Security Systems, Accessed 14 April 2009, http://documents.iss.net/ThreatIQ/ISS_XFIQ0205.pdf

Unisys (2008). '*Unisys Identifies Five Security Issues Likely to Emerge Across Multiple Industries in 2008*', BusinessWire, Accessed on 14th April 2009, http://www.businesswire.com/portal/site/google/?ndmViewId=news_view&newsId=20080115005324&newsLang=en

van der Merwe, A., Loock, M. and Dabrowski, M. (2005). '*Characteristics and Responsibilities involved in a Phishing attack'*, ACM International Conference Proceeding Series; Vol. 92, ACM, Cape Town, South Africa, pp.249-254

Wang, A.J.A. (2005). ' *Information Security Models and metrics'*, Proceedings of the 43rd annual south east regional ACM conference, vol.2, ACM, Kennesaw, Georgia, pp. 178-184

WindowSecurity.com Beyond the Firewall (White Paper). Retrieved 17 April 2009 from http://www.security-forums.com/viewtopic.php?p=5787&sid=db1bca5dcddd4bff05dd056501b7e922

Wu, M., Miller, R.C. and Garfinkel, S.L. (2006). *'Do security toolbars actually prevent phishing attacks?'*, Proceedings of the SIGCHI conference on human factors in computing systems, ACM, Montreal, Quebec, Canada, pp. 601-610