An Assessment of People's Vulnerabilities in Relation to Personal and Sensitive Data

B.G.Sanders[1], P.S.Dowland[1] and S.M.Furnell[1,2]

[1]Centre for Information Security & Network Research,
University of Plymouth, Plymouth, UK
[2]School of Computer and Information Science, Edith Cowan University,
Perth, Western Australia
e-mail: info@cisnr.org

Abstract

Social engineering refers to a number of techniques that are used to exploit human vulnerabilities and manipulate people into breaking normal security procedures. Evidence suggests that this problem is rapidly increasing and cyber criminals are using a magnitude of different avenues to reach their intended victims. This paper presents an assessment of people's vulnerabilities in relation to personal and sensitive data. The experiment used an online web survey which comprised of both direct and non-direct social engineering attack scenarios. In addition the survey measured and assessed the level of risk that social networking users are currently exposing themselves to. The results showed that respondent's security awareness levels had improved on previous studies but significant problems still existed with user's abilities to detect and appropriately respond to social engineering threats.

Keywords

Social Engineering, Human Vulnerabilities, Phishing, Social Networking

1. Introduction

The protection of personal and sensitive data has previously been allied with technical based security measures. However, it is becoming increasingly apparent that technical solutions alone will not solve the problem and that people are typically the weakest link in the security chain (Rabinovitch, 2007). As people are now classified as the weakest link, it is important to ensure a high level of education, awareness and behaviour amongst individuals in order to maximise the protection and security of personal and sensitive data (Mitnick, 2002). Differing personalities inherently bring with them various potential vulnerabilities. These vulnerabilities are often exploited using one or more social engineering exploits.

Limited protection can be implemented to protect a user from feeling vulnerable to divulging information. Unlike physical network infrastructures, no patches or security policies can be applied to improve and protect against human misjudgements.

An online survey was conducted by the Centre for Information Security & Network Research which aimed to assess the extent of human vulnerability in relation to the protection of personal and sensitive data.

2. Background

The social engineering phenomenon is nothing new. Fraud has been in existence for decades with large scale phishing attacks dating back to 2003 (Furnell, 2008). Cyber criminal activity has become more prevalent over the last five years and numerous investigations have been conducted exploring the avenues in which human vulnerabilities are exploited using different social engineering based attacks (Tipton and Krause, 2003).

Social engineering comes in many different forms but can be divided into two main categories; direct and non-direct. Direct attacks typically involve direct communication with a specific victim. Such attacks are typically executed by face to face contact or over the telephone. Non-direct attacks in contrast are not usually aimed at one specific individual or organisation but sent to a wider audience. The most common form of which is phishing emails. Mitnick and Simon (2002) states that direct social engineering attacks heavily rely on collating information about the intended victim. The plethora of readily available information which can be obtained from a magnitude of sources gives a social engineer a distinct advantage.

Prior studies have investigated and measured the viability and successfulness of both direct and non-direct attacks. In 2004, InfoSecurity surveyed 172 office workers at Liverpool Street Station. This direct based study revealed that 71% of employees were willing to divulge their login details for a free Easter egg (Leyden, 2004).

A further direct based study was conducted in 2005 to investigate the willingness of the general public to divulge personal and sensitive data. The survey disturbingly showed that 92% of the 200 demographics questioned divulged sensitive information such as their mother's maiden name, first school and date of birth in return for a chance to win free theatre tickets. In addition, many of the surveyed demographics voluntarily disclosed their names and address. The researchers reported that they had acquired enough information to access online accounts and open bank accounts in victim's names (BBC News, 2005).

A more recent non-direct study conducted by Karakasiliotis *et al.* (2007) made use of an online survey to present a mixture of legitimate and illegitimate phishing emails and respondent demographics were required to analyse and differentiate between these emails. The study revealed that out of the 179 participants, only 50% of demographics were able to correctly identify genuine emails and only 60% were able to correctly identify phishing emails.

The prior studies documented above illustrate the vulnerabilities that exist amongst the end user community and the corresponding threat that is posed upon the protection of personal and sensitive data. However many of the threats described

above have been defined and explored since the turn of the millennium and as such it would not be unreasonable to expect organisations to embrace a suitable security policy incorporating methodologies to counter and safeguard against potential social engineering attacks.

3. Understanding and Perception

Evidence suggests that the underlying reason for exploitation is due to a distinct lack of awareness and understanding. End users are blatantly unaware of the potential consequences of their actions and do not understand the value of the data to which they are responsible for.

The age old saying of 'little knowledge is very dangerous' stands true with regards to end users perception of security. The problem is further exacerbated by users misunderstanding of network and end point security based applications. Furnell (2008) states that many users completely misunderstand the level of cover that such security applications provide. Discussions with such users revealed a false sense of security in that users perceive themselves as being 'completely protected' from all types of threat including social engineering attacks because they have an 'Internet Security Suite' installed. Many users do not understand the potential level of danger and hostility they are exposed to when accessing online facilities and the aforementioned false sense of security not only increases user's complacency but also greatly increases their chances of exploitation. Indeed, a recent study conducted by Furnell *et al.* (2008) interviewed 20 novice users in detail to assess their views and experience with Internet Security. The study revealed that demographics held a general awareness of the existence of threats but less familiarity with the appropriate safeguards beyond a very basic level. In addition, the study found that users accepted that they were ultimately responsible for their own protection but appeared somewhat unconcerned about the potential impact of the threats faced (Furnell *et al.* 2008).

The sophistication of modern day security products inherently bring with them greater complexity. The extent to which such security programs can be understood is often undermined by a number of human computer interaction design issues. Complex jargon and technical terminology can potentially impede the usability of security features in practice and consequently further increase the vulnerability of end users (Furnell *et al.* 2006).

4. The Risks of Social Networking Websites

As discussed in Section 3, evidence suggests that the rapid adoption of online facilities such as social networking websites have not been matched with a corresponding embrace of security culture (Furnell, 2008). Indeed, prior research has found that end users are recklessly posting personal and sensitive data onto social networking websites oblivious of the potential consequences. Many of the 50 million 'Facebook' subscribers were reported to be under the misperception that they had an antivirus package installed and deemed themselves to be 'protected'. King

(2008) states that due to the quasi-intimate nature of social networking websites, people share all types of personal and sensitive information, leaving them open to attack. In addition, according to a senior researcher at ScanSafe Ltd, cyber criminals are using personal details from social networking websites to help make phishing emails appear more convincing (ScanSafe, 2008).

A study conducted by the Information Commissioner's Office (ICO) in 2007 revealed that 4.5million web users aged between 14 and 21 could be vulnerable to identity theft as a result of giving up personal and sensitive data on the internet. The study of 2,000 British citizens showed that two-thirds accept people who they did not recognise as 'friends' and that half purposely deliberately allow public viewing to attract new online friends. 10% of demographics stated that they were not concerned that their profile could be viewed by strangers and 7% did not consider that privacy settings were important. The study also revealed that people were posting sensitive details such as their date of birth, mother's maiden names, pet names, telephone numbers, email addresses and their home address (ICO, 2007). In addition, an article published by the Daily Telegraph in November 2007, stated that children post more personal and sensitive on social networking websites than adults (Daily Telegraph, 2007).

The evidence documented in this section begins to enlighten the reader as to the scale and significance of the threat posed by user's recklessness to post personal and sensitive data online.

5. An Assessment of People's Vulnerabilities

The prior studies presented thus far clearly illustrate a lack of awareness and understanding amongst individuals and organisations. The findings presented in the succeeding sections provide an up-to-date assessment of people's vulnerabilities in relation to personal and sensitive data.

In order to assess people's vulnerabilities in relation to personal and sensitive data the authors made use of an online survey to target demographics of varying ages, cultures and levels of education in the shortest timeframe.

5.1. Assessment Design

The survey consisted of the following five sections:

Section 1: Demographics: This section focused on the specific individual attributes of the respondent demographic. Information such as age, gender, country of origin and level of education were collated. In addition, demographics were asked if they were students at the University of Plymouth and if they had previously undertaken any security related modules. The purpose of this section was to understand if any of the aforementioned attributes affected demographics responses.

Section 2: Computer Security: In response to the concerns raised in section 3, this section asked respondents five questions regarding their system security. The aim of this section was to gain a clear insight into individual's awareness for the need of basic system security. Respondents were asked where they used a computer and if they installed the latest updates to their computer when released. They were also asked how long they spend on the internet daily and whether or not they had a firewall installed. In addition demographics were asked if they had antivirus and anti spyware package installed and how often it was updated.

Questions:		Answers:	Rationale:
1	You are about to visit a website which is of interest to you when your firewall alerts you that your PC is attempting to make a connection to the Internet. What action would you take?	(Open Question)	Measures users risk taking ability and their understanding of a firewall.
2	You receive an email from your bank, stating that they are performing updates to their system. You are asked to sign in with your online banking credentials and verify your details are correct. What do you do?	1. Click the link from the email and sign in 2. Phone your bank and ask for more details 3. Visit the site later	Measures users' ability to detect and respond to phishing based attacks.
3	You have been using another individual's computer and visited a website that appeared to be malicious. You suspect that as a result the machine has become infected with a virus. What action would you take?	1. Immediately inform the individual about your suspicions 2. Leave them to find out later 3. Try and fix the problem yourself	Measures user's honesty and the importance of trust within computer security.
4	You are at work and a colleague has left their computer terminal logged on. Microsoft Outlook is running in the task bar. What action would you take?	1. Lock their computer 2. Inform user that the computer is logged on 3.Look through their emails/documents 4. Shutdown/turn off their computer 5. Notify an onsite technician	Measures users' integrity and honesty with regards to personal and sensitive data.
5	You arrive at work one morning and realise that you have left your access card at home. You require access to a restricted area and need your card. Someone approaches the door and opens it. What would you do?	1. Follow them in and continue your day 2. Go to the card issuing office and request a new temporary access card 3. Go back home and collect your access card	Measures users' understanding and awareness of the importance and need for physical security.
6	A friend owes you money and you are having difficulty in retrieving it. One day you notice that their computer is logged into their online banking. Would you take this opportunity to transfer the funds owed to you?	1. Yes 2. No	Measure users' trust and integrity when put in an advantageous situation.

Table 1: Hypothetical Scenario Based Questions

Section 3: Security Awareness: Section 3 placed the respondent demographics in 6 different hypothetical scenarios relating to security awareness. This section aimed to understand the extent of an individual's risk taking ability as well as measuring their awareness of potential social engineering vulnerabilities. Table 1 details the questions posed in this section along with the choices of pre-defined answers.

Section 4: Social Engineering: Leading on from the research previously conducted by Karakasiliotis *et al.* (2007), this section presented respondent demographics with 5 emails from well known online companies; namely eBay, Halifax Bank, PayPal and Amazon. Respondents were asked to identify the whether they deemed the email to be legitimate or illegitimate. Evidence suggests that the majority of online users are most susceptible to phishing based attacks. It was therefore considered prudent to gain an up-to-date insight of end user's abilities to differentiate between genuine and phishing emails.

Section 5: Social Networking: As seen by the evidence outlined in section 4, the potential dangers of social networking sites are growing considerably. The final section of this study asked respondent demographics to select all of the types of personal and sensitive data they would be willing to post online. The aim of this section was to gain an up-to-date insight into the extent of which such users are making themselves vulnerable.

5.2. Results

5.2.1. Demographics

The survey assessed the abilities of 86 demographics with regards to detecting and responding to direct and non-direct social engineering attacks. Invitations were circulated using email distribution lists and the majority of respondents were computing and engineering students in either UK or French universities. It is therefore highly likely that these participants received significant previous exposure to security related education and awareness programs. In addition, this exposure could have influenced respondent's answers due to increased levels of awareness.

It is commonly acknowledged that the majority of students enrolled on technical degrees in the UK are male. In 2008 a total of 297 students were accepted onto computer science, engineering and technology degrees at the University of Plymouth. 88% were male with only 12% were female (UCAS, 2008). These statistics are reflected in the research detailed below.

83% of respondents were male and 17% female. 14% of respondents were aged between 18-20, 58% aged between 21 – 25, 20% aged between 26 – 40, 3% aged between 41 – 49 and 5% were 50 years old or more. 84% of respondents originated from developed countries leaving 16% from undeveloped countries. 30% of respondents were students of the University of Plymouth out of which 74% had previously undertaken one or more security modules. The remaining 70% of

participants comprised of (26%) students from ESIEA Engineering Institute, France and (74%) were non-students from the UK.

The study found that none of the aforementioned variables significantly influenced demographic responses. Indeed, the results suggest that individuals of all ages, levels of education and countries of origin lacked awareness regarding social engineering exploits.

5.2.2. Computer Security

52% of respondents spent more than 4 hours online a day and 30% spent between 2 and 4 hours online daily. 85% used a computer both in work and at home. These results show a high level of online activity amongst respondent demographics. As discussed earlier in this document, it is crucial that end user awareness is sufficient enough to safeguard against the ever increasing threats and exploitations.

Figure 1 shows that the majority of surveyed demographics realised the importance of applying critical updates and the necessity of utilising a firewall. The results were more sporadic regarding the installation and updating of antivirus and antispyware packages. This indicates that users are unaware of the importance of antivirus and antispyware programs.

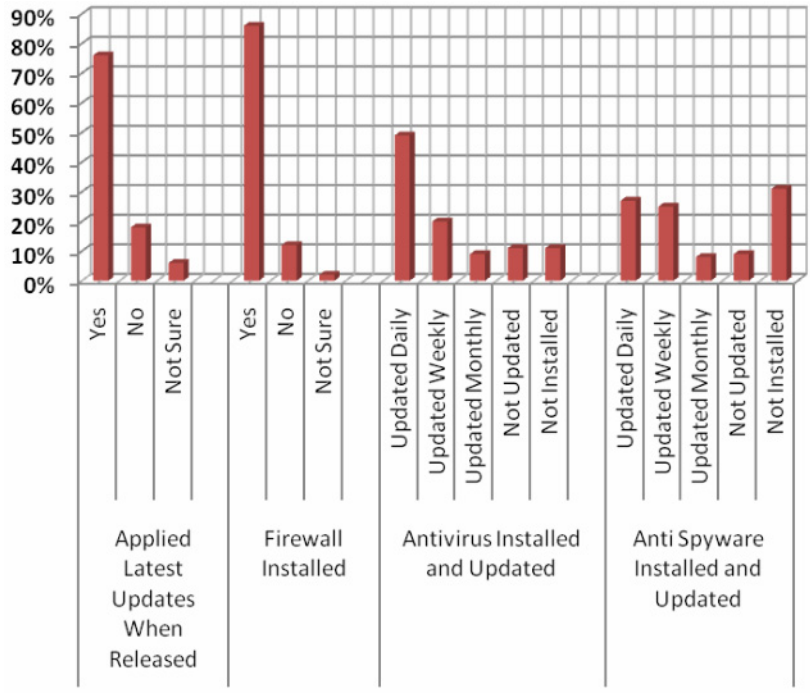

Figure 1: Computer Security Results

5.2.3. Security Awareness

Understanding the need for installing and updating protective security software is crucial. End users without adequate up-to-date security software are vulnerable to exploitation. Personal computers are often hacked to gain personal and sensitive information such as a person's identity and bank details.

The first question (Table 1) in this section asked respondents what action they would take if their firewall alerted them that their PC is attempting to make a connection to the internet. The question asked respondents to type an answer into a text box. As the demographics answers varied considerably due to the question being 'open', an analysis of these responses is summarised below.

Out of the total 86 respondents 15% did not give any answer to the above mentioned question. This indicated that some respondents did not understand the question posed. 23% stated that they would continue to view the webpage regardless of any firewall alert. 19% stated that they would open the website if they knew the website was legitimate but would close it if unsure. 15% stated that they would close the webpage immediately and block the URL. 26% stated that they would investigate the webpage using security facilities such as a firewall, antivirus or anti spyware software. Additionally 2 respondents stated that they would research the alert using an online search engine. 2% of respondents claimed that they would attempt to view the webpage on another computer, thereby placing another computer at risk rather than their own.

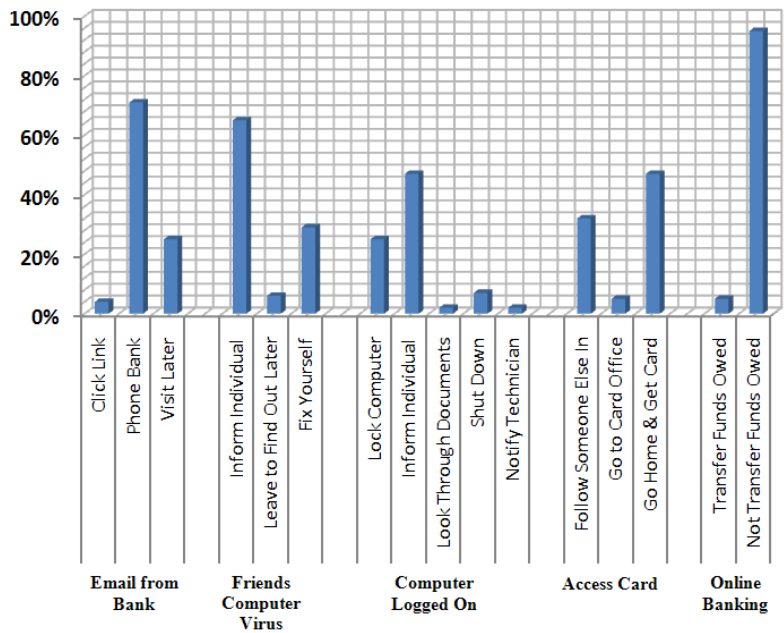

Figure 2: Security Awareness Results

Figure 2 shows the responses to the questions detailed in Table 1. The majority of respondents were able to correctly respond to situations which required an awareness of security and individual integrity. 32% claimed that they would follow another employee into a building in the event of leaving their access card at home. This result would suggest that a number of individuals do not understand the need for physical security. Direct social engineering attacks are successfully executed by a person claiming to be who they are not. Physical security and identity cards are a crucial counter measure in helping to prevent such attacks.

5.2.4. Social Engineering

The results shown in Figure 3 show a distinct lack of awareness amongst respondent demographics regarding phishing based attacks. 59% of respondents incorrectly identified the eBay security email as legitimate and 69% incorrectly identified the genuine eBay PowerSeller email as being a phishing email. The results were further analysed and it was found that respondents from undeveloped countries answered more favourably than those from developed countries. In addition students of the University of Plymouth who had previously studied one or more security modules performed worse than students who did not.

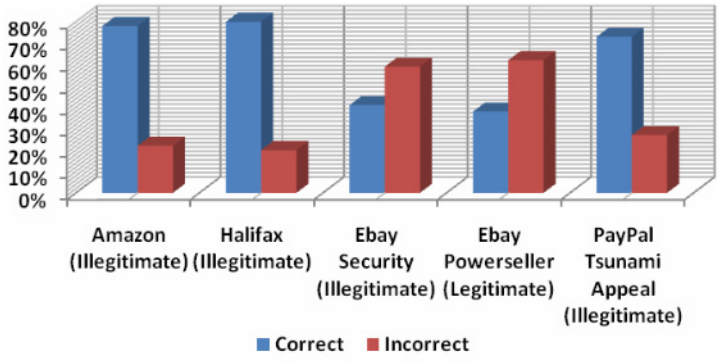

Figure 3: Social Engineering Results

5.2.5. Social Networking Websites

Out of the total 86 respondents 78% were members of one or more social networking websites leaving 22% who were not. The results in Figure 4 support the findings of previous researchers in that end users join social networking sites and post personal and sensitive information online. A small number of respondents were even prepared to post critically sensitive information such as their mother's maiden name (5%) and credit card details (2%) online.

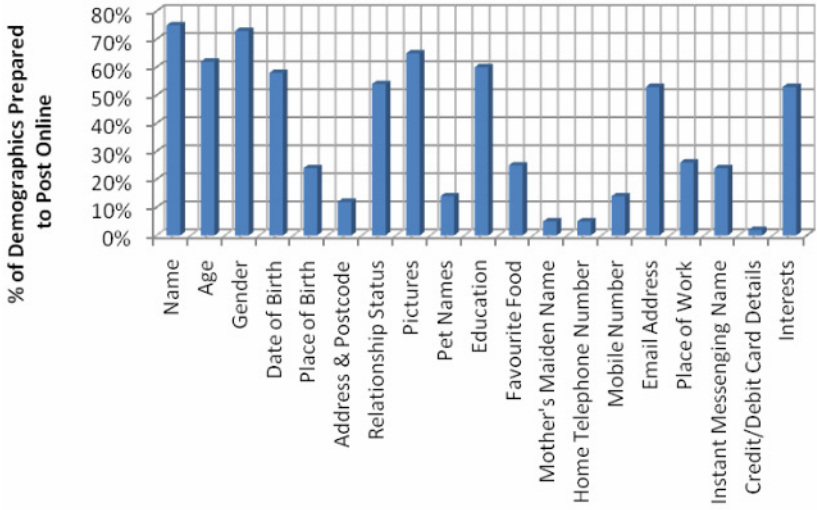

Figure 4: Social Networking Websites

6. Conclusions

This paper provides significant evidence that people are vulnerable to exploitation due to a lack of awareness of security issues. The results revealed that individual factors such as age and gender did not particularly influence demographics responses. Indeed none of the respondents were able to correctly identify all of the social engineering vulnerabilities despite the majority of demographics being educated to postgraduate level.

Demographics responses to the computer security and security awareness sections were promising and showed an improved level of awareness. The majority of respondents appeared to understand the need for essential security and could be trusted in a position of responsibility.

The responses to the social engineering and social networking websites however were more concerning. The results suggested that end users had problems differentiating between genuine and phishing emails. In addition it was clear that demographics were not aware of the potential consequences of carelessly posting personal and sensitive data online. The aim of this report was to assess people's vulnerabilities with regards to personal and sensitive data and the results have indeed facilitated a conclusive outcome that awareness raising strategies need to be implemented in order to safeguard people from exploitation.

7. References

BBC News, (2005) 'How to Sell Yourself for a Song' [Online] Available: http://news.bbc.co.uk/2/hi/technology/4378253.stml [Date accessed: 8th January 2008]

Daily Telegraph, (2008), 'Children's social-networking sites: set your little monsters loose online' [Online] Available: http://www.telegraph.co.uk/connected/main.jhtml?xml=/connected/2007/11/17/dlkids17.xml [Date accessed: 24th November 2008]

Furnell, S., (2008), 'End User Security Culture – A Lesson That Will Never Be Learnt?', Computer Fraud & Security, April 2008: pp. 6-9

Furnell, S., Jusoh, A., Katsabas, D. and Dowland, P., (2006), 'Considering the Usability of End-User Security Software', Proceedings of the 21st IFIP International Information Security Conference (IFIP SEC 2006), Karlstad, Sweden.

Furnell, S., Tsaganidi, V. and Phippen, A., (2008), 'Security Beliefs and Barriers for Novice Internet Users', Computers and Security 27: pp235-240

Information Commissioners Office, (2007), 'Social Networking' [Online] Available: http://www.ico.gov.uk/for_the_public/topic_specific_guides/social_networking.aspx [Date accessed: 27th November 2008]

Karakasiliotis, A., Furnell, S. and Papadaki, M., (2007). 'An assessment of end-user vulnerability to phishing attacks', Journal of Information Warfare, vol. 6, no. 1, pp.17-28.

King, P., (2008), 'Cyber Crooks Target Social Networking Sites', Point for Credit Research & Advice, 1/1/2008: pp. 9

Leyden, J., (2003) 'Office Workers Give Away Passwords for a Cheap Pen' [Online] Available:http://www.theregister.co.uk/2003/04/18/office_workers_give_away_passwords/ [Date accessed: 27th November 2008]

Mitnick, K.D. and Simon, W.L., (2002) 'The Art of Deception – Controlling the Human Element of Security' Wiley Publishing, Inc. ISBN: 0-7645-4280-X

Rabinovitch, E., (2007), Staying Protected from Social Engineering, *IEEE Communications Magazine, September 2007.*

ScanSafe, (2008), 'Vulnerabilities of Social Networking Websites' [Online] Available: http://news.bbc.co.uk/1/hi/technology/7156541.stm [Date accessed: 24th November 2008]

Tipton, H. and Krause, M., (2003) 'Information Security Management Handbook', 5th Edition, CRC Press, ISBN: 0849308887

UCAS, (2008), UCAS Statistical Services – Annual Datasets, [Online] Available: http://www.ucas.ac.uk/about_us/stat_services/stats_online/annual_datasets_to_download/ [Data accessed: 3rd April 2009]