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

B.G.Sanders and P.S.Dowland

Centre for Information Security and Network Research,
University of Plymouth, Plymouth, United Kingdom
e-mail: info@cscan.org

Abstract

Standards bodies and industry organisations spend a considerable amount of time, effort and money on the development and deployment of next generation solutions that address network security issues. However it is becoming increasingly apparent that people are in fact the main weakness with regards to the protection of personal and sensitive data.

This paper explores in detail the areas in which personal and sensitive data was socially engineered. The study investigated people's attitudes to security, their risk taking ability and their awareness regarding online and offline security. The analysis supports the theory that the security of data is entirely dependent on the security awareness and knowledge of individuals. In addition the study revealed that students who had undertaken one or more security modules at University had a greater awareness of security vulnerabilities, yet had limited knowledge regarding social engineering exploits.

The paper concludes that a number of individuals had little awareness and understanding regarding basic computer security and the need for such security. The results showed a distinct lack of respect and awareness amongst demographics in relation to online security and the security of others. These respondents were unaware of the potential consequences of disrespecting implemented security measures and as such were considered more vulnerable. The study also revealed that none of the respondents could correctly differentiate between a legitimate and illegitimate (Phishing) email which consequently increased the possibility of exploitation. In addition it was revealed that many individuals were making themselves increasingly vulnerable to social engineering attacks by posting personal and sensitive information on social networking websites.

Keywords

Social engineering, people's vulnerabilities, Phishing, passwords, cyber crime

1 Introduction

Regardless of how well a given network infrastructure is technically secured, the protection of sensitive data is still entirely dependant on the awareness and trustworthiness of its users. Security awareness of users is based on their education, background, experience and beliefs.

Due to the dramatic improvement in technical security, cyber criminals have resorted to socially engineering trusted users of a network in order to gain critical information such as login credentials.

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

With the present global state of information technology where the internet is generating a great deal of revenue and growing at an exponential rate it is crucial that awareness is raised throughout organisations in order to protect personal and sensitive.

An online survey conducted by a postgraduate student at the University of Plymouth assessed the extent of human vulnerabilities in relation to personal and sensitive data. The study revealed that respondents from various countries around the world were making themselves vulnerable to social engineering attacks which are largely due to a lack of awareness and understanding. It was found that individuals are willing to sacrifice the security of themselves and others for time and convenience.

2 Social Engineering

Social engineering is defined as the technique for obtaining confidential or sensitive information by interacting and deceiving people that can access that information (Burgoon, Qin, 2007). With the implementation of modern security technologies, attackers find exploiting human vulnerabilities much easier and quicker than conventional hacking (Twitchell, 2006).

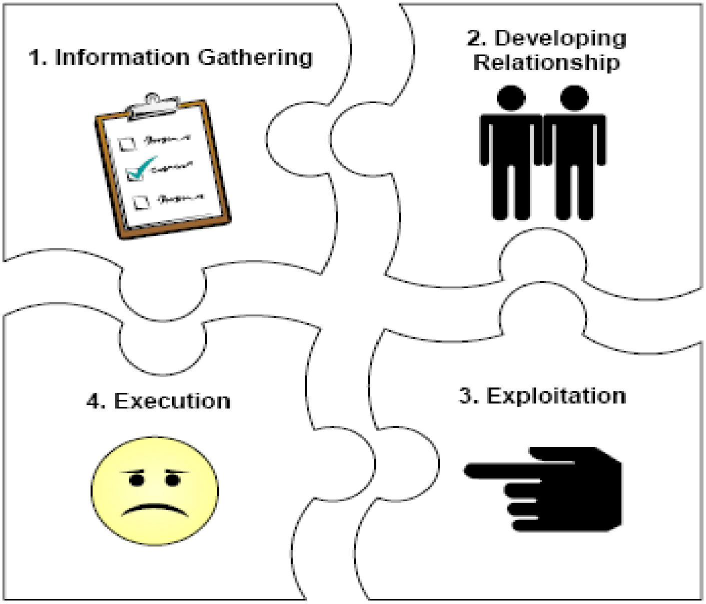

Figure 1: Social Engineering Cycle (Allen, 2006)

Figure 1 illustrates the social engineering cycle. This cycle consists of four phases: Information Gathering, Relationship Development, Exploitation and Execution. Each social engineering attack is unique in approach and execution and is likely to involve multiple phases/cycles (Allen, 2006).

Social engineers, unlike traditional hackers, exploit human vulnerabilities as opposed to technical weaknesses. Humans have been characterised as the ‘weakest link’ in the security chain as there are no rules or patches that can be applied to protect their vulnerabilities (Mitnick, 2002).

The ability to detect social engineering and deception differs between individuals. Factors such as truth-bias, stereotypical thinking and processing ability form the basis of human judgement (Burgoon, Qin, 2007). As humans have different personalities and varying levels of perception, this brings with it different vulnerabilities and weaknesses which a talented social engineer can detect and exploit (Mitnick, 2002).

Social engineering is considered to be a high risk threat to the protection of personal and sensitive data. However, at this stage there is a distinct lack of factual evidence to support such a statement (Karakasiliotis, 2006). The existence of social engineering to date is merely supported by anecdotal evidence and as such makes it unquantifiable. An assumption is made that the reason for the lack of tangible evidence is to prevent embarrassment to both individuals and organisations. In addition, public knowledge of a successful social engineering attack could be damaging to a company’s reputation and call it’s integrity into question.

Social engineering has become more prevalent over the last five years (Grant, 2007) and surveys have been conducted to identify different aspects of socially exploited vulnerabilities. The following social engineering techniques have been defined:

2.1 Pretexting

Pretexting is a technique which involves creating and using an invented scenario in order to dupe the intended target into divulging personal and or sensitive information. This technique is usually executed over the telephone and normally requires an amount of prerequisite knowledge about the victim. This prerequisite knowledge can usually be acquired by researching public information resources, such as those listed on the previous page (Federal Trade Commission, 2006).

2.2 Phishing

Phishing, also known as ‘brand spoofing’ or ‘carding’ is the attempt to falsify or forge a legitimate company’s e-mail address or website in order to scam an e-mail recipient into providing personal and sensitive information. Phishing criminals aim to obtain information such as login credentials, credit card information and identity details. The technique of phishing has been around since 1995 but became more prominent in July 2003 when criminals began to actively target large financial institutions; namely E-Loan, Wells Fargo, E-Gold and CitiBank (Lance, 2005).

The most prominent methods of phishing to date are email forgery, false websites, caller identification spoofing, cross-site scripting attacks and malware/Trojans (Lance, 2005).

2.3 Pharming

Pharming is a more insidious variation of Phishing. Its fundamental technique is the same as phishing in that it uses forged websites to capture personal and sensitive information. Pharming, however, redirects a user to a false website as they attempt to access a legitimate website. This redirection, otherwise known as 'domain spoofing' can be initiated by an emailed virus that lies dormant on the victim's computer until the specific web address (URL) is entered. An automatic redirection can also be facilitated by poisoning the Domain Name System (DNS). Once a computer is infected and the user is redirected to a false website then any information entered will be captured by hackers (Cisco Systems, 2007).

2.4 Evil Twins

The 'Evil Twins' technique is again a variation of phishing. Evil twins offer users a wireless connection service and look identical to one a user would find in any Wi-Fi hotspot or internet cafe. As the broadcasted Wi-Fi connection looks identical to legitimate connections, it is almost impossible for the victim to differentiate between the two. Once the user is connected to the rouge access point, fraudsters are able to capture credentials and credit card details by using a man-in-the-middle (MITM) attack (Delaney, 2005).

2.5 Interactive Voice Response

Interactive Voice Response (IVR) is a phone technology that enables a computer to detect voice and touch tones using a normal telephone call. Fraudsters use rouge IVR's to replicate a legitimate copy of an organisation's IVR system. Typical target organisations include banks and other financial institutions. This scam normally relies on generating a need for the customer to phone into the rogue system and this can be achieved by the sending of a Phishing email. The rogue IVR system will request that the user inputs their relevant personal and sensitive, which in turn gives the social engineers full access to the victim's exploited accounts (Microsoft, 2006).

3 Demographics

Respondent demographics varied in age, gender, levels of education and countries of origin. Such information was collected throughout the survey to establish whether or not the aforementioned variables affected demographics responses. Indeed it was revealed that none of these variables significantly influenced demographics responses and in fact individuals of all ages, levels of education and countries of origin lacked awareness regarding social engineering exploits.

A total of 86 responses were collated. 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.

4 Computer Security

The study investigated and measured user's awareness of basic computer security as well as the security based resources available to them. Respondents were asked where they use 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 installed and the frequency to which they updated it.

The survey revealed that the majority of respondents spent more than four hours online a day and applied the latest security updates to their computer upon release. The survey revealed that males spent more time online than females and as such had a better understanding of computer security. Additionally, younger respondents, the majority of whom were heavy users (spending more than four hours online daily) had a better awareness of security issues and as such protected themselves more effectively against potential security threats. It was likely that this was due to the fact that younger demographics had far greater exposure to computers from an early age unlike older respondents who would not.

A comparison was drawn between respondents from developed and undeveloped countries. It was assumed that respondents from developed countries would have a better understanding of computer security than respondents from undeveloped countries. This assumption was based on the fact that developed countries are more likely to have a greater number of computational resources than undeveloped countries. Indeed it was revealed that there was little difference between responses between developed and undeveloped countries. In fact it was found that respondents from undeveloped countries had a better understanding than those from developed countries. This outcome was due to the fact that respondents from undeveloped countries were postgraduate students of the University of Plymouth.

Comparisons were drawn between respondents with varying qualifications. It was assumed that higher qualified respondents would respond more favourably than those with fewer qualifications. It was found that the results did not support this hypothesis and in fact there was little difference between responses. Respondents in the 'No Qualifications' group and 'GCSE' group all had a firewall installed whereas higher qualified respondents did not or were unsure. Additionally 17% of respondents with Bachelors Degrees and 11% of respondents with Masters Degrees did not have an antivirus package installed. These results indicate that higher qualified respondents may well have a better understanding of computer security but are complacent about the need for it.

Additionally results were compared between respondents who had previously undertaken one or more security modules and those who had not. It was found that respondents who had not previously undertaken security modules performed worse than those who did. 10% of respondents who had undertaken security modules did not have an antivirus package installed where as 100% of the respondents who had not undertaken security modules did have antivirus protection. Moreover 35% of respondents who had undertaken security modules did not have an anti spyware package installed whereas 100% of the respondents who had not undertaken security modules did have anti spyware protection.

5 Security Awareness

The survey further measured respondent's attitudes towards security. It additionally aimed to understand individual's willingness to take risks which could potentially place themselves or others at risk. Demographics were asked what they would do if their firewall alerted them that their computer was attempting to make a connection to the internet whilst attempting to view a webpage. 23% of respondents claimed that they would continue to view the webpage regardless. 19% stated that they would open the webpage if they knew the source but would close it if they did not. 15% said that they would close the webpage immediately and block the URL and 26% claimed they would investigate the webpage using security facilities such as firewalls and anti virus packages. Surprisingly 2% of respondents stated that they would open the webpage on another individual's computer thereby putting that computer at risk. 15% of the total demographics did not respond.

The above results show a distinct lack of respect and awareness regarding online security and the security of others. It is also apparent that people are unaware of the potential consequences of disrespecting security measures.

Respondents were also placed in a number of hypothetical situations which measured their honesty as well as their understanding of the importance of security. Demographics were asked what they would do if they received an email from their bank asking them to login with their credentials. 72% of both male and female respondents stated that they would phone the bank and ask for more details. 28% of males and 9% of females stated that they would click the link and sign in as requested, leaving 18% of females who would visit the site later.

The second question asked respondents what they would do if they believed that a friends computer had been infected with a virus whist they were surfing the internet. 64% of male respondents and 74% of female respondents stated that they would immediately inform the individual. 3% of males and 27% of females would leave the owner to find out later leaving 33% of males who would try and fix the problem themselves. The results show that a percentage of respondents are willing to leave another individual vulnerable to exploitation instead of owning up to their own mistakes. Leaving a computer which has been infected could at least lead to data corruption and theft.

Respondents were then asked what action they would take if they noticed that a work colleague had left their computer logged on with Microsoft Outlook running in the taskbar. 31% of males and 27% of females stated that they would lock the colleague's computer. 53% of males and 55% of females would inform the individual. 10% of males and 9% of females would shut the computer down and 2% of males and 5% of females would look through personal files and emails. Overall the responses to this question were mostly positive; however a small number of demographics admitted that they would invade the privacy of others.

The survey proceeded to ask demographics what they would do if they got to work one morning and realised that they left their access card at home. 34% of males and 55% of females would follow someone else into the building and continue their day. 60% of males and 36% of females would go to the card office and obtain a temporary card for that day leaving 5% of males and 9% of females who would go home and collect their own access card. This question measured demographics understanding of the importance of security policies. In this instance access cards are used to identify employees. If such policies are disregarded then an organisation is more vulnerable to social engineering attacks due to the fact it will be more difficult to differentiate between legitimate employees.

Finally respondents were asked what they would do if a friend, who had owed them money for sometime had left their online banking account logged on. 97% of males and 82% of females stated that they would not transfer the funds owed to them leaving 3% of males and 18% of females that would. This question measured a respondent's level of trust. Transferring funds without the owner's authorisation could have constituted theft.

6 Social Engineering

Demographics were presented with five different emails and asked to identify them as legitimate or illegitimate. Four out of the five emails were illegitimate and were in fact Phishing emails (section 2.2). The aforementioned emails are detailed in table 1.

Question	Correct Answer
1. Amazon.co.uk Email	Illegitimate
2. Halifax Bank Email	Illegitimate
3. Ebay Security Email	Illegitimate
4. Ebay Powerseller Email	Legitimate
5. PayPal Tsunami Appeal Email	Illegitimate

Table 1: Correct answers for social engineering emails

Male – 77% of male respondents correctly identified the Amazon.co.uk email as being illegitimate and 23% did not. 83% correctly identified the Halifax email as being illegitimate and 17% were incorrect. 62% correctly identified the Ebay Security email as being illegitimate and 38% did not. 65% incorrectly identified the Ebay Powerseller email as being illegitimate and only 35% identified it as being legitimate. 72% correctly identified the PayPal Tsunami Appeal email as illegitimate and 28% did not.

Female – 80% of female respondents correctly identified the Amazon.co.uk email as being illegitimate and 20% did not. 67% correctly identified the Halifax email as being illegitimate and 33% were incorrect. 47% correctly identified the Ebay Security email as being illegitimate and 53% did not. 53% incorrectly identified the Ebay Powerseller email as being illegitimate and only 47% identified it as being legitimate. 73% correctly identified the PayPal Tsunami Appeal email as illegitimate and 27% did not.

The results revealed that regardless of age, gender, country of origin or level of education, none of the surveyed demographics were able to correctly identify all of the emails presented to them. This in turn showed a distinct lack of awareness and understanding of social engineering techniques.

7 Social Networking Websites

Demographics were further asked if they were members of a social networking website. If the answer to that question was ‘Yes’ then the demographics were presented with a list of possible details which are most commonly found on social networking websites. By analysing what details respondents were prepared to post online, their level of vulnerability could be measured.

Out of the total 86 respondents 67 (78%) were members of one or more social networking websites leaving 19 (22%) who were not. The results are displayed in table 2.

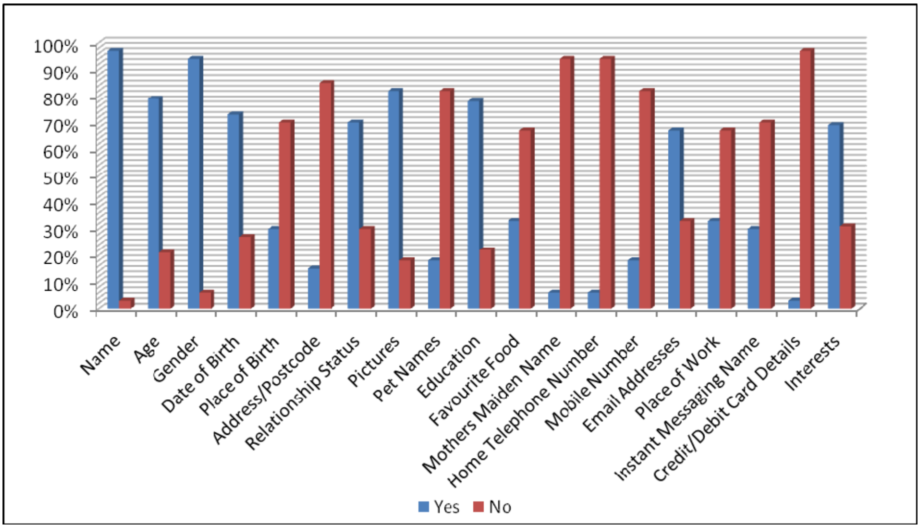

Figure 2: Social Networking Respondent Answers

Figure 2 shows a statistical view of the responses generated in section 5. From studying the results shown in table 2 and figure 2 it is clear that a number of users of social networking websites are highly vulnerable to social engineering attacks.

Name	97% of respondents posted their name on a social networking website leaving 3% who would not.
Age	79% of respondents posted their age on a social networking website leaving 21% who would not.
Gender	95% of respondents posted their gender on a social networking website leaving 5% who would not.
Date of Birth	73% of respondents posted their date of birth on a social networking website leaving 27% who would not. Dates of birth are personal to an individual and are often used for identification purposes.
Place of Birth	30% of respondents posted their place of birth on a social networking website leaving 70% who would not. Such information is used for identification purposes and password reset facilities.
Address and Postcode	15% of respondents posted their address and postcode on a social networking website leaving 85% who would not. Various parts of addresses and postcodes are nearly always used when verifying a person's identity.
Relationship Status	70% of respondents posted their relationship status on a social networking website leaving 30% who would not.
Pictures	82% of respondents posted pictures of themselves on a social networking website leaving 18% who would not. Pictures enable social engineering to visually identify their targets and as such this facilitate easier exploitation.
Pet Names	18% of respondents posted the names of their pets on a social networking website leaving 82% who would not. Pet names are often used as security questions to enable access to more personal and sensitive information namely passwords.
Education	78% of respondents posted their educational background on a social networking website leaving 22% who would not. Educational details are often used in security questions; for example 'What was the name of your first school?'
Favorite Food	33% of respondents posted their favourite food on a social networking website leaving 67% who would not. Details of favourite food are often used in security questions.
Mother's Maiden Name	6% of respondents posted their mother's maiden name on a social networking website leaving 94% who would not. Mother's maiden name is a very common question used in verifying a person's identity.
Home Telephone Number	6% of respondents posted their home telephone number on a social networking website leaving 94% who would not. Social engineers often use a telephone to execute a technique known as 'pretexting' (Section 2.1)
Mobile Number	18% of respondents posted their mobile telephone number on a social networking website leaving 82% who would not. Pretexting is also facilitated using mobile telephone numbers
Email Addresses	67% of respondents posted their email addresses on a social networking website leaving 33% who would not. Social engineers use email address to target individuals with phishing mail (Section 2.2)
Place of Work	33% of respondents posted their place of work on a social networking website leaving 67% who would not. Social engineers learn the structure of a company's hierarchy in order to pretext desired information.
Instant Messaging Name	30% of respondents posted their instant messaging name on a social networking website leaving 70% who would not. Instant messaging addresses are used by social engineers and cyber criminals to make direct contact to individuals.
Credit/Debit Card Details	3% of respondents posted their credit and debit card details on a social networking website leaving 97% who would not. Respondents who posted such information online are very susceptible to fraudulent attacks from social engineers and cyber criminals.
Interests	69% of respondents posted their interests on a social networking website leaving 31% who did not.

Table 2: Social Networking Website Results

8 Conclusions and the Future

The range of respondent demographics varied considerably in age, gender, country of origin, and educational background. It was found that individual responses did not vary according to the aforementioned variables.

Section 2 found that the majority of respondents held a reasonable amount of knowledge with regards to basic computer security. The results of this section were not influenced by the variables contained within section 1. In order to facilitate a more accurate and meaningful analysis equal participation would be required from demographics of different ages, genders, countries of origins and educational backgrounds.

Section 3 found that a number of respondents had little regard for the need of security and the consequences of not respecting implemented security measures. If individuals do not understand and consequently do not adhere to security practices then they and any organisation to which they work for are likely to be highly vulnerable to social engineering attacks.

Section 4 found that none of the respondents were able to correctly identify all of the emails as legitimate or illegitimate. This clearly indicates that there is a distinct lack of awareness regarding Phishing based attacks. This lack of awareness combined with a lack of understanding and respect for implemented security measures (section 3) heightens the risk of attack on a given individual or organisation.

Section 5 found that many respondents were willing to post a personal profile online containing sensitive information which could be used to gain access to facilities such as password reset tools and telephone banking services.

Each section measured the extent to which different vulnerabilities could be exploited in order to gain access to personal and sensitive data. Section 2 measured people’s awareness of technical security whilst section 3 measured people’s attitudes and respect for the need of security by placing them in hypothetical situations which gave them the opportunity to breach or ignore privacy and security issues. Section 4 measured people’s abilities in detecting the most common social engineering technique known as Phishing. The ability to detect such attacks is crucial given that divulging such sensitive information could lead to exploitation. Section 5 aimed to measure how vulnerable individuals were making themselves by posting a repository of personal information about them online.

This research shows that no matter how well a given system is implemented it is impossible to completely circumvent risk. Hence due to the fact that technology is continuously and rapidly evolving, so are new technical and social vulnerabilities.

In light of the foregoing it is important that organisations and its employees are as dynamic and adaptable as possible. Individuals need to be adaptable to change in order to minimise the threat of exploitation. Many individuals do not like change, particularly within the workplace and as such somewhat prohibits effective security management. In addition it is vital that individuals are aware of the risks and potential consequences of neglecting security procedures. Organisations need to ensure that its employees are fully aware of what security features surround them and their purposes for their implementation and then the employees must ensure that these procedures are completely adhered to.

With regards to future research further monitoring and analysis on the topic of social engineering is critical due to the fact that individuals and organisations underestimate the power that personal and sensitive information gives to cyber criminals. It is recommended that attempts to raise user awareness are implemented and the outline vulnerabilities are surveyed on a regular basis.

9 References

Allen, M., (2006) 'Social Engineering – A Means to Violate a Computer System' SANS Institute USA [Online] Available: http://www.sans.org/reading_room/whitepapers/engineering/529.php?portal=a41a35b5183a4de5bc80070697433f71 [Date accessed: 29th August 2008]

Burgoon, J.K. and Qin, T., (2007) 'An Investigation of Heuristics of Human Judgment in Detecting Deception and Potential Implications in Countering Social Engineering' *IEEE Explore:* 152-169

Cisco Systems Inc. (2007) 'Protect Against Social Engineering' [Online] Available:http://www.cisco.com/web/about/security/intelligence/mysdn-social-engineering.html [Date accessed: 15th January 2008]

Delaney, K., (2005) 'Hackers Use Two New Tricks to Steal Online Identities' The Wall Street Journal May 17th 2005:B1 [Online] Available: http://www.lookstoogoodtobetrue.com/fraudtypes/hacking.pdf [Date accessed: 15th January 2008]

Grant, I., (2007) 'Social engineering on the rise', [Online] Available: http://www.computerweekly.com/Articles/2007/11/27/228312/social-engineering-attacks-on-the-rise.htm [Date accessed: 19th August 2008]

Karakasiliotis, A., (2006) 'Assess User's Security Awareness of Social Engineering and Phishing' MRes Thesis , University of Plymouth: 1

Lance, J. and Steward, J., (2005) 'Phishing Exposed' Sygress Publishing, ISBN: 159749030X

Microsoft USA (2006) 'Phone Phishing Scams Direct You to Call a Phone Number' [Online] Available: http://www.microsoft.com/protect/yourself/phishing/phone.mspx [Date accessed: 15th January 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