A Practical Assessment of Social Engineering Vulnerabilities

T.Bakhshi, M.Papadaki and S.M.Furnell

Centre for Information Security and Network Research, University of Plymouth, Plymouth, United Kingdom
e-mail: cisnr@plymouth.ac.uk

Abstract

Social engineering refers to the selection of techniques that exploit human weaknesses and manipulate people into breaking normal security procedures. This may involve convincing people to perform atypical actions or divulge confidential information. It remains a popular method of bypassing security because attacks focus on the weakest link in the security architecture: the staff of the organization, instead of directly targeting technical controls, such as firewalls or authentication systems. This paper investigates the level of susceptibility to social engineering amongst staff within a cooperating organisation. An email-based experiment was conducted, in which 152 staff members were sent a message asking them to follow a link and install a claimed software update. The message utilised a number of social engineering techniques, but was also designed to convey signs of a deception in order to alert security-aware users. In spite of a short window of operation for the experiment, the results revealed that 23% of recipients were successfully snared by the attack, suggesting that many users lack a baseline level of security awareness that is useful to protect them online.

Keywords

Social engineering, IT Security, Phishing, Deception.

1. Introduction

Social Engineering remains a popular method of compromising the security of computing systems. According to Thornburgh (2004) social engineering has gained profound acceptance in the information technology community as an effective social and psychological tool for exploiting the IT security mechanism of a target organization. Renowned hacker turned security consultant Kevin Mitnick suggests that it is much easier to trick somebody into giving his or her password than to carry out an elaborate hacking attempt for this purpose (Mitnick and Simon, 2002). Such a process may lead to the generation of useful data for the social engineer such as insight into the security policy of an organization, the countermeasures in place and specifics relating to personnel and their level of security privilege for possible use in future attacks. Social engineering often requires a considerable effort in planning and research in order to be successful. Mitnick and Simon (2002) compare a social engineering attack to a software development lifecycle and summarize the process into four steps: research; development of rapport and trust; exploitation of trust; and

utilization of information. From a social engineer's perspective research is vital, as it provides a plethora of information regarding the target that could be used in carrying out an attack. Such information can be gathered from numerous sources. Erianger (2004) and Granger (2001) refer to dumpster diving, suggesting that an attacker may go through the paper waste produced by an organization to gain any general and confidential information that may be useful. The same is also true for shoulder surfing. While investigating a social engineer's research toolkit, Nolan and Levesque (2005) suggest that global search engines such as Google can provide much useful information regarding an organization or an individual. The leads generated as part of this process may serve as further input into the same search engine to gather refined results and help the social engineer carry out a better planned attack. Whichever the method of research employed by a social engineer, the vital ingredient without which successful social engineering attack would not be possible are the people within the organization that is being targeted. The employees of an organization need to be persuaded to give vital information or access relating to the targeted system, and as such proper awareness and training of employees is essential to preserve security.

This paper provides further evidence of users' susceptibility to the problems, by presenting the results of an email-based social engineering study that was conducted amongst staff within a cooperating organisation. The primary aim of the research was to assess the threat that social engineering vulnerabilities pose to IT systems and to raise staff awareness of the threat. Section 2 discusses the existing work in this area, and section 3 describes how the experiment was designed. This is followed by section 4, which presents specific details about the execution of the experiment, and section 5, which provides a critical analysis of results from the study. Finally, section 6 contains conclusions from this work.

2. Background

The investigation of user susceptibility to social engineering threats has been the focus of a number of prior studies. Orgill et al. (2004) used a physical approach, by posing to be an individual from an organisation's computer support department and asking employees for a range of information (e.g. usernames, passwords, etc.). The findings from this study were alarming, showing that around 80% of participants provided their username and almost 60% also provided their password. Greening (1996) used an email-based approach in Sydney University, by sending emails to undergraduate computer science students improperly requesting usernames and passwords in the pretext of intrusion detection and subsequent system upgrade. 47% of students fell for this trick, and provided their valid username and password details. A more recent phishing-type study was mounted by Dodge and Ferguson (2006), who conducted their study as part of information assurance training for students at the United States Military Academy. Students were tested against three scenarios, assessing their willingness to: click an embedded link within an email message; open a .html email attachment; follow a link to a website and provide sensitive information. All exercises revealed significant elements of failure, and helped to

inform the evolution of the Academy's awareness programme and other operational security practices.

A combination of physical and technical approaches was utilised by Secure Network Technologies in the audit of a credit union organisation (Stasiukonis, 2006). Specifically, they developed a Trojan that could email the usernames, passwords and hardware configuration of an employee's system, and then copied the Trojan onto 20 USB memory sticks, which were placed in various places of the organisation. Fifteen of the sticks were found by employees, and all were subsequently plugged into the corporate computers. It should be noted that prior to the launch of the audit, employees had been made aware of the fact that they would be audited on human weaknesses.

A different approach was adopted by Karakasiliotis et al. (2007), who carried out a web-based survey to investigate users' level of susceptibility to phishing attacks by asking them to distinguish whether 20 different messages were genuine or phishing attempts (from a set that actually contained 9 genuine and 11 bogus messages). From the 179 respondents that took part, the results revealed a great level of uncertainty and confusion amongst participants, and a tendency of being overcautious when asked to determine the legitimacy of email messages. Specifically, 32% of messages were incorrectly characterised, and 26% of messages were not characterised at all. Specifically, participants mistook phishing messages as genuine in 28% of cases. Genuine messages were considered as illegitimate in 37% of cases.

Such prior works reveal the considerable vulnerability posed by the end-user community if they are not appropriately aware and attuned to the potential threats. However, given that such threats are now well-recognised in the security domain, it would not be unreasonable to expect organisations to take steps to guard against them. Nonetheless, it is likely that many organisations have work to do in this respect, and will consequently find that their users are still very susceptible to such deceptions.

3. Assessing susceptibility to social engineering in practice

In order to assess susceptibility to social engineering in practice, the authors designed an experiment to mimic the techniques used in realistic social engineering scenarios. An email-based approach was chosen as the basis for the study, with the premise being a message to users asking them to install a software update from an accompanying website. In order to obtain results from a genuine user population, the experiment was conducted within a cooperating organisation, which was interested in what the findings would reveal about their users' level of security awareness (indeed, the intention was not simply to exploit the users as an experimental population, but rather to inform genuine aware-raising activities to the benefit of both them and the organisation). The organisation's IT department was informed of the experiment and advised on the wording of the associated email message

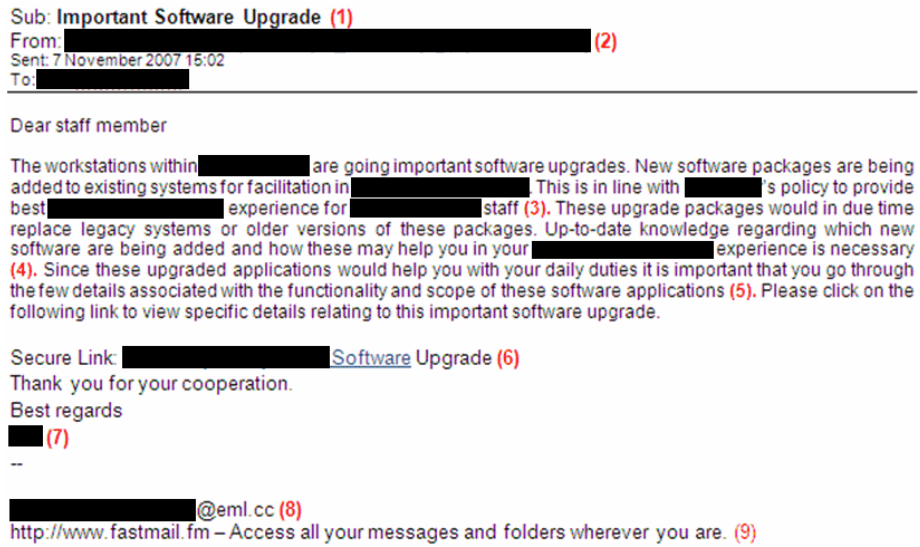
(primarily in order to ensure that it was not too similar to mailings that they might genuinely send).

The participating organisation had an overall staff base of over 2,000 people. However, in order to ensure a manageable experiment, it was decided to target only the staff from within a single department. A key consideration here was to ensure that the experiment was containable in the event of problems (which proved to be a relevant concern once the experiment had begun). The department concerned included a mixture of operational and administrative personnel, but all shared the characteristic of being regular IT users with a need to access email as part of their regular day-to-day duties.

Email was considered to be the best communication medium for the experiment, due to the fact that email addresses of staff could be easily obtained from the organisation's extranet pages, and also because all the members of staff could be addressed individually within a short timeframe, without rising too much suspicion or concern within the department. In addition, email communication is greatly utilised in social engineering attacks, especially phishing. In order to keep the experiment realistic, no insider information was used; instead, all the specific details that were utilised were obtained from a publicly available source; namely the organisation's external website. However, the actual email address that was used for the experiment does not exist.

3.1. Experimental design

As indicated above, the premise of the email was to inform staff of an important software update and prompt them to follow a hyperlink to an external website, where the 'update' could be installed. It should be noted that this is not the way updates are installed within the organisation, and the IT department does not communicate with staff in this way. Therefore, the mere fact that someone was requesting the user to install updates in this way should have been the biggest tell-tale sign of a likely attack. In order to further enable people to recognise the attack, several more tell-tale signs were utilised. Figure 1 depicts the email content, noting that some of the text has been blacked out in order to conceal the name of the organisation involved and the nature of its business. It should be noted that the topic of the email was specifically chosen as something that recipients would be unlikely to feel the need to share and discuss, particularly with anyone outside the organisation. If, by contrast, the message had masqueraded as a virus warning (or some other topic likely to provoke concern and/or have relevance beyond their own organisation) then there would have been a considerable risk of recipients then forwarding it on to others, and thereby creating a potentially large-scale incident in the public domain.


Sub: **Important Software Upgrade (1)**
From: [redacted] **(2)**
Sent: 7 November 2007 15:02
To: [redacted]

Dear staff member

The workstations within [redacted] are going important software upgrades. New software packages are being added to existing systems for facilitation in [redacted]. This is in line with [redacted]'s policy to provide best [redacted] experience for [redacted] staff **(3).** These upgrade packages would in due time replace legacy systems or older versions of these packages. Up-to-date knowledge regarding which new software are being added and how these may help you in your [redacted] experience is necessary **(4).** Since these upgraded applications would help you with your daily duties it is important that you go through the few details associated with the functionality and scope of these software applications **(5).** Please click on the following link to view specific details relating to this important software upgrade.

Secure Link: [redacted] Software Upgrade **(6)**
Thank you for your cooperation.
Best regards
[redacted] **(7)**
--

[redacted]@eml.cc **(8)**
http://www.fastmail.fm – Access all your messages and folders wherever you are. **(9)**

Figure 1: E-mail message sent to staff with classic signs of social engineering

For the purposes of this discussion, a number of elements in the message have been numbered in order to highlight the aspects that were intended to facilitate the social engineering, as well as to give some intentionally suspicious indicators for security-aware recipients:

1. *Attention-grabbing Subject*: The subject field informs the reader about an important software upgrade and prompts the reader for immediate action (possibly opening the content of the email message). The title is quite general, and does not give any specific details of the product that needs to be updated.
2. *Trusted Email Source*: The email appears to originate from the computing services of the organisation. In fact, this email address does not exist, and it has been spoofed to appear genuine. Spoofing email addresses is a trivial task, and plenty of email services available on the internet offer this service for free. This particular email originated from the www.fastmail.fm server which offers email spoofing service to a limited extent.
3. *Confidence Building*: Information is being given in order to increase the reader's confidence prior to the part of the message that asks them to do something.

4+5. *Social Engineering Techniques*: The user is being advised to go through the details of the software upgrade, with the text indicating the benefit to the user and the importance of them doing what is requested (thus utilising two potential psychological triggers).

6. *Trusted Domain*: The reader is being asked to follow a link that appears to be from the organisation's own network. In fact, the link is actually referring to a webpage that is entirely unrelated to the organisation. This facility is again

included in many mail server applications and the present case is using the service offered by www.fastmail.fm.

7. *Generic Sender*: Information regarding the sender is withheld and a generic name was supplied. Although a more convincing deception could potentially be achieved by putting a named contact (particularly if it was a name that staff would be likely to recognise as legitimate), this was deliberately avoided in order to give the message more chances of raising the recipients suspicions.

8+9. *Actual Email Server*: The email service of www.fastmail.fm offers a limited spoofing capability and as such the original sending email server address is appended to each outgoing email. The actual email server address has been left in the email to give the reader another clue as to what is actually happening.

Any recipients clicking the link in the email were forwarded to an external website, which was intentionally badly designed in order to offer further suspicious indications that could prevent people from proceeding with the software installation. Specifically, the webpage tried to imitate the general look of the organisation's own website, but intentionally utilised text and graphics that were in fact one badly pixelated image. Apart from this low resolution image, the webpage also consisted of a button that allowed the members of staff to proceed with the installation. After clicking on the button, the user was directed to a second page, which provided very general information about Microsoft Office (again in an image form), and prompted them to close the browser window.

3.2. Data collection

In order to preserve the anonymity of participants, only two sets of data were collected:

- the unique number of people who clicked the embedded link in the email and visited the first page of the website. This was collected with a javascript counter script that was embedded in the first page of the website.

- the unique number of people who clicked the 'Proceed' button on the first page of the website. This was collected with a cgi-script, and sent an email to the researcher with the date and time of the click action.

It should be noted that, unlike real social engineering attacks, no actual information was collected from the victims, no software was installed on the participants systems, and the security of their systems was in no way compromised in this experiment.

3.3. Operation of the experiment

The experiment received ethical approval from the authors' University, and was launched on the 7th of November 2007. A total of 163 emails were sent between 15:09 hrs and 17:46 hrs on 7 November 2007. The emails were sent via www.fastmail.fm which provides limited spoofing capability for sending email

messages. Emails were sent to each recipient individually. The reason for this was twofold. Firstly, it was important to avoid spamming the organisation's staff, so the gradual submission of traffic across the network would avoid this problem. Moreover, solitary employees can reportedly be more easily manipulated than those in groups (Orgill et. al, 2004). The email could only be delivered to 152 staff members out of 163, as 11 recipient email addresses were unreachable. Hence, the total number of participants in the experiment is considered to be 152.

After running for approximately 3.5 hours, the experiment was ceased and the experiment website was shut down, after a request from the organisation's IT department (who became wary of allowing the study to continue after some respondents had reported the problem to them). Following the termination, a second email explaining the purpose of the original message and the research project was sent to each of the 152 staff members (this time sent from the lead researcher's university email address). In order to limit any consequent concerns, the recipients were assured that:

- no details had been taken from them and their systems had not been affected in any way;
- no-one who followed the link in the email or clicked the 'Proceed' button on the website was individually identifiable;
- anyone wishing their actions to be excluded from the research could contact the investigators (with their identity not being disclosed further).

This email also offered the chance to contact the principal investigators for any concerns regarding the project. Staff members were also given a link to an awareness-raising website (offer additional information about the project and the threat posed by social engineering attacks), and reminded that the IT department would not issue software update requests in this manner.

4. Results

From a security perspective, a desirable response to the email would have been a refusal to follow the embedded link, and prompt notification of IT department about the incident. In reality, the responses were very different. This section analyses the results that were obtained from the study, by conducting both quantitative and qualitative analysis.

4.1. Quantitative Analysis

Out of 152 email messages that were sent, 35 unique staff members (approximately 23%) followed the link within the email message and visited the experiment website. The bulk of these users (~21) visited the experiment website between 16:00 hrs and 17:20 hrs while email messages were still being sent. This can be related to the fact that this is a time when most of the staff members in the organisation would be

checking their email messages in office before official closing hours. Having said that, the following factors could have adversely influenced this percentage:

- The majority of staff members visited the website during the closing hours (16:00-17:30) and it is likely that a good number of recipients would have likely left their offices by the time the email sending process would have finished (17:46 hrs).

- The termination of the experiment website was at a time when the website was still reporting visits and as such the correct percentage of unique visits is likely to have been higher.

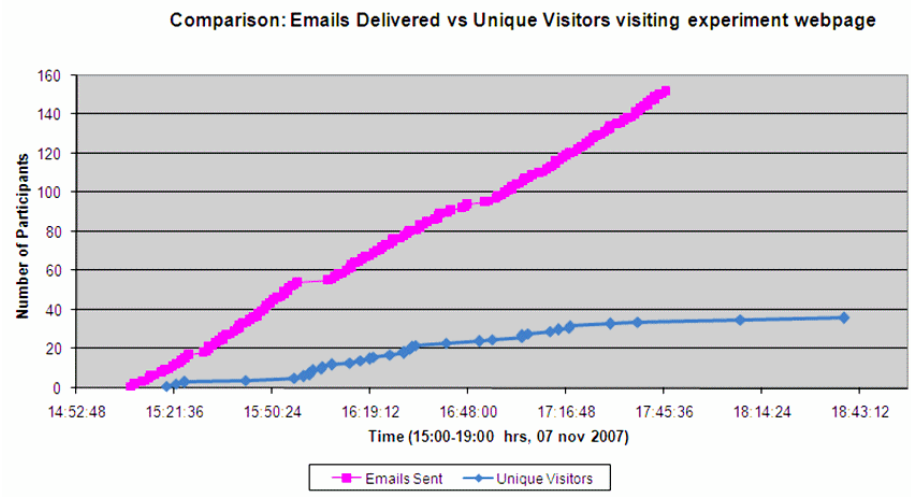


Figure 2: Total Emails Delivered vs number of Unique Visitors

Figure 2 shows the number of unique visitors on the website, and the number of emails that were sent to staff members throughout the duration of the experiment. All the people who followed the link and visited the first page of the website also clicked the 'Proceed' button to install the claimed update. This can be evidenced by the number of emails that were generated from the cgi-script, which was the same as the number of unique visitors to the first page. This confirms that the respondents did not accidentally click on the first page, as making the same mistake consecutively is unlikely. It also reveals that even the appearance of a badly presented webpage was not enough to alert respondents and deter them from installing potentially unsafe software. Figure 3 depicts the timeline between visitors clicking the 'proceed' button and unique visitors of the website. It is evident from the Figure that the timing of the two types of incidents is inter-related, which means that there is no evidence to suggest there were cases of respondents clicking on the 'Proceed' button several times, and other respondents only visiting the first page.

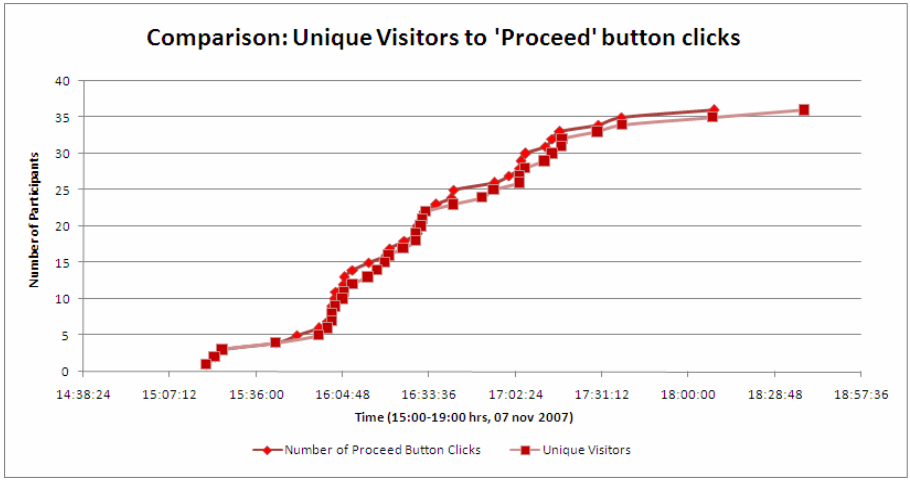


Figure 3: Unique Visitors vs number of 'proceed' button clicks

When comparing the results of the experiment to the results from similar research experiments and surveys, as mentioned in section 2, it is evident that the level of staff susceptibility to social engineering attacks is in some cases comparable, and in others less significant to similar studies. The levels of susceptibility reported by Orgill et al (2004), and Greening (1996) were significantly higher, with results of 60% and 47% respectively. The web-based survey from Karakasiliotis et al (2007) reported 28% of cases when illegitimate messages were mistaken for legitimate. The main difference between these studies is the fact that the first two were conducted in a real-life scenario and therefore one could argue that they reflect a more accurate picture of how respondents react in real life. A potential limitation of Karakasiliotis et al's study is the fact that participants were aware that they were being tested and so may have been over-cautious in their answers. One would expect that the results of the current study, which was conducted in a real-life scenario, would be comparable to the ones from Orgill et al (2004) and Greening (1996). However, two factors are likely to have contributed to the lower figure. Firstly, several aspects of the experiment were intentionally designed to give security-aware users the chance to notice the deception. Secondly, the fact that the experiment was terminated early would have meant that some of the email recipients did not have the chance to read and act upon the message before the associated website was taken off-line.

4.2. Qualitative Analysis

Several issues have been examined in order to gain a better insight into the level of susceptibility of the organisation's staff on social engineering techniques. These are presented in the following sections.

4.2.1. Feedback from participants

After the follow-up explanatory email message was sent to staff, four recipients provided feedback to the investigators, which gave insight into the rationale behind their actions. It should be noted that all 4 users followed the link and clicked the 'Proceed' button. Two users did not detect the social engineering attempt, and one of them admitted to 'installing the software update' without suspecting anything. Their feedback is presented below:

> "You got me! And that is a bit of a wake-up call for me, as I like to believe that I know what I am doing, in terms of not opening emails that look suspicious, and looking at where links take me before I click them. It just goes to show...."
>
> Participant 1

> "Very nifty, one always looks out for phishing using the identity of banks and other large corporations, but one never expects the [the IT department] to be misused for these purposes. I almost fired off an email to [the IT department] to complain about their unprofessionalism. Well done!"
>
> Participant 2

An interesting finding comes from the other two members of staff. Both were suspicious of the email, but nonetheless complied with its instructions, claiming that they did so out of curiosity or concern for security. These participants had incorrectly concluded that it was safe enough to go and take a look at the suspect site, and seemed unaware that merely following the link could have been enough to compromise their system. This suggests that even when a level of threat-awareness has been established, users are still capable of making unwise decisions if they have not received adequate guidance.

4.2.2. Staff's lack of awareness

Another aspect that needs to be investigated is the level of guidance and education that is available to staff by the organisation. Given that there was no security awareness programme in place, the rules and regulations relating to IT policy were examined, in order to find references to good practice on detecting and reacting to social engineering attacks. Documents on IT policy are available on the organisation's website and cover the key factors that users have to take into account while using the IT resources.

After reviewing those documents, it was found that there is very little information available that could support the user to identify a social engineering attempt. Although there is useful general guidance about safe usage of emails, there is no specific reference to social engineering attacks, how they could be detected, and how

users should react to them. The existing rules encourage users to use signatures in order to verify the identity of senders, not to forward virus notifications or chain emails to others, and to report such incidents to the IT department if in doubt. Perhaps the most relevant guideline is the one which prompts users to delete and not open unsolicited emails that contain attachments, as this method is likely to be used to transmit viruses. The same guideline of not opening the content should have been extended to all unsolicited emails, including ones that do not have an attachment but could nonetheless contain a link where the malware could be obtained from. Finally, there is no specific training material that could be used to raise awareness on social engineering. Given the increased popularity of such methods to compromise the security of systems, the need for awareness training is very important.

5. Conclusion

The experiment itself proved to be a very interesting exercise, yet a difficult one to plan and implement, mainly due to the risk of upsetting people in the process. The main challenge was the need to get meaningful and realistic results, without generating ill-feeling. Although approval and support from relevant parties was obtained prior to the experiment, this support was not given until the end.

The results of the experiment clearly revealed a significant level of vulnerability to social engineering attacks. The fact that almost a quarter of the staff members complied with a request that put their system at risk reveals a clear problem, and does not bode well for their chances of resisting a real incident. Moreover, the fact that this level of compliance was observed in spite of an attack that was in many ways signposted as suspicious further reinforces the view that users represent easy targets, and cannot be relied upon to have natural instincts to protect themselves against online threats. As a consequence, the need to raise user awareness of social engineering and the related techniques is crucial, as the success of such methods will otherwise ensure their ongoing use in future attacks.

References

Dodge R. and Ferguson A. (2006), 'Using Phishing for User Email Security Awareness', in *Security and Privacy in Dynamic Environments*, S.Fischer-Hübner et al. (eds), pp. 454-459, Springer, New York.

Erianger L. (2004), 'The weakest link', *PC Magazine*, issue 23, pp. 58-59

Granger S. (2001), 'Social engineering fundamentals, part I: Hacker tactics'. Retrieved April 24, 2007 from http://www.securityfocus.com/infocus/1527

Greening T. (1996), 'Ask and Ye Shall Receive: A Study in 'Social Engineering'', *ACM SIGSAC Review*, vol. 14, no.2, pp. 8-14, ACM Press NY, USA.

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.

Mitnick K. and Simon W. (2002), 'The art of deception: Controlling the human element of security'. Indianapolis, Indiana: Wiley publishing, Inc.

Nolan and Levesque (2005), 'Hacking human: data-archaeology and surveillance in social networks', *ACM SIGGROUP Bulletin,* vol. 25, no.2, pp. 33-37, ACM Press NY, US.

Orgill G.L., Romney G.W., Bailey M. and Orgill P. (2004), 'The urgency for effective user privacy-education to counter social engineering attacks on secure computer systems', *CITC – Proceedings of 5th conference on IT education*, pp. 171-181, ACM Press NY, U.S.

Stasiukonis S. (2006), 'Social Engineering, the USB way', *Dark Reading Online Magazine*, Retrieved 1 June 2007 from
http://www.darkreading.com/document.asp?doc_id=95556

Thornburgh T. (2004), 'Social Engineering: The ''Dark Art'. *InfosecCD Conference,* October 8, 2004, Kennesaw GA, US.

Acknowledgments

This work could not have been conducted without the help of Dr Paul Dowland, who provided feedback on the design and implementation of the experimental approach.