Social Engineering Vulnerabilities

T.Bakhshi and M.Papadaki

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

Abstract

Social engineering refers to the phenomenon of circumventing technical security mechanisms inherent in a system by manipulating legitimate users of the system using a host of physical and psychological compromising methods. This may lead to a compromise of the underlying IT systems for possible exploitation. 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 electronic and cryptographic security algorithms. Universities and academic institutions are no exception to this vulnerability and the present research aims to investigate the level of susceptibility of university staff to social engineering vulnerabilities. This research entailed an experiment involving email based auditing technique directed at staff in the Faculty of Technology, University of Plymouth. The results were analysed from a quantitative and qualitative perspective and compared with results generated from similar experiments to ascertain the level of staff's susceptibility to this threat.

Keywords

Social engineering, IT systems security, Computer security threat

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 then to carry out an elaborate hacking attempt for this purpose (Mitnick and Simon 2002). A social engineer (SE) may bypass the identification process of an organization or a system either individually or by a combination of: counterfeiting IDs, posing to be someone else (e.g. employee, support staff, visitor, etc.) and by compromising a legitimate user/admin staff with necessary privileges who could allow the SE access to the system. Such a process even if ineffective in the first instance may lead to the generation of useful data for the SE 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 requires a considerable effort requiring planning and research to be successful. Mitnick and Simon(2002) while elaborating the art of social engineering compares a social engineering attack to a software development life cycle and summarizes the art into four steps of research, development of rapport and trust, exploitation of trust and utilization of information. Research from an SE’s perspective is vital as it provides a plethora of information regarding the organization which 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 in their discussions suggesting that a SE 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. Nolan and Levesque (2005) while investigating a social engineer’s research toolkit 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 a SE 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 by a SE to give vital information or access relating to the targeted system and as such proper awareness and training of employees regarding this vulnerability can lead to an increased level of security. Employees in universities and academic institutions are not an exception to this vulnerability and a range of social engineering techniques may be targeted at them for compromising the security of their computer systems. In the present research the aim is to analyse whether this is true and assess the faculty of technology staff’s susceptibility to such attacks in University of Plymouth. The University of Plymouth is a public institution with a student population of approximately 30,000. The present project was carried within the faculty of technology; the primary audience being staff of the faculty. The respective faculty has both academic as well as support and administrative staff from diverse educational backgrounds having different levels of IT experience and provides a relatively rich environment for carrying out such a vulnerability study. The primary aims of the research were to assess the susceptibility that social engineering vulnerabilities pose to IT systems within the faculty and to raise staff awareness regarding this peculiar security threat. The following section, section (2) discusses the existing work in this area, section (3) describes the research methodology employed, section (4) analyses the results and section (5) derives the conclusions of this study.

2 Existing research

Similar research has been carried out by Orgill et. al (2004) and Greening (1996) in corporate and educational environments respectively. Orgill et. al (2004) used a physical approach by posing to be an individual from computer support department and asking employees for a range of information (e.g. usernames, passwords, etc.) while Greening (1996) used an email based approach by sending emails to undergraduate computer science students improperly requesting usernames and passwords using the pretext of intrusion detection and subsequent system upgrade in Sydney University. Karakasiliotis et. al (2007) carried out a web-based survey to ascertain the level of susceptibility of unsuspecting internet users to ‘phishing’ attacks under the auspices of Information Security and Network Research Group, University of Plymouth.

Social engineering audits are an important tool for measuring the vulnerability of an organization against social engineering attacks. A well implemented audit can lead to useful results that could be used to further the awareness of staff and employees regarding social engineering vulnerabilities. However, as Jones (2003) suggested there is a considerable lack of procedures regarding social engineering vulnerability audits and has further provided a generic template for carrying out such audits. This fact has been endorsed by Orgill et. al (2004) who consequently used a customized form of the template provided by Jones (2003) for carrying out social engineering vulnerability audit in a corporate organization. Referring to Jones (2003) schema, the social engineering audit is primarily composed of two phases i.e. a pre-audit phase and an auditing phase. The pre-audit phase includes definition of mission objectives, obtaining permission from relevant authorities, etc. while the auditing phase may utilize techniques such as intelligence gathering, physical entry, shoulder surfing, telephone based auditing or email based auditing, etc. The template provided by Jones (2003) serves as a useful example of social engineering vulnerability audits and was customized in the present research according to the requirements at hand as described in the following sections.

3 Research methodology

In accordance with the present research aims the template provided by Jones (2003) served as a useful blueprint. Customization of this template in accordance with the present research formed the basis of the research methodology as described below.

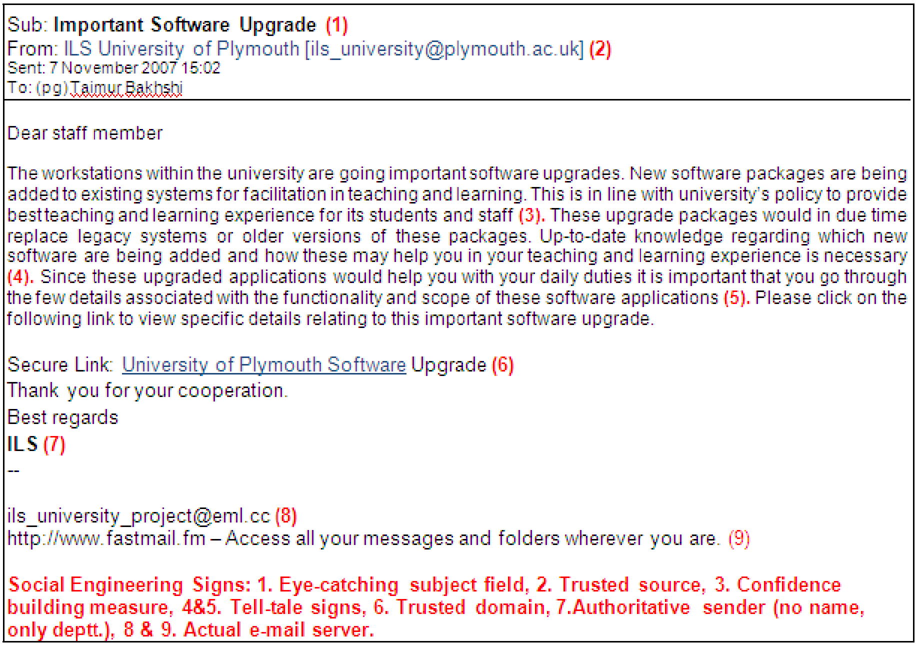
3.1 Pre-audit phase

The pre-audit phase primarily addressed the social engineering auditing technique, background research and experiment approval from concerned bodies. E-mail based auditing technique was employed as the aim was to analyse the implications social engineering vulnerability would have on the security of IT systems and as such e-mail based communication with the staff provided a relevant auditing technique. Hence the associated research experiment used an email based message directed towards staff in faculty of technology soliciting an improper request by the computer support department in the university requiring the user to click on a link embedded in the email message. The webpage would in turn report the unique number of individuals visiting the webpage. The logic here refers to the fact that an analysis of staff's susceptibility to social engineering vulnerabilities can be can be made judged by considering whether they are able to identify this as a social engineering attempt or not. Karakasiliotis et. al (2007) conducted similar survey based study using twenty questions each having an email message from companies, banks, etc. and requiring the participant to judge the legitimacy of the message.

Subsequently, email addresses of faculty staff had to be accounted and 152 email addresses of a total faculty staff of approximately 165 were retrieved from the university website. Finally approval from the relevant departments the Information and Learning Service (ILS) and faculty of technology Ethics Committee were sought for the research experiment. This was furnished on conditions that the security of the staff clicking on the embedded link would not be compromised in any way (i.e. no account of staff names, IP addresses would be stored) and that the staff would be explained purpose of the research at the end of the experiment with the provision that staff may opt out from the results of the study on request. These conditions were adhered to and an explanatory email was sent to staff at the end of the experiment with further link to social engineering identification resources.

3.2 Auditing Phase

The auditing phase included the design of the actual email message containing tell-tale signs of social engineering informing the staff of an important software upgrade and requesting embedded URL to be clicked which would direct the user to an external website emulating to be the university website providing innocuous information about MS Office 2007 and related products. Tell-tale signs of social engineering had been included in order to give the staff a fair chance to spot this attempt. The associated website comprised two web pages and two separate tools were used to report the number of visitors to the website. These included a cgi-script reporting the number of visitors visiting both pages and an invisible counter (java-script) reporting both the unique number of visitors as well as total hits to the website. The content of the email sent to staff is given in Fig.1 with pointers highlighting social engineering signs.



Sub: **Important Software Upgrade** (1)
From: ILS University of Plymouth [ils_university@plymouth.ac.uk] (2)
Sent: 7 November 2007 15:02
To: (pg) Taimur Bakhshi

Dear staff member

The workstations within the university are going important software upgrades. New software packages are being added to existing systems for facilitation in teaching and learning. This is in line with university's policy to provide best teaching and learning experience for its students and 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 teaching and learning 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: University of Plymouth Software Upgrade (6)

Thank you for your cooperation.

Best regards

ILS (7)

--

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

Social Engineering Signs: 1. Eye-catching subject field, 2. Trusted source, 3. Confidence building measure, 4&5. Tell-tale signs, 6. Trusted domain, 7.Authoritative sender (no name, only deptt.), 8 & 9. Actual e-mail server.

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

4 Results

The research experiment was conducted on November 7, 2007 and 152 email messages were sent to staff members. Instead of carbon copying the email message to all the 152 individuals, each email was sent individually. The reason for sending each email individually was twofold. Firstly, it was important avoiding spamming university'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). It was perceived that on receiving an email message reporting 'software updates' by ILS and noting the 'fishy' signs, staff could have looked at other recipients of the same message and contacted them regarding the issue rather than ascertaining the legitimacy of the message themselves, or perhaps contacting the apparent sender of the message (in this case ILS) before following the message which would be a positive sign (i.e. employee's resistance to comply with an improper request).

4.1 Quantitative Analysis

Out of 152 email messages sent, 35 unique staff members (approximately 23%) followed the content of the email message and visited the experiment website. The first email was sent to faculty of technology staff at 15:09 hrs and the last email at 17:46 hrs on 07 November 2007. The bulk of the 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 university would be checking their email messages in office before official closing hours. However there are a few biasing factors that may have influenced this percentage:

a) 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).

b) The shut down of experiment website was at a time when the website was still reporting visits and as such the correct percentage of staff members visiting the website is likely to have been more than 23%.

4.2 Qualitative Analysis

From a qualitative perspective it would be useful to compare the results generated by other similar research experiments and surveys mentioned in section 2 to the results of the present experiment.

- Orgill et. al (2004) reported a cumulative result of 59.38% staff of a total of 32, being vulnerable to social engineering by providing their passwords. Greening (1996) reported approximately 47% of end users (university students) out of a total of 291 as being vulnerable. Karakasiliotis et. al (2007) reported approximately 32% of end users out of 179 participants of the 'phishing' survey as being unable to identify an 'illegitimate' email message while another 26% being apparently confused and unable to judge at all.

- The present experiment approximated 23% of 152 staff being susceptible, unable to identify a social engineered e-mail message considering the actual percentage may have been higher. Hence, it can be concluded by experiment results that the percentage of respondents is more or less the same compared to similar studies. This essentially means that social engineering susceptibilities are inherent in university staff as among other computer users such as corporate office workers, university students, general population, etc. and user education regarding this vulnerability is necessary.

- Employee reaction was reported to be a mix in the experiments by Orgill et. al (2004) and Karakasiliotis et. al (2007) and also observed in the present research experiment, some employees clicking the embedded link while the rest querying the relevant computer support department (ILS). The present experiment was slightly different as being a real scenario the reporting mechanism did not account for user comments other than any voluntary response by the staff on receiving sent the explanatory email. While factors such as notion of asserting authority by using the name of ILS, originating email address, URL/Link, forceful language, confidence building measures etc. were incorporated in the research experiment.

The more or less same number of respondents in this experiment compared to similar studies by Orgill et. al (2004), Greening (1996) and Karakasiliotis et. al (2007) could be attributed to the following factors.

4.2.1 Staff's lack of awareness

The IT policies, rules and regulations available on the ILS website provide a modular approach to key factors that the university computer users (including staff and students) have to take into account while using university resources. The rules related to IT policy use which may assumedly be relevant to countering a social engineering attempt as undertaken in the experiment include documents such as Email/Outlook Etiquette (Email 2007) and Good Practice and Marketing and Communications Department guide (Marketing 2006). There is scanty information available in these guidelines that could support the user in effectively identifying a social engineering attempt via an email message and it can be deduced that staff require awareness regarding social engineering vulnerabilities at least from this information channel.

4.2.2 Context of the email message

A good environment for a social engineering audit as described by Greening (1996) and importance of context of the email Karakasiliotis et. al (2007) mentioned by is crucial for the success of a social engineering attempt. Factors that would have biased the result of the experiment and are nonetheless valid and applicable in real social engineering attempts are mentioned below.

a) A week before the experiment the university portal had been updated and was experiencing considerable problems with regards to user access and other technical issues. In such an environment an email from the ILS regarding important software upgrade would not be considered 'un-common'. This was further fortified by the fact that the domain name of the sender's email address had been spoofed to 'plymouth.ac.uk', hence a way of legitimising the sender as being authentic

b) The timing of the experiment could have influenced the results in the sense that by the time the email messages were received most of the staff would be preparing to leave their offices and this ‘rush’ factor could have added to their susceptibility.

4.2.3 Post experiment derivations

After successfully being run for approximately two hours (18:46 hrs)t the experiment has to be halted and a list of all staff email addresses to which the email had been sent be provided due to intervention by ILS. The experiment website was also consequently shut down at 18:50hrs.

The main reason for this action was a misunderstanding in relation to a requirement for the experiment approval by ILS, which wanted the experiment not to appear to originate from them. However, since the name and address of ILS in the email was spoofed and paraphrased, the project supervisor did not think that this particular requirement was invalidated. Also, ILS’s name is present in the university external website (ILS 2007) and so it could have been more easily used in a real social engineering attempt. This of course was not the view from ILS, which led to the termination of the experiment.

Subsequently the ILS wanted to make changes to the explanatory email message. A comparison between the previous email message and modified version revealed two interesting additions by ILS included below.

1. ILS was not the actual sender of the email, ‘ils_university@plymouth.ac.uk’ does not exist

It can be suggested that the staff members may have responded to the same address for contacting ILS regarding further queries. The email address ils_university@plymouth.ac.uk had actually been spoofed and possibly mail sending error would have led to more subsequent explanations by ILS. Hence, ILS wanted to make it clear that it was not the actual sender of the email message and the associated email address did not exist.

2. ILS would in any case never send out links for software upgrades in this manner.

It appears that staff members were unaware that software upgrades would not be sent out in this manner before this incident and may have considered the email to be about a genuine software upgrade. ILS took this opportunity in educating the staff that software patches would never be sent in this manner so that the staff could avoid such scenarios in future.

In conclusion it would be feasible to judge that the email message caused considerable confusion to staff members. It would be appropriate to assume that had an individual with a malicious intent composed such a message originating from an authority such as ILS and requested something improper (e.g., username, password, click on external link, etc.) from the staff members the consequences would have been far shoddier.

5 Conclusion

Having discussed the quantitative and qualitative aspect of the study in detail the following provide a summarisation of the analysis and discussion of the results generated as part of this research experiment.

- 23% of the staff members were in some way or another vulnerable to social engineering attacks this includes the individuals who deliberately visited the website knowing it was a compromising attempt and those who failed to recognize this attempt at all despite the ‘tell-tale’ signs included in the message.

- Approximately 23% of the 152 recipients (faculty of technology) staff being susceptible and unable to identify a social engineered e-mail message when compared to similar experiments by Orgill et. al (2004), Greening (1996) and Karakasiliotis et. al (2007) suggests that the percentage of respondents is more or less the same. This essentially means that social engineering susceptibilities are as inherent in university staff as among other end users including corporate office workers, university students, general population, etc. and user education regarding this vulnerability is necessary.

- In most instances the availability of internal organization structure and policies on dealing with various scenarios is readily available to external public. In the present case this would be the role of ILS, the email addresses and contact details of staff members as well as some general guidelines and escalation procedures related to IT services in University of Plymouth. Such information would be quite useful to a social engineer in executing a well planned compromising attempt.

- The overall context of the email message i.e. using ILS’s name, the timing of the email message, the spoofed originating email address, ‘tell-tale’ sings of social engineering and lack of information among staff regarding the method of software upgrades affected the overall result. Such features are imitated in genuine scenarios and therefore, the experiment provided a factual account of the susceptibility level of staff to social engineering attempts which is almost the same when compared to similar experiments meaning that social engineering poses a considerable threat to computer security.

6 References

Email/Outlook (2007), ‘Email/Outlook Etiquette and Good Practice’. Retrieved on December 21, 2007 from https://exchange.plymouth.ac.uk/intranet///computing/Public/policies/Email%20Etiquette%20ver3.2.pdf

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.

ILS (2007), 'ILS Self-help home accessed via opening hours'. Retrieved on December 21, 2007 from http://www.plymouth.ac.uk/pages/view.asp?page=719

Jones C (2003), 'Social Engineering: Understanding and Auditing'. Retrieved on December 18, 2007 from http://www.giac.org/practical/GSEC/Chris_Jones_GSEC.pdf

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. Retrieved on January 3, 2007 from http://www.infowar.com/index.php?act=attach&type=post&id=11

Marketing (2006), 'Marketing and Communications Department – Policies and Procedures on News Alerts'. Retrieved on December 21, 2007 from https://exchange.plymouth.ac.uk/intranet///computing/Public/policies/News%20alert%20policy.pdf

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 GL, Romney GW, Bailey Mg 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.

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