Improving Awareness on Social Engineering Attacks

A.Smith and M.Papadaki

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

Abstract

Social engineering as a method of attack is by no means a new concept, and can be easily defined as the exploitation of human weakness, gullibility and ignorance. If one was a believer in religion it could be argued that the first case of social engineering was achieved by the devil (the serpent), tricking Eve into eating forbidden fruit, thus releasing knowledge of good and evil into the world, essentially getting someone in a position of trust to perform an action they themselves could not. Social Engineering can be seen throughout history, possibly changing its alias from time to time, but still realising the same results from what is a relatively simple technique. Examples of this can be seen throughout conflicts such as World War I and II, the term 'propaganda' was adopted to describe what was essentially social engineering in a new form, with an attempt to control the attitudes and behaviour on a large scale (Jastrow & Podhoretz, 2000).

However at current within the general IT community and especially amongst home users, the awareness of social engineering and its many implementable techniques is relatively low. The purpose of this research is to build an understanding of all the currently known about trends associated with the social engineering methodology of hacking and discover what attempts are being performed to raise users awareness to these issues. This research will cumulate in the development of an experiment, designed to evaluate the success of a newly designed educational tool based on the research discovered.

Keywords

Social Engineering, Awareness Schemes, Website Design, Learning Sciences

1 Introduction & Background

The technique of social engineering has evolved somewhat over time into a tool now used by the modern hacking community, a method which relies on influence and persuasion to deceive victims into divulging their most sensitive information. A successful social engineer is extremely adept at convincing people that he/she is someone he/she is not. Through this method of manipulation, unauthorised entities can gain access to personal information or secured systems which, by design they should never have access to. This result makes the social engineer an extremely dangerous individual, who is often able to take advantage of people to obtain information, without the use of technology (Mitnick, 2002).

The SANS institute, over the last several years has publicised a worrying statistic within the trends of social engineering, the results from several surveys reveal that

these techniques at bypassing security measures are on the increase. In most high profile organisations around the world, more and more elaborate security systems are being implemented to protect the perimeter of their networks, making it increasingly more difficult for hackers to gain entry with the traditional technological attacks. These systems, although proving very successful at halting the success rate of traditional attacks, are forcing the hacking community to develop new ways to gain access, thus Paller (2007) stated on behalf of the SANS institute, that social engineering seems to be a growing technique of choice for the modern hacker.

The influx of success by social engineering is in no small part attributed to the lack of education amongst users of IT systems. Surveys conducted over the last five years have proved that office workers (people who should be trained to understand the importance of security) are more than happy to give away personal information and security credentials when presented with the right reward or incentive (Wood, 2007). With this being the case for working professionals, it begs the question regarding home and general users, who lack any form of technical training, and their ability to identify and defend themselves against these growing internet based threats.

Due to the flexibility of social engineering, it has been branded by many security consultants as not unlike a disease, which has the ability to morph and disguise itself in new forms every time it is discovered. From this perspective, it shows exactly how social engineering can be a difficult threat to defend against, even if you, as a user are aware of the potential to this threat.

Examples of this can be seen in recent times through the introduction of more complex SPAM email messages, designed specifically with wording and structure to meet the statistical pass requirements of many SPAM filters acceptance policies. Even after methods such as this have been discovered, social engineers have shown the ability to mutate their attempt to include compressed archives, or embedded pictures as new techniques to combat the growing success of SPAM filters. This inability to effectively stay ahead of the growing number of methods has lead to an increasing success rate of these malicious techniques to commit identity theft, fraud and the successful building of botnet farms.

Even with all the current documentation and research which has been performed, social engineering is still not being treated with the respect it deserves. This factor can be attributed at least in part to the sheer number of traditional hacking techniques which have plagued the IT community for decades. Unfortunately this leaves attacks such as phishing, which are growing in number every day, still only being treated as an annoyance by many within the community.

Prevention of social engineering techniques is not only limited by the awareness of users to the threat, but also the effort placed by the social engineer, more than not users are falling for social engineering attacks due to the shear level of professionalism the effort entails, websites and emails which are so convincing that even the most security conscious expert requires time to uncover the underlying malicious intent of the scheme.

A great deal of the research encountered, leads to the conclusion that the most effective way to prevent successful social engineering attacks, is through the education of potentially targeted users. This defence technique, which falls into the category of semantic learning, teaches the users not only to be aware of the end results or the known attacks, but develop a deeper understanding of the principals behind them. This leads to users being able to recognise social engineering attacks which they may not have been originally educated about by recognising the characteristics which are sometimes common to all many techniques.

2 Prior Research into Social Engineering

The current research found indicates that a great deal of work has been done by previous authors into defining the term social engineering and tracking new techniques employed by its users. This includes, but not limited to several well known security organisations that are actively tracking the progress of this technique and attempting to define the damages caused by it. Paller (2007) and King (2002) have both published reports detailing the current level of threat which social engineering poses. Unfortunately this seems to be the extent of the endeavour, lacking any details regarding progressive defence's measures which are being developed by the security community.

Symantec (2006), as a public organisation dedicated to the eradication of malicious cyber crime, have taken to more direct technical methods, and although somewhat biased due to their self promotion, do actively advertise the need for anti-phishing, anti-spyware & adware software, which they themselves provide. The development of these automated tools often fall short of obeying the published "Eight Golden Rules of Interface Design" (Shneiderman, 1997), which are a proposed collection of principals which were derived heuristically from experience and applicable in more interactive systems, the 8 rules are as follows;

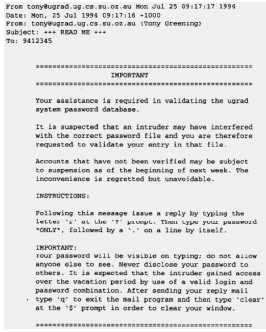
- Strive for consistency
- Enable frequent user to use shortcuts
- Offer informative feedback
- Design dialogs to yield closure
- Offer simple error handling
- Permit easy reversal of actions
- 7 Support internal locus of control.
- Reduce short term memory load

Due to lack of obedience to some of these rules, users have often been found not to understand or necessarily act upon the advice provided (Wu, Miller & Garfinkel, 2006).

Paller (2007) has also stated that the current levels of awareness amongst home user's and businesses is insufficient to combat this growing threat, an opinion which seems to be backed up by works of Plymouth University students Karakasiliotis, Furnell & Papadaki (2007) & Bakhshi (2008) who's efforts lead to similar conclusions, where there is still a distinct lack of awareness amongst users.

Adding to this, a previously undertaken research project by Tony Greening (1996 pp. 8-14) shows the results of an experiment conducted at the University of Sydney aimed at revealing the awareness of students to the vulnerabilities of social engineering, again these results were not positive in favour of the student, showing most had little or no concept of the security threats, though 1996 was some time before the current level of threat that social engineering is now regarded as. This experiment, results published alongside a report entitled 'Ask and Ye Shall Receive' was in line with a perception which reformed social engineer Kevin Mitnick has expressed on several occasions, whereby simply asking for the required information is often enough. Example experiments such as this one, where fraudulent emails are sent to users in an effort to retrieve targeted information are not uncommon and have been used in various studies to test user's abilities to identify social engineering attacks. The Sydney University experiment, as shown in the figure below shows how a simplistic email with address spoofing and well formatted content can provide effective results, in this case out of 338 targeted students, 138 of them responded with their correct credentials to the phishing attempt.

However, some of the most definitive recent work on phishing is displayed in the results from the APWG (2007) survey and shows that the overall awareness of the problem is still not uniform amongst all survey participants, adding to the issues surrounding awareness is the steady number of new phishing attempts, as can be seen from figure 2 taken from the APWG (2007) survey, the numbers of these attempts per month remains consistent throughout the year.



From tony@ugrad.cs.su.oz.au Mon Jul 25 09:17:17 1994
Date: Mon, 25 Jul 1994 09:17:16 +1000
From: tony@ugrad.cs.su.oz.au (Tony Greening)
Subject: +++ READ ME +++
To: 9412345

IMPORTANT

Your assistance is required in validating the ugrad system password database.

It is suspected that an intruder may have interfered with the correct password file and you are therefore requested to validate your entry in that file.

Accounts that have not been verified may be subject to suspension as of the beginning of next week. The inconvenience is regretted but unavoidable.

INSTRUCTIONS:

Following this message issue a reply by typing the letter 'r' at the '?' prompt. Then type your password *ONLY*, followed by a '.' on a line by itself.

IMPORTANT:
Your password will be visible on typing; do not allow anyone else to see. Never disclose your password to others. It is expected that the intruder gained access over the vacation period by use of a valid login and password combination. After sending your reply mail type 'q' to exit the mail program and then type 'clear' at the '$' prompt in order to clear your window.

Figure 1 - Sydney University, Greening (2006)

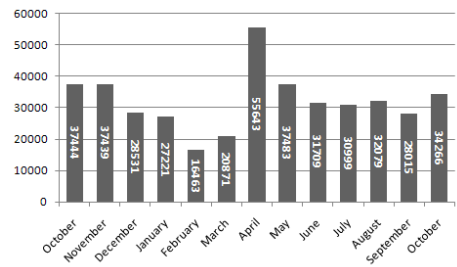


Figure 2 - New Phishing Sites by Month Oct. '06 - 07' (based on figures from the APWG)

3 Existing awareness, deaf ears or definite response

Security awareness is a concept which has not fallen on deaf ears over the years, organisations and home users are constantly harassed by security concerns from their own personal computers or policies in place within their organisations, claims from within the IT community have speculated that user education is a pointless endeavour (Evers, 2006) claiming that security is always a secondary concern to end users and that the true response to enhanced security lies with the developers of applications and systems. Despite these claims, there is significant evidence to say

that well designed security education can be effective (Kumaraguru *et al.*, 2007), where web based training, contextual training and embedded training have all shown to increase users ability to accurately identify an attack.

A study performed by Robila, James & Ragucci (2006 pp. 237-241) which utilised a more direct form of education to the users, with the introduction of a classroom discussion style environment. Subjects were included in an interactive group study session which focused on the threats of phishing and the attributes to be aware of when dealing with such threat, then allowed to take independent quizzes to test this knowledge, results from this experiment provided favourable results that users were better suited to deal with the illegitimate correspondence after their discussion orientation to the subject material.

Many of the technical social engineering methods revolve around the same techniques of fooling the user into submitting their information, primarily it is only the delivery method which changes, via Instant chat (allowing a more persuasive method to be attempted by the attacker) or through pop-up browser windows on legitimate sites (often caused by malware infected servers). Through review of these several other established methods of user awareness, it would seem conclusive that training of user is the most effective way to reduce (but not necessarily eradicate) a users susceptibility to social engineering attacks.

4 Design of a new educational tool

The background research performed in pursuit of this paper have led to the discovery of numerous already in existence social engineering awareness schemes, some details of which can be found in the previous chapter. After careful review of these other attempts and analysis of their relative success the following lists of design features were draw up as a guide of requirements for the creation of a new social engineering awareness tool.

- Comprehensive literature about a wide range of social engineering techniques
- Categorised material
- Links to additional material which is current and either presented in a satisfactory way or complete to the point of no further additions being made.
- Links to recent, past and ‘in the public eye’ news regarding social engineering trends or techniques
- A user quizzes section which allows users to test themselves on their ability to recognise and defend against social engineering attacks.
    - Quizzes should;
        - Be simplistic
        - Be Short
        - Be Multiple Choice
        - Have the ability to copy and paste URL’s (as much as possible)

    - Have the ability to assist the user, in the event they lack the appropriate knowledge to complete the question
    - Contain real world scenarios or examples of real world attack materials
    - Be detailed enough for users to arrive at informed decisions
    - Have questions based on worldwide organisations, not region specific
    - Promote users repeat efforts, implementation of some form of management console to allow quiz management and overview of progress by the user
    - Provide feedback on progress and places for improvement
- Modular design to allow additional *New* techniques and trends to be added easily
- Quick and Simple (average user, not IT specialist) method of adding new content or editing old content when needed
- Contain a spokesperson, a representative entity to which users can turn to for help, or relate the material to (a teacher, mentor or character to associate education with)
- Online assistance to users who have difficulty in using the material provided (user guides to explain the general operation of the site).

4.1 Educational Concept

As has been discovered throughout the research phases, the power of interactive learning systems have been somewhat in doubt until recent years. However, with the publication of results from experiments such as the Anti-Phishing Phil game (Kumaraguru *et al.*, 2007) and endeavors now being attempted by large organizations to create interactive education games, the true power of these efforts is now becoming evident (Havenstein, 2008).

As thus, some of these concepts were incorporated into this attempt at an educational tool and focused on supplying users with an educational experience based around learning science principals. Within the context of this design, the Social Ed website focused on providing a conceptual educational experience, whereby users are presented with material in a form which they can relate to, adding to this is the availability of interaction through the quizzes which has proven to improve the effectiveness of learning skills (Carnegie Mellon, 2007).

5 Experiment & Results

Once the implementation of the social education website was complete, and populated with general educational content regarding social engineering and techniques for defending against it an experiment was designed which requested volunteer users to participate in a trial period of the site, undertaking quizzes and utilising the literature material provided.

All of the results collected throughout this experiment of the project were stored in a MySQL database and left to build throughout this period, approximately 46 subjects

participated in the experiment throughout the trial period, falling into the groups shown in table 1.

Subject Group	Quantity of Subjects
UoP Technical Students	5
UoP Technical Staff	3
Non Technical UoP & Public Organisation Staff	28
UoP Non-Technical Students	5
Non-Technical Individuals	5
TOTAL	46

Table 3 - Social Ed Respondents

Each of these subjects participated in several of the available quizzes, resulting in approximately 327 quiz results being collected within the database. The graph below shows that there was a direct correlation discovered between the pass rates of users in relation to their reading of the provided educational material. Although the results also confirm that users who did not engage in any prior reading before taking the quiz were also successful at attaining pass marks, there is statistically noticeable increase between these two sets of results.

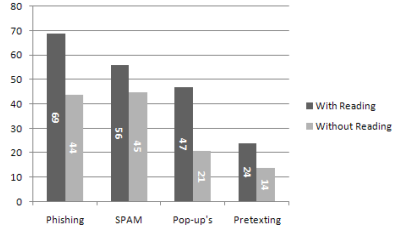


Figure 3 - Social Ed Quiz Pass Results (With and Without Reading)

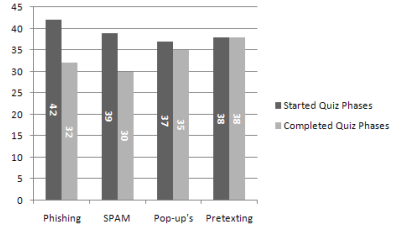


Figure 4 - Completed all Phases on Social Ed Site

In an effort to determine how successful the goal oriented design of the quizzes section was, an analysis was performed on these results to determine how many of the users who performed the available quizzes continued through all phases of testing. As can be seen from the results in figure 4 the overall number of test subjects to complete all the available phases is virtually identical to the number of people who started the quizzes (people who took a phase 1 quiz), this shows that the learning sciences principal of goal oriented design does actively encourages users to pursue a satisfactory result once started.

6 Conclusion

This attempt was designed and approached as a task to actively discover the underlying landscape behind the current trends and techniques of social engineering and the security communities approach to combat these techniques. From the research performed it quickly became evident that the most agreed upon method for

preventing the success of social engineering was through the education of potential victims to the techniques and their inherent characteristics.

In regards to the incorporation of learning science principals to create a goal orientated system with assistive agents, the experiment results also seem to indicate that the created tool actively engages the users and promotes their own inherent want for success. This result is reflected through the analysis of users who not only took part in the quizzes, but without any prompting from the system or invitation to continue with testing completed all available phases of the quiz.

7 References

Apwg (2007) Report for the Month of October 2007, *Phishing Activity Trends.* Available at: http://www.antiphishing.org/reports/apwg_report_oct_2007.pdf (Accessed: 24 January 2008).

Carnegie Mellon (2007) *Anti-Phishing Phil*. Available at: http://cups.cs.cmu.edu/antiphishing_phil/new/index.html (Accessed: 13 December 2007).

Evers, J (2006) *Security expert: User education is pointless*. Available at: http://news.cnet.com/2100-7350_3-6125213.html (Accessed: 5 June 2008).

Greening, T (1996) 'Ask and Ye Shall Receive : A Study in 'Social Engineering'', *ACM Press NY*, Vol 14, ACM Press NY, pp. 8-14. [Online]. Available at: http://portal.acm.org/citation.cfm?id=228292.228295&coll=GUIDE&dl=GUIDE&CFID=437183&CFTOKEN=10292806 (Accessed: 25 January 2008).

Havenstein, H (2008) *Video games poised to boost corporate training*. Available at: http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9113861&intsrc=hm_list (Accessed: 29 August 2008).

Jastrow, R and Podhoretz, N (2000) *Two faces of reality, the Georrge Marshall Institute*. Available at: http://www,marshall.org/pdf/materials/60.pdf (Accessed: 21 December 2007).

Karakasiliotis, A, Furnell, S.M and Papadaki, M (2007) *Advances in Network & Communication Engineering*. 4th edn: University of Plymouth.

King, B (2002) 'Security?, We've Heard of It', *Silicon.com* [Online]. Available at: http://software.silicon.com/security/0,39024888,11032629,00.htm?r=57 (Accessed: 18 January 2008).

Kumaraguru, P, Rhee, Y, Acquisti, A and Cranor, L, F, Hong, J & Hong, E (2007) *Protecting People from Phishing: The Design and Evaluation of an Embedded Training Email System.* Institute for Software Research: Carnegie Mellon University.

Mitnick, K and Simon, W (2002) *The Art of Deception: Controlling the human element of security*: Wiley Publishing Inc.

Paller, A (2007) 'For Questions : Allan Paller', *SANS Institute* [Online]. Available at: http://www.tippingpoint.com/pdf/press/2007/SANSTop20-2007_112707.pdf (Accessed: 22 November 2007).

Shneiderman, B (1997) *Designing the User Interface*. 3rd edn.: Addison Wesley.

Wood, P (2007) 'Social Engineering', *Social Engineering* [Online]. Available at: http://www.fbtechies.co.uk/Content/News/PeteSpeak.shtml (Accessed: 20 November 2007).