Improving Awareness of Social Engineering Attacks

Aaron Smith, Maria Papadaki, Steven M. Furnell

Improving Awareness of Social Engineering Attacks

Aaron Smith[1], Maria Papadaki[1] and Steven Furnell[1]

[1] Centre for Information Security & Network Research, University of Plymouth, Plymouth, United Kingdom, cisnr@plymouth.ac.uk

Abstract: Social engineering is a method of attack involving the exploitation of human weakness, gullibility and ignorance. Although related techniques have existed for some time, current awareness of social engineering and its many guises is relatively low and efforts are therefore required to improve the protection of the user community. This paper begins by examining the problems posed by social engineering, and outlining some of the previous efforts that have been made to address the threat. This leads toward the discussion of a new awareness-raising website that has been specifically designed to aid users in understanding and avoiding the risks. Findings from an experimental trial involving 46 participants are used to illustrate that the system served to increase users' understanding of threat concepts, as well as providing an engaging environment in which they would be likely to persevere with their learning.

Keywords: Social Engineering, Awareness Raising, Learning Sciences

1. Introduction

Social engineering relies on techniques such as influence and persuasion to deceive victims into breaching security and divulging their most sensitive information [1]. 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 that, by rights, they should never have access to. This makes the social engineer an extremely dangerous adversary, who is often able to take advantage of people to obtain information, without the use of technology [2].

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 [3] 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 [4]. 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 that 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 that 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 sheer 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. Emerging attacks, such as spear phishing (which are individually tailored for specific targets), provide evidence of such trends.

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 also to develop a deeper understanding of the principals behind them. This leads to users being able to recognise social engineering attacks that they may not have been originally educated about by recognising the characteristics that are sometimes common to all many techniques.

2. Social Engineering Threats

A review of the literature 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. Unfortunately this seems to be the extent of the endeavour, lacking any details regarding progressive defence measures that are being developed by the security community.

Paller [3] has stated that the current levels of awareness amongst home users and businesses is insufficient to combat this growing threat; an opinion which seems to be supported by work of [5] whose efforts demonstrate users' frequent inability to distinguish social engineering attempts from genuine communications (when considered in the context of email and phishing), as well as their tendency to base their judgments upon inappropriate criteria.

Adding to this, research conducted by Greening [6] 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. In this case, out of 338 students targeted using a simplistic email with address spoofing, 138 responded with their correct credentials. Although practical instances of such messages have become much more widespread since 1996, subsequent experiments of a similar nature do not inspire any greater confidence in users' abilities to identify social engineering attacks [7,8].

However, findings results from the Anti-Phishing Working Group show that the volume of the problem remains significant, with an average of over 25,600 unique phishing scams being identified per month in Q2 of 2008 [9]. As such, from just this vector alone, users have a significant potential to encounter social engineering, and a chance of falling victim to it if they are not appropriately attuned to the threat.

3. Promoting Awareness of Social Engineering

Although some have speculated that user education is a pointless endeavour [10], claiming that security is always a secondary concern to end-users and that the true response to enhanced security lies with applications developers, there is significant evidence to suggest that well-designed security education can be effective [11]. Indeed, web-based training, contextual training and embedded training have all been shown to increase users ability to accurately identify an attack.

A study performed by Robila et al. [12] utilised a more direct form of user education, 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 email, Instant Messaging (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.

Following the review of previous works and an analysis of their relative success the following elements of content were considered desirable to guide the creation of a new social engineering awareness website:

- Awareness-raising material about a wide range of social engineering techniques
- Links to supporting material such as news reports regarding social engineering trends or techniques
- Quizzes allowing users to test their own ability to recognise and defend against social engineering attacks.
- Online assistance to users who have difficulty in using the material provided (e.g. user guides to explain the general operation of the site)

While it would be fair to say that the power of interactive learning systems has been somewhat doubted in the past, the publication of results from experiments such as the Anti-Phishing Phil game (see http://cups.cs.cmu.edu/antiphishing_phil/new/index.html) and endeavors now being attempted by large organizations to create interactive education games have meant that the true power of these efforts is now becoming evident [13]. As such,

some of these concepts were incorporated into this attempt at providing an educational tool, and focused on supplying users with an educational experience based around learning science principles.

In order to further support the user, and to enhance the identity of the site, it was considered useful to incorporate a character that users can turn to for help, or relate the material to. The character in question, named Edward, acts as the user's teacher and mentor during the use of the site, as depicted in Figure 1.

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 can improve the effectiveness of learning skills [11].

Figure 1 The main interface of the Social-Ed site.

The system is based upon a modular design, in order to allow content relating to additional techniques and trends to be added easily. In the first instance, however, the prototype implementation covered phishing, spam, pop-ups and pretexting. These topics were selected based upon their severity, and their relevance to end-users in an organizational context. For example, phishing is one of the most common online forms of social engineering, manifesting itself through emails and fraudulent websites aimed at fooling a victim into divulging their personal details [14]. Spam is quite possibly one of the original technical social engineering methods, and it is essentially unsolicited email that often promises something to the victim that may not always have a genuine basis. Pop-ups have similar characteristics, but arrive in a web-browsing context and very often seek to trick the recipient by claiming to be an offer or a warning. Spam and pop-ups can

be mostly characterized as annoying rather than dangerous to most end users, however they represent threats that are extremely common and difficult to avoid, given the sheer number of examples that are encountered every day [15]. Finally, pretexting is a very common social engineering technique that involves an attacker having a pre-determined target and planning their attack methodically to achieve success. The act of inventing a scenario which can be used by the social engineer to persuade their victim to release the information they require is far more than a simple lie, often background research must take place to build up to the final 'targeted' information [16].

4. Experimental Findings

Once the implementation of the website was complete, and populated with content covering social engineering attacks and defences, an experimental trial was mounted in order to assess the usefulness of the approach in practice. A total of 46 subjects participated in the experiment, with the participant base largely drawn from students and academic staff, and incorporating a mix of technical and non-technical backgrounds.

The website itself was populated with general educational content regarding social engineering threats, and techniques for defending against them, based upon information gathered during the research phase of this project. Several primary quizzes were implemented within the scope of the project using real world examples of social engineering attacks. Proven phishing attack sites, which were retrieved from the Anti-Phishing Working Group (APWG) website were implemented as screenshot questions and annotated for the purposes of these quizzes. Several spam-related quizzes were created using tagged spam mail from personal email accounts and also further examples from the APWG archive. Further quizzes were also developed on the topics of Pop-Ups and Pretexting. However, less emphasis was placed on the populating these aspects, as they are less prominent amongst the deceptions that users might encounter.

Quizzes on the different topics were graded according to the level of assistance available from Edward. In phase 1 and 2 quizzes, users were provided with hints applicable to the question shown, providing them with the valuable 'life line' evidenced in the Anti-Phishing Phil game. Phase 3 quizzes were void of this feature, and consequently users who reached the final phase of the quiz were alone in their efforts to succeed. However, no limit was placed on retakes, allowing subjects to fail any phase quiz and retake it at their leisure, introducing a level of motivation to the user to progress to the next phase.

Each of these subjects participated in several of the available quizzes, resulting in 327 quiz results being logged within the database. This information is presented in Table 1, which also indicates how the activities were distributed across the different topic areas represented within the site.

Table 1. Distribution of quizzes taken during the Social-Ed trial.

Quiz category	Phase 1	Phase 2	Phase 3	Total quizzes
Phishing	42	37	34	113
Spam	39	35	30	104
Pop-ups	37	35	NA	71
Pretexting	38	NA	NA	38
Total				327

In terms of the effectiveness, Figure 2 shows a direct correlation between the pass rates of users in relation and their reading the provided educational material. Although users who did not engage in any prior reading were also had some success, there is a noticeable increase between these two sets of results.

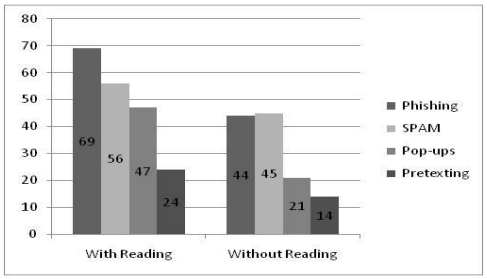

Figure 2 Social-Ed quiz pass results (with and without reading).

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 Figure 3 the overall number completing all the available phases is virtually identical to the number who started the quizzes (people who took a phase 1 quiz), suggesting that the learning sciences principle of goal-oriented design encourages users to seek a satisfactory result once started.

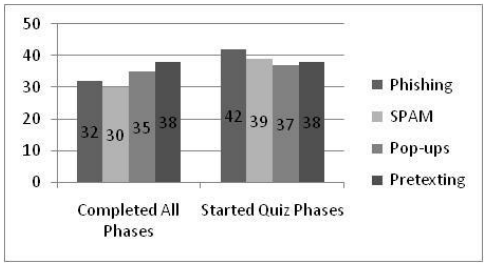

Figure 3 Commencement versus completion of Social-Ed quizzes.

5. Conclusions

A key mechanism for combating social engineering must be the education of potential victims, in order to raise their awareness of the techniques and how to spot them. The research has demonstrated that a web-based approach utilising a goal-orientated system can actively engage users and promote their own desire for success. Further assessment would, however, be advantageous in order to determine the extent to which increased awareness actually reduces the incidence of related breaches.

References

1. Papadaki, M., Furnell, S.M.. Dodge, R.C. Social Engineering: Exploiting the weakest links, European Network & Information Security Agency (ENISA), Heraklion, Crete (2008).
2. Mitnick, K., Simon, W. The Art of Deception: Controlling the human element of security, Wiley Publishing Inc. (2002).
3. Paller, A. For Questions: Allan Paller, SANS Institute, http://www.tippingpoint.com/pdf/press/2007/SANSTop20-2007_112707.pdf (2007).
4. Wood, P. Social Engineering', Social Engineering, http://www.fbtechies.co.uk/Content/News/PeteSpeak.shtml (2007).
5. Karakasiliotis, A., Furnell, S.M., Papadaki, M. An assessment of end-user vulnerability to phishing attacks, Journal of Information Warfare, 6, 17-28 (2007).
6. Greening, T. Ask and Ye Shall Receive: A Study in 'Social Engineering, ACM Press NY, 14, 8-14 (1996).
7. Dodge, R.C., Carver, C., Ferguson, A.J. Phishing for User Security Awareness, Computers & Security, 26, 73-80 (2007).
8. Bakhshi, T., Papadaki, M., Furnell, S.M. A Practical Assessment of Social Engineering Vulnerabilities. In: Clarke, N.L., Furnell, S.M. (eds.) Second International Symposium on Human Aspects of Information Security and Assurance (HAISA 2008), pp. 12--23, University of Plymouth (2008).
9. APWG. Phishing Activity Trends Report Q2/2008. Anti-Phishing Working Group, April-June 2008, http://www.apwg.org/reports/apwg_report_Q2_2008.pdf (2008).
10. Evers, J. Security expert: User education is pointless. http://news.cnet.com/2100-7350_3-6125213.html (2006).
11. Kumaraguru, P., Rhee, Y., Acquisti, A., Cranor, L.F., Hong, J., Hong, E. Protecting People from Phishing: The Design and Evaluation of an Embedded Training Email System. Institute for Software Research, Carnegie Mellon University (2007).
12. Robila, S.A., James, J., Ragucci, W. Don't be a phish: steps in user education, in 11th Annual SIGCSE Conference on Innovation and Technology In Computer Science Education (ITICSE '06), pp. 237—241 (2006).
13. Havenstein, H. Video games poised to boost corporate training. Computerworld, 26 August 2008 (2008).
14. Rhodes, C. Safeguarding Against Social Engineering, East Carolina University, Article at http://www.infosecwriters.com/text_resources/pdf/Social_Engineering_CRhodes.pdf (2007).
15. Microsoft. How to Protect Insiders from Social Engineering Threats, Midsize Business Security Guidance. http://technet.microsoft.com/en-us/library/cc875841.aspx (2006).
16. Thapar, A. Social Engineering : An Attack Vector Most Intricate to Tackle, Infosec Writers, www.infosecwriters.com/text_resources/pdf/Social_Engineering_AThapar.pdf (2007).