User security awareness of social engineering and phishing

A.Karakasiliotis, S.M.Furnell and M.Papadaki

Network Research Group, University of Plymouth, Plymouth, United Kingdom
e-mail: info@network-research-group.org

Abstract

Social engineering is a significant problem involving technical and non-technical ploys in order to extract information from unsuspected users. This paper presents an assessment of user resilience to such ploys in the form of email phishing attack. Our experiment used an online web survey which included a mix of legitimate and illegitimate emails and asked users to differentiate between them. A total of 179 participants were involved and the assessment shows that they correctly identified legitimate emails on average of 50%, whereas illegitimate emails were correctly identified on average of 60%. However, in many cases participants who correctly identified illegitimate emails could not reason their selection based on criteria that illustrate their security awareness.

Keywords

Social engineering, phishing, attack, security, awareness, criteria

1. Introduction

Social engineering is a significant and crucial threat that to information system security, both in its own right and as a technique within other threats such as phishing, vishing, and malicious attachments. Over the last few years various sources have highlighted some basic information about the kind of techniques that were used, the success rate of this attacking method and its relation to the user behavior (Leyden, 2004; BBC News, 2005; Silicon.com, 2006).

Harl (1997) defined social engineering as "the art and science of getting people to comply with your wishes. It is not a way of mind control, it will not allow you to get people to perform tasks widely outside of their normal behaviour and it is far from foolproof". Many other authors, such as Allen (2006), have established this definition as the most common describing term of social engineering in information systems. Nonetheless, it is extremely difficult for someone to define social engineering within just a couple of sentences, because of the myriad ploys that may be involved. So, to add more detail, social engineering is the term that refers to a 'hacking' method in which the attacker exploits the user's behaviour via a series of psychological or/and social ploys, and through technical or/and non-technical communication processes, in order to gain the user's trust and achieve desired result (normally in terms of getting them to part with information).

The purpose of this paper is to assess user awareness of social engineering threat through phishing attacks.

2. Background

The techniques that attackers may use to extract information from users can be separated in two main categories, namely psychological and technological methods. In our experiments these two approaches were analyzed together in the context of phishing emails.

According to research on the topic of social influence (Petty and Cacioppo, 1986) the main human behaviours that are based on judgment can be separated in two categories that refer to central and peripheral route of persuasion based on the ELM (Elaboration Likelihood Model) theory. Moreover, Cialdiny (2000) mentions that there are six basic tendencies of human behaviour that are responsible for a form of behaviour change-compliance with a request. These influential routes are defined as authority, scarcity, liking, reciprocation, commitment (consistency) and social proof (validation). Furthermore other researchers from the field of information technology have referred to some other behavioural traits such as 'conformity' and the 'desire to be helpful' (Stevens, 2002), as well as factors of 'inexperience' and 'curiosity' (Jordan and Goudey, 2005). In phishing attacks, these influential methods can be implemented through the technique of semantic deception (Fette *at al.* 2006), which is achieved through the language used in the text body of email.

On the other hand the technical method that is used to leverage user trust can be performed in other ways. More specifically, in phishing attacks, technical ploys can be defined based on user visual deception (Dhamija et. al 2006) through multiple techniques. A phishing attack can contain two main steps; a phishing email and a bogus web site. Moreover it is up to the attacker if he will use further techniques, such as malicious attachments (Everett, 2004) in the email in order to exploit a vulnerable to user system or if he will include a hyperlink in the email body. In most common phishing attacks, the URL redirects the user to a bogus web site in order to collect sensitive personal information such as login credentials (username, password) and financial details (account/PIN number), or alternatively to download a malicious file (Forte, 2005).

Visual deception in phishing attacks can be achieved through many technical ploys, such as masking the fraudulent URL to make the email appear legitimate (Huseby, 2004), and stealing HTML code from a genuine web site (in order to create the bogus one by mirroring it) (Drake *et al*. 2004). Other techniques could involve the inclusion of banners, logos and trademarks to give the email and the web site a plausible appearance. Also, in the email part, spoofing the email address of sender and displaying a URL that contains https could be possible. On the other hand, the bogus web site may contain plausible security indicators, such as padlock icon (denoting SSL, Secure Socket Layer) (Dhamija and Tygar, 2005) and security certifications such as VeriSign.

The aim of the research at this stage was to assess users' awareness of social engineering via a web survey that would investigate their knowledge of the above ploys and techniques. In common with other experiments (Robila and Ragucci, 2006;

Dhamija *et al.* 2006), our investigation focused on the email part of the phishing attack and specifically on the participants' ability to identify such techniques.

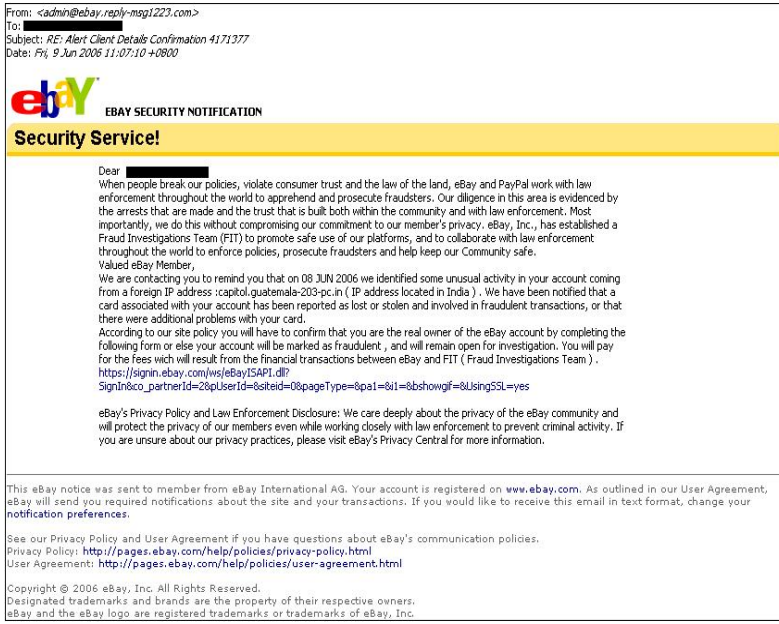
3. Methodology

The experiment used an online survey and included two main sections. The first collected personal information about participants, and included seven questions covering demographic details and technical background (e.g. Internet habits). The second section consisted of 20 questions, each of which presented the user with an email message and asked them to consider whether or not it was genuine or a phishing attempt. Each question had three options (illegitimate, legitimate and do not know) and an optional text box for participants to briefly explain their reasoning.

The demographic questions collected general details such as gender, nationality, and age in order to separate participants into different categories and make a comparison analysis between these categories. In the second part of the demographics we tried to investigate if the security awareness is related to the educational or employment background of the participants. The last part of the demographics asked participants about their internet habits (e.g. online shopping, e-banking, online purchases of bill payments, etc.) and the protection mechanisms (e.g. anti-phishing toolbar) that they use against phishing threat by giving three answering options (yes, no and do not know).

The design of the second part of the survey was more complicated, as it was based on a series of criteria that were related to methods of phishing. So the 20 email questions were separated in two main categories of illegitimate (11 email snapshots) and legitimate (9 email snapshots). As already mentioned above, each question had three possible answers, with the 'do not know' option set as the default..

The main concept of the survey was to benchmark participants' responses to different technical and influential ploys that attackers may include in their emails. The 20 messages used as the basis for the questions were selected from a combination of anti-phishing advisory sites, as well as from emails received by the investigators themselves. The emails included representation from a variety of online services that could be phishing targets (e.g. e-banking 8/20, online-shopping 4/20, online purchases of bill payments 5/20, etc.), as well as a range of different attacking techniques (such as collection of personal and financial information from bogus web site 7/11, downloading malicious software 1/11, opening malicious attachment 1/11, vishing 1/11 and PO BOX 1/11 technique). Figures 1 and 2 below illustrate examples of the illegitimate messages used in the study.


From: <admin@ebay.reply-msg1223.com>
To: [redacted]
Subject: RE: Alert Client Details Confirmation 4171377
Date: Fri, 9 Jun 2006 11:07:10 +0800

EBAY SECURITY NOTIFICATION

Security Service!

Dear [redacted]
When people break our policies, violate consumer trust and the law of the land, eBay and PayPal work with law enforcement throughout the world to apprehend and prosecute fraudsters. Our diligence in this area is evidenced by the arrests that are made and the trust that is built both within the community and with law enforcement. Most importantly, we do this without compromising our commitment to our member's privacy. eBay, Inc., has established a Fraud Investigations Team (FIT) to promote safe use of our platforms, and to collaborate with law enforcement throughout the world to enforce policies, prosecute fraudsters and help keep our Community safe.
Valued eBay Member,
We are contacting you to remind you that on 08 JUN 2006 we identified some unusual activity in your account coming from a foreign IP address :capitol.guatemala-203-pc.in (IP address located in India) . We have been notified that a card associated with your account has been reported as lost or stolen and involved in fraudulent transactions, or that there were additional problems with your card.
According to our site policy you will have to confirm that you are the real owner of the eBay account by completing the following form or else your account will be marked as fraudulent , and will remain open for investigation. You will pay for the fees wich will result from the financial transactions between eBay and FIT (Fraud Investigations Team) .
https://signin.ebay.com/ws/eBayISAPI.dll?
SignIn&co_partnerId=2&pUserId=&siteid=0&pageType=&pa1=&i1=&bshowgif=&UsingSSL=yes

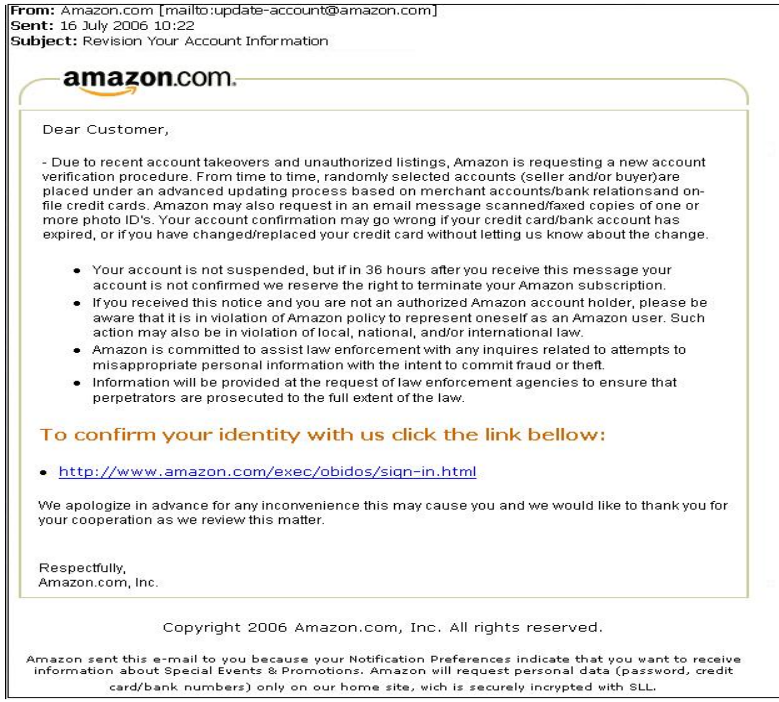
eBay's Privacy Policy and Law Enforcement Disclosure: We care deeply about the privacy of the eBay community and will protect the privacy of our members even while working closely with law enforcement to prevent criminal activity. If you are unsure about our privacy practices, please visit eBay's Privacy Central for more information.

This eBay notice was sent to member from eBay International AG. Your account is registered on www.ebay.com. As outlined in our User Agreement, eBay will send you required notifications about the site and your transactions. If you would like to receive this email in text format, change your notification preferences.

See our Privacy Policy and User Agreement if you have questions about eBay's communication policies.
Privacy Policy: http://pages.ebay.com/help/policies/privacy-policy.html
User Agreement: http://pages.ebay.com/help/policies/user-agreement.html

Copyright © 2006 eBay, Inc. All Rights Reserved.
Designated trademarks and brands are the property of their respective owners.
eBay and the eBay logo are registered trademarks or trademarks of eBay, Inc.

Figure 1: Illegitimate email from eBay


From: Amazon.com [mailto:update-account@amazon.com]
Sent: 16 July 2006 10:22
Subject: Revision Your Account Information

amazon.com

Dear Customer,

- Due to recent account takeovers and unauthorized listings, Amazon is requesting a new account verification procedure. From time to time, randomly selected accounts (seller and/or buyer)are placed under an advanced updating process based on merchant accounts/bank relationsand on-file credit cards. Amazon may also request in an email message scanned/faxed copies of one or more photo ID's. Your account confirmation may go wrong if your credit card/bank account has expired, or if you have changed/replaced your credit card without letting us know about the change.

- Your account is not suspended, but if in 36 hours after you receive this message your account is not confirmed we reserve the right to terminate your Amazon subscription.
- If you received this notice and you are not an authorized Amazon account holder, please be aware that it is in violation of Amazon policy to represent oneself as an Amazon user. Such action may also be in violation of local, national, and/or international law.
- Amazon is committed to assist law enforcement with any inquires related to attempts to misappropriate personal information with the intent to commit fraud or theft.
- Information will be provided at the request of law enforcement agencies to ensure that perpetrators are prosecuted to the full extent of the law.

To confirm your identity with us click the link bellow:

- http://www.amazon.com/exec/obidos/sign-in.html

We apologize in advance for any inconvenience this may cause you and we would like to thank you for your cooperation as we review this matter.

Respectfully,
Amazon.com, Inc.

Copyright 2006 Amazon.com, Inc. All rights reserved.

Amazon sent this e-mail to you because your Notification Preferences indicate that you want to receive information about Special Events & Promotions. Amazon will request personal data (password, credit card/bank numbers) only on our home site, wich is securely incrypted with SLL.

Figure 2: Illegitimate email from Amazon

Other design criteria were based on visual aspects in order to investigate the role that these can play in deceiving the participants. So, 14 emails were colored snapshots

with logos, banners, trademarks, etc. (six legitimate and eight illegitimate), whereas the other six were plain text messages (three legitimate and three illegitimate).

Other characteristics represented in the emails included typos, errors or even grammar mistakes (in 7 of the 11 illegitimate messages). Another language-related factor had to do with the influential techniques that the emails used, with a range of persuasive methods being represented, such as scarcity (2/11), authority (7/11), social proof (2/11) and desire to be helpful (1/11), with some emails including a combination of techniques.

4. Experimental results

A total of 179 participants (75% of whom were male) filled out the survey, which was available on the Internet for a period of 19 days. The requirements for someone to participate to our study were the understanding of the English language (as the emails were written in English) and the use of Internet. The total population of participants included representation from 22 different nationalities, with the majority (97%) having a higher education qualification. In terms of age groupings, 76% were aged 18-29 and 24% above 30.

According to the Figure 3 below that represents the total results of the participants for each question separately we can observe that in most cases, opinions are very divided and there is only a small number of cases where respondents clearly come down to one side (questions 3, 14, and 20) and in some cases they answered dramatically wrong (question 3).

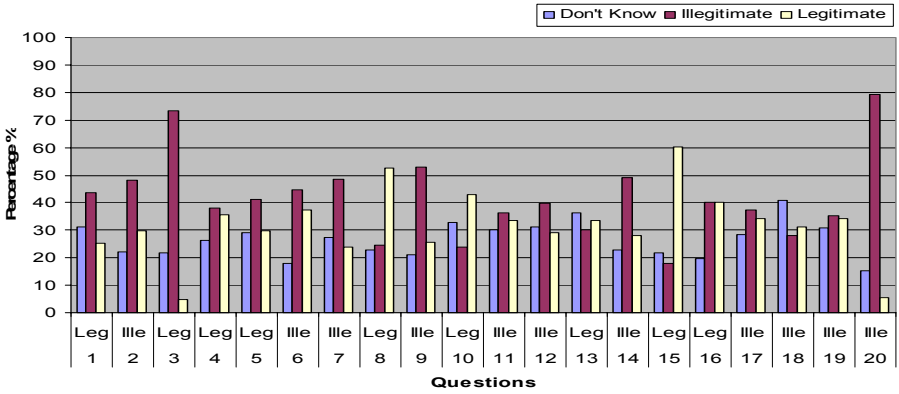


Figure 3: General results from survey

The overall success rate of participants in correctly identifying illegitimate emails was 42%; on the other hand 32% could correctly identify a legitimate email, and 26% selected the 'do not know' option (thus illustrating the confusion of the participants). From the analysis based on demographics we determined that there were no significant differences relating to age or gender, but there were notable changes based on the participants' work/study background. More specifically, 31% of the total population was related to the IT/Computing sector. From these

participants the success rate of identifying correctly emails was 25% for legitimate, 52% for illegitimate and 23% for those that didn't know. Also some changes compared to general results were observed when measuring subsets of participants based on their Internet habits. These changes showed a small increase of success in identifying illegitimate messages, but not as much change for identification of legitimate emails.

Feedback comments were left by 47% of participants, enabling a deeper analysis of their criteria for judgment in each case. We observed that 40 participants made judgments based on visual indicators, such as the presence of logos, banners, trademarks, footer, fonts and copyright symbol. From those participants, 55% selected the legitimate option. The results also showed that a plain text email was more likely to be judged as illegitimate compared to messages with color and images.

Considering the influence of technological factors, 52 participants made a judgment based on whether email contained a URL (70% select the illegitimate option). Furthermore, 26 participants mentioned the fact of http or https, and 39 made a comment about using a verification process (e.g. "have to check this by opening a browser window and typing the given URL into this"). Only 12 of them manually checked the correctness of the URLs and 40 participants made a selection based on the given email address. Considering judgments of personal information, 18 participants gave an answer based whether the email contained a recipient name or not, and 67 participants did so based on other personal information.

From the perspective of language, we understood that 19 participants focused on the language mistakes such as typos and grammar errors. Moreover 34 participants selected answers on the basis of emails that claimed to offer opportunities, while 26 did so based on emails that used forceful language. Also from an analysis of influential techniques it seems that the techniques of authority and desire to be helpful are the least correctly identified from the participants, compared to the techniques of social proof and scarcity.

5. Discussion

Our experiment revealed a significant failure by participants to correctly classify the emails (with average of do not know answers 26%). Comparing our findings to similar studies (Robila and Ragucci, 2006) we highlighted a slight difference in the overall results. More specifically, Robila and Ragucci (2006) mention that participants were able to correctly identify legitimate and illegitimate emails in 60% and 53% of cases respectively. Our findings showed that participants did the same on average of 50% and 60% respectively. However, this difference could possibly exist because of a series of reasons (e.g. different number of participants, different emails, and the addition of a 'do not know' option in our case).

Moreover from the investigation of visual attention, language attention and technological awareness we revealed interesting findings. More specifically participants made a selection based on incorrect criteria in many cases (e.g. based on

logos, copyright symbols and footers in the emails, and in other cases influenced from the type of language that the emails used). Moreover, the fact that many participants mentioned technological aspects in the email in order to support their thesis shows a level of security awareness. However, in many cases the participants mentioned these aspects but their reasoning led them to draw the wrong conclusion about legitimacy.

6. Conclusion

The practical study was a good idea to investigate the phenomena of social engineering through phishing attacks with emails. The need for security awareness on the topic is imperative, but the way to achieve such awareness could be a difficult process due to the technical unfamiliarity or the behavioral traits of each user.

Future work could address a deeper analysis of how individual factors (such as visual, technological and language characteristics) have an effect, rather than having messages that include combinations of several of them. Another possible direction for future work would be the use of emails with real links instead of email snapshots, as this would enable more interactive exploration by the users (thus more accurately mirroring the real-life scenarios in which phishing messages would be encountered).

7. References

Allen, M. (2006), Social Engineering: A means to violate a computer system, SANS Institute, http://www.sans.org/reading_room/whitepapers/engineering/529.php, (accessed 10 August 2006)

BBC News. (2005), How to sell your self for a song, BBC News, http://news.bbc.co.uk/1/hi/technology/4378253.stm, (accessed 06 August 2006)

Cialdini, R. (2000), Influence: Science and practice, 3rd edn., New York: HarperCollins, ISBN: 0-3211-8895-0

Dhamija, R. Tygar, J. D. (2005), Phish and HIPs: Human Interactive Proofs to Detect Phishing Attacks, in Proceedings of the Second International Workshop on Human Interactive Proofs, H.S. Baird and D.P. Lopresti (Eds.): HIP 2005, Springer-Verlag Berlin Heidelberg, pp127–141.

Dhamija, R. Tygar, J. D. and Hearst, M. (2006), Why Phishing Works, to appear in the Proceedings of the Conference on Human Factors in Computing Systems (CHI2006), Montréal, Québec, Canada, pp: 1-10

Drake, C. Oliver, J. J. and Koontz, E. J. (2004), Anatomy of a phishing email, in Proceedings of the First Conference on Email and Anti-Spam (CEAS), 2004, http://www.ceas.cc/papers-2004/114.pdf, (accessed 12 August 2006)

Fette, I., Sadeh, N. and Cranor, L. (2006), Web Security Requirements: A Phishing Perspective, Carnegie Mellon University, http://www.w3.org/2005/Security/usability-ws/papers/13-cmu requirements/#search=%22Web%20Security%20Requirements%3A%20A%20Phishing%20Perspective%20Fette%22, (accessed 30 August 2006)

Forte, D. (2005), Spyware: more than a costly annoyance, Network Security, Vol. 2005, No. 12, pp8-10.

Harl. (1997), People Hacking the Psychology of Social Engineering, Text of Harl's Talk at Access All Areas III, http://www.noblit.com/docs/people-hacking.pdf, (accessed 10 August 2006)

Huseby, S. H. (2004), Innocent Code: A security wake-up call for web programmers, John Wiley & Sons. Ltd, Sussex, U.K., 0-470-85744-7.

Jordan, M. and Gouday, H. (2005), The Signs, and Semiotics of the Successful Semantic Attack, 14th Annual EICAR Conference 2005, St.Juliens/Valletta, Malta, ISBN: 87-987271-7-6, pp: 344-364.

Leyden, J. (2004), Brits are crap at password security, The register, http://www.theregister.co.uk/2004/04/20/password_surveys/, (accessed 06 August 2006)

Petty, R. E., and Caciopo, J. T. (1986), Communication and persuasion: Central and peripheral routes to attitude change, New York: Springer-Verlag.

Robila, S. and Ragucci, J. (2006), Do not be a Phish: Steps in User Education, ACM SIGCSE: Vol. 38, No. 3.

Silicon.com. (2006), What the security 'stitch-up' should teach as, Silicon.com, http://software.silicon.com/security/0,39024655,39156525,00.htm, (accessed 06 August 2006)

Stevens, G. (2002), Enhancing Defenses Against Social Engineering, SANS Institute, GIAC, http://www.sans.org/infosecFAQ/social/defense_social.htm, (accessed 10 August 2006)