4-12-2006

Assessing end-user awareness of social engineering and phishing

A Karakasiliotis,
University of Plymouth

S M. Furnell
University of Plymouth

M Papadaki
University of Plymouth

Recommended Citation

Karakasiliotis,, A., Furnell, S. M., & Papadaki, M. (2006). Assessing end-user awareness of social engineering and phishing. DOI: https://doi.org/10.4225/75/57a80e47aa0cb

DOI: 10.4225/75/57a80e47aa0cb
7th Australian Information Warfare and Security Conference, Edith Cowan University, Perth Western Australia, 4th - 5th December, 2006.

Assessing end-user 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: nrg@plymouth.ac.uk

Abstract

Social engineering is a significant problem involving technical and non-technical ploys in order to acquire information from unsuspecting users. This paper presents an assessment of user awareness of such methods in the form of email phishing attacks. Our experiment used a web-based survey, which presented a mix of 20 legitimate and illegitimate emails, and asked participants to classify them and explain the rationale for their decisions. This assessment shows that the 179 participants were 36% successful in identifying legitimate emails, versus 45% successful in spotting illegitimate ones. Additionally, in many cases, the participants who identified illegitimate emails correctly could not provide convincing reasons for their selections.

Keywords

Social engineering, phishing, security awareness.

INTRODUCTION

Social engineering is a significant threat to the security of systems and data. Harl (1997) defines the technique as "the art and science of getting people to comply with your wishes", and numerous cases can be identified in which related methods are used by attackers to assist in compromising a system or acquiring information. Social engineering methods may be targeted against both organisational employees and private individuals, and a notable aspect in which the problem has come to prominence in recent years is the threat of phishing. Indeed, findings from the Anti-Phishing Working Group suggest a growing threat, with 23,670 unique reports being received in July 2006, as compared to 14,135 a year earlier (APWG, 2006). These scams not only represent a problem to the unwitting recipients, but also an unwelcome threat to the reputations of the organisations and brands that are impersonated. Unfortunately, as the attacks themselves have become more sophisticated, it has become progressively more difficult for those targeted by phishing messages to distinguish them from genuine correspondence. This can be directly related to advances in the social engineering and deception methods used by the attackers.

This paper examines the extent to which end-users are susceptible to email-based social engineering and phishing threats. The discussion begins with a brief coverage of the psychological and technical ploys that may be utilised to help fool a potential target into trusting an email message. From this foundation, the remainder of the paper then presents details of a study conducted by the authors, in order to determine whether users can distinguish between legitimate emails and illegitimate messages that attempt to employ some of the aforementioned techniques. The results are presented and discussed, leading to conclusions about the consequent difficultly of guarding against such attacks.

BACKGROUND

Social engineering may involve both psychological and technological ploys in order to leverage the trust of the target. From the former perspective, the attacker can exploit characteristics of human behaviour in order to increase the chances of the user doing what is desired. For example, Cialdini (2000) mentions that there are six basic tendencies of human behaviour that may influence compliance with a request - namely authority, scarcity (e.g. claiming that something is in short supply or available for a limited period only), liking, reciprocation, commitment (consistency) and social proof (i.e. increasing the chances of a request being complied with by claiming that other people have already done the same thing). Similarly, within the field of information technology, Stevens (2000) refers to behavioural traits such as 'conformity' and the 'desire to be helpful', while Jordan and Goudey (2005) refer to factors of 'inexperience' and 'curiosity' that may be exploited.. 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 an email.

In the phishing context, psychological methods are often accompanied by further ploys achieved via technical means. A phishing attack can often contain two main steps, a phishing email and a bogus web site. Hyperlinks are typically included in the message text, with the URL redirecting the user to the bogus site in order to collect sensitive information such as login credentials and financial details, or alternatively to download a malicious file (Forte, 2005). Alternatively, an attacker may accompany a message with a malicious attachment in order to exploit a vulnerable user system, with the text in the message body then being used to encourage the user to open the attachment. This is a widely-utilised technique in the dissemination of malware such as worms and Trojan horses, with a classic example being the Love Bug worm from May 2000, which fooled users into opening a worm by pretending to be a love letter.

Visual deception in phishing attacks can be achieved through many ploys to make the email appear legitimate, such as masking a fraudulent URL (Huseby, 2004) and stealing HTML code from a genuine web site in order to create a bogus one by mirroring it (Drake et al. 2004). Images with banners and logos can also be used to create a more plausible appearance. Further techniques that may be used to gain the user's trust include spoofing the email address of the sender, and presenting URLs that contain 'https' in the message to suggest a secure link. Meanwhile, the bogus web site may contain plausible security indicators, such as the padlock icon to denote a secure session (Dhamija and Tygar, 2005), and misusing images of security seals (such as the VeriSign and TRUSTe logos).

The aim of the research was to assess users' susceptibility to social engineering by mounting a survey to investigate their knowledge of the associated ploys and techniques. In common with previous experiments in the field (Robila and Ragucci, 2006; Dhamija et al. 2006) our investigation focused on the email part of the phishing attack, and specifically on the criteria that participants used to identify such techniques.

INVESTIGATIVE METHODOLOGY

The experiment was designed based on an online survey and it included two main sections. The first section collected demographic details about respondents (e.g. gender, age, nationality, education and employment background) and their Internet usage (e.g. use of online services such as shopping and banking, and any mechanisms already used to guard against phishing threats). This was followed by the main body of the survey, which consisted of 20 questions, each presenting the participant with an email message, and asking them to judge its legitimacy. In each case, respondents could chose one of three options ('illegitimate', 'legitimate' and 'don't know', with the latter being set as the default), and could optionally complete a text box to explain their reasoning.

A range of email messages were used as the basis for the investigation, which represent a variety of both legitimate correspondence that typical Internet users may receive, and a number of common email ploys used by attackers. The 20 email questions were composed from 11 illegitimate and 9 legitimate messages, and were gathered from a combination of websites showing phishing-related examples, as well as emails that the authors had personally received. The nature of the messages is summarised in Table 1 (with illustrative examples of four of the actual messages being presented in Figures 1 to 4), which lists them in the order that they were presented in the survey. In each case, the apparent source is indicated, alongside an indication of whether or not the message was in fact genuine. The messages are then categorised according to various characteristics of their appearance, all of which recipients may potentially use to aid their decision about whether to trust the content or not:

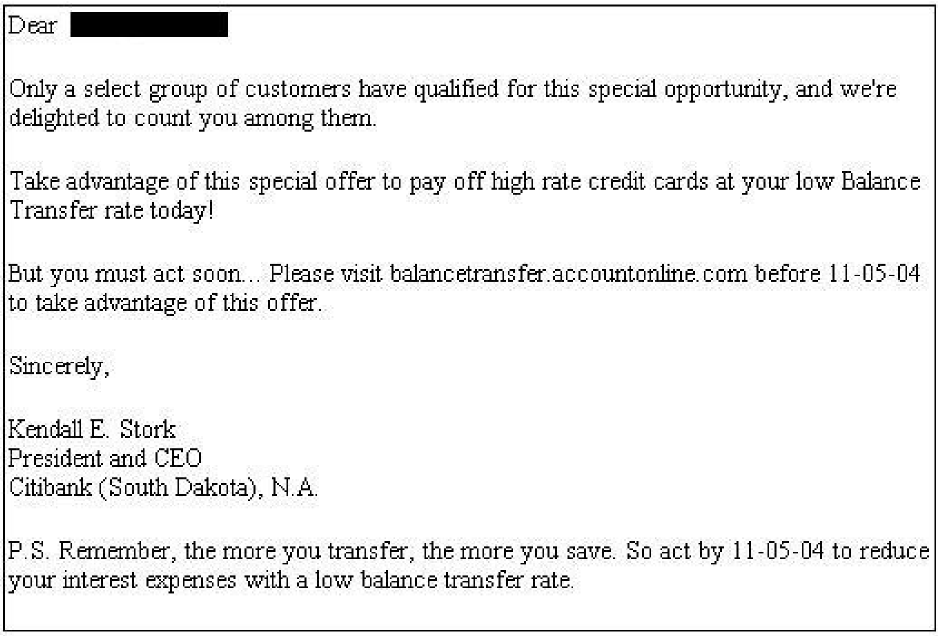
- **Identifiable recipient**: Did the message include something that addressed the recipient by name or some other characteristic (e.g. part of an account number) that could assist to verify whether or not the sender was in possession of valid details about them?

- **Identifiable sender**: Did the message body indicate the name of a specific individual that a recipient could attempt to contact (i.e. instead of a generic claim such as 'XYZ security team' etc).
- **Images / logos**: Did the message include graphical content that could help to improve the appearance, emphasize brand identity, etc?
- **Untidy layout**: Was the message presented in an unprofessional manner (e.g. line breaks in the middle of sentences)?
- **Typos / language errors**: Did the message contain any spelling mistakes or grammatical errors?
- **URL / link**: Did the message seek to encourage the recipient to follow a hyperlink?

The final column of the table indicates what the message was intending to convey – which, in the case of the illegitimate messages, indicates the means by which it was attempting to deceive and persuade the recipient. From an inspection of the table, it is clear that none of the appearance-related characteristics could be regarded as a definitive indicator of legitimacy. Although characteristics such as untidy layout and typographic/grammatical errors were only observed in illegitimate messages (and could therefore be used to raise a recipients suspicion), their absence certainly did not mean that a message was genuine.

Question number and claimed sender		Type of message	Appearance-related characteristics						Purpose of message
			Identifiable Recipient	Identifiable sender	Image / logo	Untidy layout	Typos/ lang. errors	URL/ link	
1	Bank of America	Legitimate	✓		✓				Notification of deposit.
2	NatWest Bank	Illegitimate						✓	Request for account verification
3	Citibank	Legitimate	✓	✓				✓	Opportunity to transfer credit card balances
4	Chase Credit Cards	Legitimate			✓			✓	Opportunity to transfer credit card balances.
5	Cross Country Bank	Legitimate						✓	Request to access online account in order to retain access.
6	Halifax Bank	Illegitimate			✓			✓	Request for account verification.
7	Lloyds TSB	Illegitimate			✓		✓	✓	Request for account verification.
8	CapitalOne	Legitimate	✓		✓			✓	Notification of account statement available for viewing.
9	Microsoft	Illegitimate			✓			✓	Instructs recipient to download a security patch.
10	Network Solutions	Legitimate			✓			✓	Annual confirmation request for domain name details.
11	eBay	Illegitimate	✓		✓			✓	Request for account verification.
12	eBay	Illegitimate			✓		✓	✓	Request to join eBay PowerSeller programme (sent to an unnamed recipient).
13	eBay	Legitimate	✓					✓	Request to join eBay PowerSeller programme (sent to a named recipient).
14	WorldPay	Illegitimate		✓		✓			Claim of chargeback made to recipient’s account. Accompanied by a malicious executable attachment.
15	PayPal	Legitimate	✓		✓			✓	Notification of payment.
16	PayPal	Legitimate	✓						Request (sent to named recipient) to update card details
17	PayPal	Illegitimate	✓		✓				Vishing scam
18	PayPal	Illegitimate			✓			✓	Request for tsunami disaster relief donation
19	Amazon	Illegitimate			✓			✓	Request for account verification.
20	British/Intercontinental Free Lottery	Illegitimate		✓		✓	✓		Request for personal information in order to claim prize money.

Table 1: Summary of the email messages used in the study



Dear [redacted]

Only a select group of customers have qualified for this special opportunity, and we're delighted to count you among them.

Take advantage of this special offer to pay off high rate credit cards at your low Balance Transfer rate today!

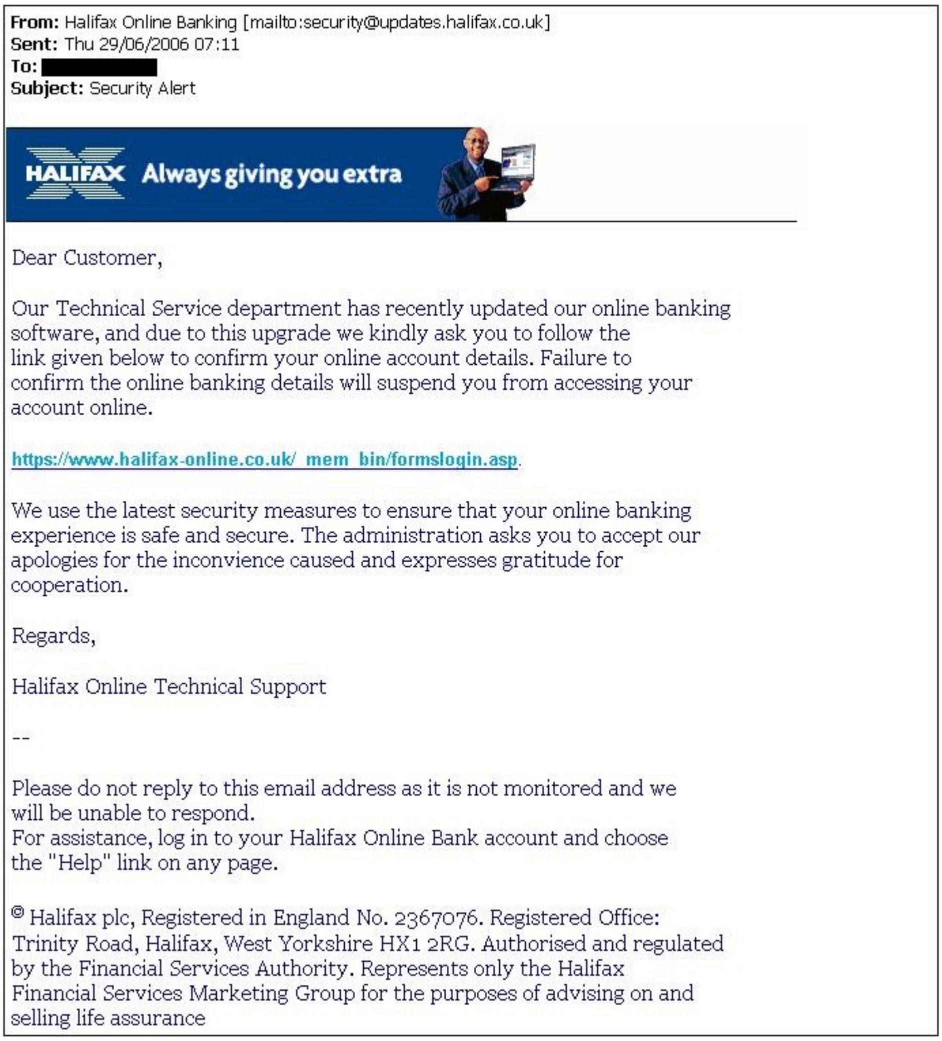
But you must act soon... Please visit balancetransfer.accountonline.com before 11-05-04 to take advantage of this offer.

Sincerely,

Kendall E. Stork
President and CEO
Citibank (South Dakota), N.A.

P.S. Remember, the more you transfer, the more you save. So act by 11-05-04 to reduce your interest expenses with a low balance transfer rate.

Figure 1: Message 3 (legitimate)



From: Halifax Online Banking [mailto:security@updates.halifax.co.uk]
Sent: Thu 29/06/2006 07:11
To: [redacted]
Subject: Security Alert

Dear Customer,

Our Technical Service department has recently updated our online banking software, and due to this upgrade we kindly ask you to follow the link given below to confirm your online account details. Failure to confirm the online banking details will suspend you from accessing your account online.

https://www.halifax-online.co.uk/_mem_bin/formslogin.asp.

We use the latest security measures to ensure that your online banking experience is safe and secure. The administration asks you to accept our apologies for the inconvience caused and expresses gratitude for cooperation.

Regards,

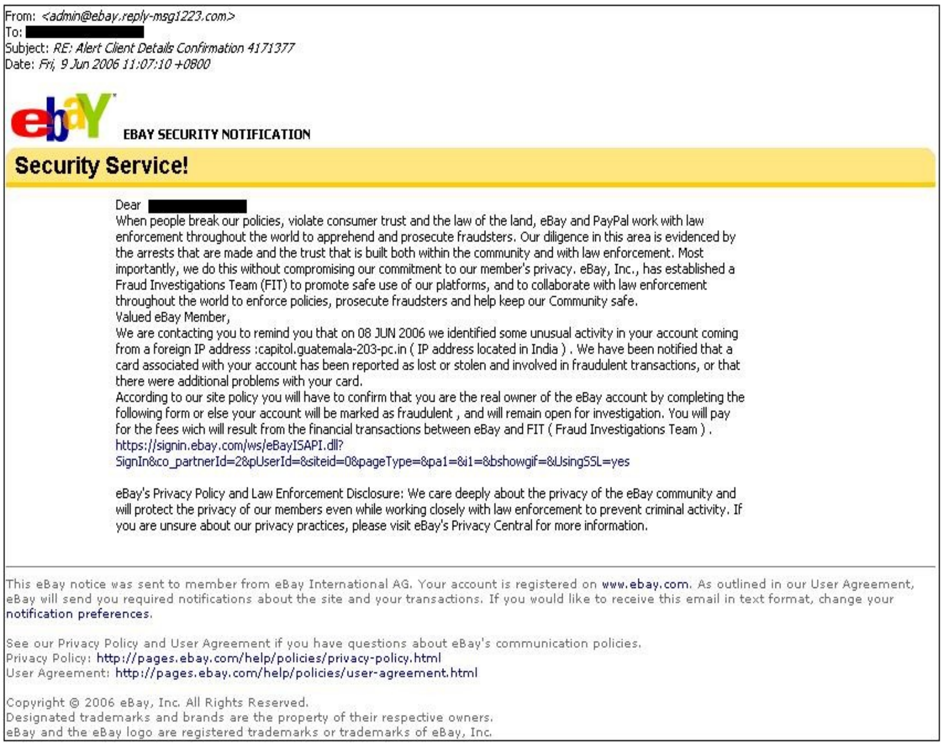
Halifax Online Technical Support

--

Please do not reply to this email address as it is not monitored and we will be unable to respond.
For assistance, log in to your Halifax Online Bank account and choose the "Help" link on any page.

© Halifax plc, Registered in England No. 2367076. Registered Office: Trinity Road, Halifax, West Yorkshire HX1 2RG. Authorised and regulated by the Financial Services Authority. Represents only the Halifax Financial Services Marketing Group for the purposes of advising on and selling life assurance

Figure 2: Message 6 (illegitimate)



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

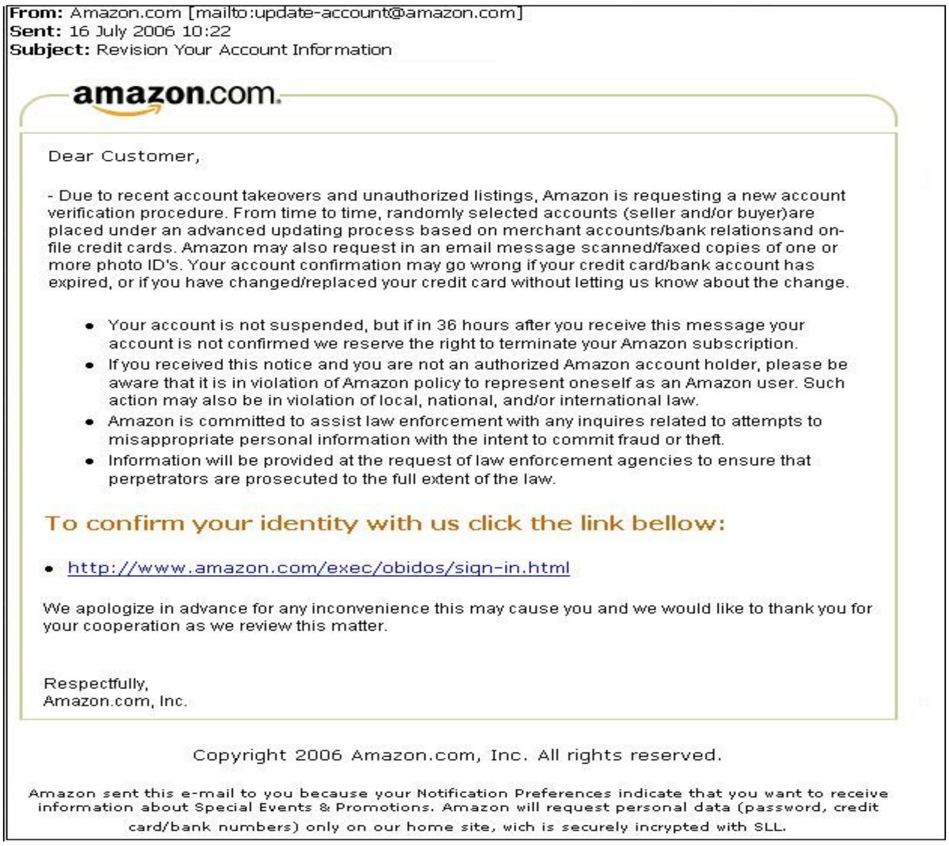
eBay's Privacy Policy and Law Enforcement Disclosure: We care deeply about the privacy of the eBay community and will protect the privacy of our members even while working closely with law enforcement to prevent criminal activity. If you are unsure about our privacy practices, please visit eBay's Privacy 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 3: Message 11(illegitimate)



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

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 4: Message 19 (illegitimate)

EXPERIMENTAL RESULTS AND ANALYSIS

A total of 179 participants completed the survey over 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. According to our findings the total population included 22 different nationalities and a mix of gender (75% male and 25% female). Also, the majority of participants (97%) were higher educated persons, with 76% in the 18-29 range, and the remainder being 30+ years old.

Overall findings

Figure 5 depicts the overall responses observed for each question. One immediate observation is that, in most cases, opinions were very much divided, with only a small number of cases in which respondents had a clear majority view one way or the other (e.g. questions 3, 14, and 20). Furthermore, in some cases the majority view was dramatically wrong (e.g. question 3). This clearly shows that many users typically face a hard task to differentiate between a genuine email and a bogus one based upon the message content alone.

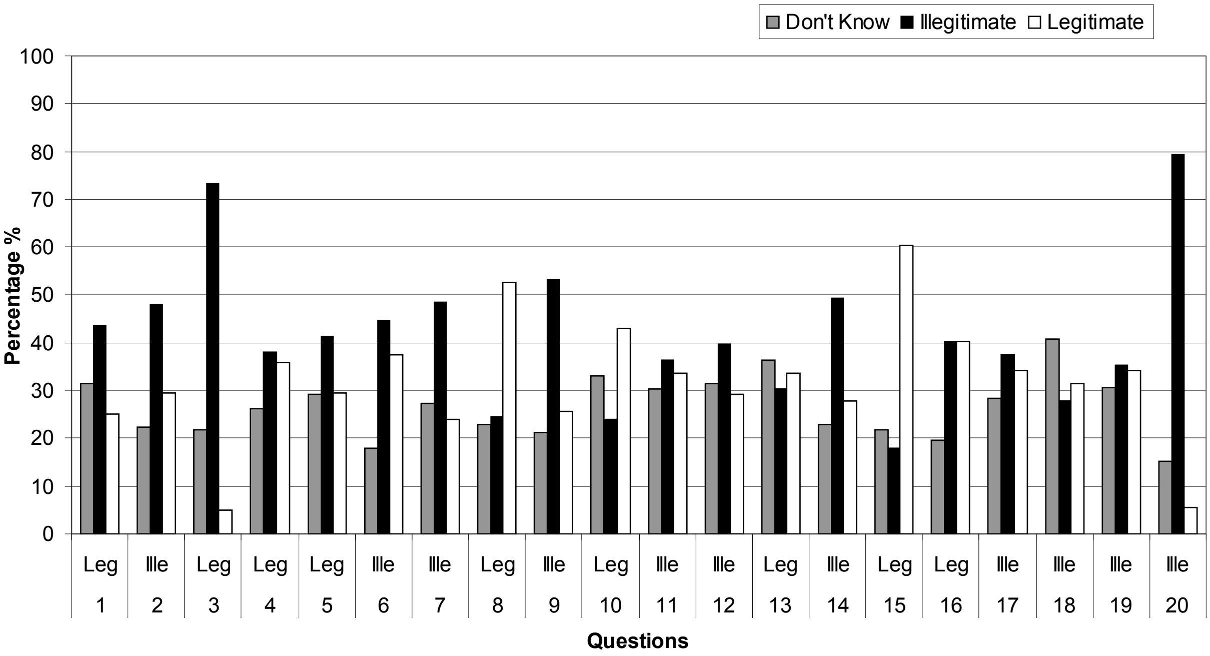


Figure 5: Overall opinions for each of the 20 messages

The overall level of correct classification (i.e. indicating 'legitimate' for genuine messages and 'illegitimate' for bogus ones) 42%, while misclassification was 32%. This, alongside the additional 26% of 'don't know' responses, clearly illustrates the level of confusion amongst the participants. Analyzing subsets of the participants based upon the demographics we established that there were no significant differences relating to gender, age, or nationality. The results did, however, reveal that the participants were more prone to misclassifying legitimate messages, potentially suggesting that the phishing threat (and possibly the survey exercise itself) causes a heightened level of suspicion.

	Correctly classified	Incorrectly classified	Don't Know
Legitimate messages	36	37	27
Illegitimate messages	45	28	26
Overall	42	32	26

Table 2: Classification of messages by participants

These findings can be compared to those from other experimental work. For example, Robila and Ragucci (2006) discovered that, on average, their 48 participants were able to correctly identify 60% of legitimate messages and 53% of illegitimate ones. However, it should be noted that this study used a different set of email questions, and did not include the option for participants to select a ‘don’t know’ option, as was possible in our case.

Rationale for judgments

According to the feedback comments (which were left by 89 participants) we were able to make a deeper analysis by examining the participants’ judgment criteria in each case. A total of 1,653 distinct comments were made, which were then grouped for analysis according to whether they related to the influence of visual factors, technical cues, and language characteristics within the messages.

In terms of visual factors, we observed that 40 of the participants made judgments based on indicators such as logos, banners, trademarks, footer, fonts and copyright symbols. From those participants, 55% used these characteristics as a basis for deciding that the message was legitimate. It was also noted that participants were more likely to regard a plain text (i.e. ASCII format) email as illegitimate (60%) than one in HTML formet that included colour (40%).

From the perspective of technical cues, 52 participants made a judgment based upon the URL shown in the message (with 70% selecting the ‘illegitimate’ option). Furthermore, 26 participants mentioned ‘http’ or ‘https’, and 39 made a comment to suggest that they could use the URL for verification purposes by typing it directly into a browser rather than clicking the link. Meanwhile, 40 participants made a selection based on the presence of an email address.

From the investigation of language and content-related characteristics, we understood that 19 participants focused on the language mistakes, such as typos and grammatical errors. Several observations were based upon the level of personal (i.e. recipient-specific) information in the messages. For example, 18 participants made reference to the presence (or absence) of the recipient’s name in the email, while 67 made comments based upon the presence of other personal information (e.g. the 4 last digits from account numbers). Many participants also focused upon the intention of the language used in the message. For example, 34 participants commented upon emails that purported to relate to an offer or opportunity for the recipient, while 26 participants were influenced by messages that used forceful language. Also from an analysis of influential techniques it seems that messages that involve asserting authority or exploiting the recipient’s desire to be helpful are most likely to be misclassified, compared to those attempting to exert influence based upon social proof or scarcity, which participants were more able to classify correctly.

Judgment Criteria		Illegitimate	Legitimate	Mixed
Visual	Coloured email			✓
	Plaintext email	✓		
	Logo/Trademark		✓	
	Footnote		✓	
	Copyright		✓	
Technical	There is https		✓	
	There is no https	✓		
	There is URL/Link	✓		
	There in no URL/Link			✓
	Verification process			✓
	Manually URL check	✓		
	Sender email address	✓		

Language and content	Personalized email (e.g. recipient name)	✓		
	Other personal data (e.g. 4 last digits)			✓
	Typos/grammar errors	✓		
	Promoting offers / opportunities	✓		
	Using forceful language			✓
	Attempting to trigger desire to be helpful			✓
	Asserting authority			✓
	Using social proof	✓		
	Indicating scarcity	✓		

Table 3: Influence of different factors in determining decisions about message legitimacy

It was also notable that although visual factors, technical cues and language characteristics were often being used as judgment criteria, participants were often arriving at incorrect decisions as a result. For instance, with the illegitimate email used in Q6 (see Figure 2), which contained logo, footer and copyright symbol elements, almost a quarter of the 39 participants who left comments used one or more of these factors to justify a choice of 'legitimate'. Similarly, although many participants commented upon the technical cues within the emails, much of their interpretation was wrong. As examples, we can consider the messages previously depicted in Figures 3 and 4. Figure 3 is an illegitimate email from eBay with spoofed email address (i.e. admin@ebay.reply-msg1223.com), while Figure 4 is an illegitimate email that includes a non-secure URL for login (http://www.amazon.com/exec/obidos/sign-in.html). However, several of the participants identified these factors as aspects that increased their confidence.

Based upon the overall findings that we observed from the comments, Table 3 summarises the typical influence of the various factors, indicating whether each was most commonly commented upon as a factor leading to a judgement of legitimacy or illegitimacy. In some cases (where there was less than a two thirds majority indicated in one way or the other) the influence of the factor was considered to be mixed, and thus it does not have a clear role in leading participants to a legitimacy decision.

CONCLUSION

The practical study has enabled a deeper investigation of the phenomena of social engineering through phishing attacks with emails, providing insight into the reasons that users become victims of such ploys. The resulting need for increased security awareness is clear, but the way to achieve such awareness could be a difficult process due to the technical unfamiliarity or the behavioural traits of each user.

It is recognized that our participants were only able to judge legitimacy on the basis for the content of the messages, and were not able to assist their decisions by considering the context in which an email was received. In practice, this aspect would very often aid a decision. For example, if a message asking for verification of account details was received from a bank with which the recipient was not a customer, then this would typically be a good indication that the message was bogus.

Another limitation in this study was that the candidate messages inter-mixed the different factors of interest (e.g. use of visual indicators, styles of language, and technical cues). A more specific study of the influences that each of these aspects may hold could be achieved if participants were specifically instructed to consider them in isolation (i.e. purely based on the appearance of the message, is it legitimate or illegitimate?). As such, this represents a potential aspect of future research. However, possibly the most important near-term priority for the industry in general is to ensure adequate awareness of, and action against, the phishing threat. This not only applies to end-users who may receive the messages, but also the organizations that may find their brand being hijacked.

REFERENCES

APWG. (2006), Phishing Activity Trends Report, Anti-Phishing Working Group, July 2006. http://www.antiphishing.org/reports/apwg_report_july_2006.pdf (accessed 26 September 2006).

Cialdini, R.B (2000), Influence: Science and practice, 3rd ed., New York: HarperCollins.

Dhamija, R. and 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, pp1-10

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, UK, 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, pp344-364.

Robila, S.A. and Ragucci, J.W. (2006), "Don't be a Phish: Steps in User Education", ACM SIGCSE: Vol. 38, No. 3.

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

COPYRIGHT