12-1-2006

Societal Aspects of Phishing

James W. Ragucci
Montclair State University

Stefan Robila
Montclair State University, robilas@mail.montclair.edu

Societal Aspects of Phishing

James W. Ragucci
Department of Computer Science
Montclair State University
Montclair, NJ
raguccij1@mail.montclair.edu

Stefan A. Robila
Department of Computer Science
Montclair State University
Montclair, NJ
robilas@mail.montclair.edu

Abstract

The damage caused by phishing does not only apply to monetary property alone. The fragile bonds of trust that organizations build with their constituents are shattered in the process. As people loss faith in the reliability of electronic communication methods, companies loss their customer base. In the case disasters, people can spend billions in preparation, to analyze weaknesses and improve recovery time, only to have thrust shattered by phishing attacks. This in turn causes a significant loss in money, resources and time.

In this study we review the main characteristics of phishing attacks and their impact to society. Based on current trends, we predict an increase in frequency and precision of these attacks and suggest best practices for both user and business education such that the impact is minimized.

1. Introduction

Phishing is defined as sending e-mails claiming to be from legitimate business and trying to entice the recipients into giving up confidential information. A successful phishing attack can have disastrous consequences for the victims leading to financial losses and identity theft. While relatively low in success rate until now, phishing attempts have recently increased in frequency as well as quality, requiring a fresh look at their impact, at detection methods and education efforts.

In this paper we address several new issues related to phishing. First, we investigate the concept of context-aware attacks where the phishing message is formed based on context information related to the victim (such as coming from businesses most likely associated to the victim). We discuss several approaches to acquiring such information and also see whether an increase in the success rate is resulting.

Second, we investigate the effect phishing has on legitimate businesses and the communication with their customers. Faced with over 150,000 unique attacks in 2005 alone [1], banking and other financial institutions have increasingly taken active steps in educating their customers on fraudulent activities. Unfortunately, in this process, two disturbing trends are noted. First, legitimate institutions themselves do not follow 'good communication' rules further increasing the general population confusion. Second, increased awareness of phishing leads to an increased false positive identification, where legitimate messages are discarded, thus hindering communication.

Our third research direction is the impact of phishing attacks when associated to disaster reaction and recovery. In these instances, given the highly emotional nature of the events as well as the new phishing issues discussed above, it is expected that the attack success rate will significantly increase. This in turn will result in decreased trust and support for legitimate agencies and also add to confusion.

Trust, support and reliable communication are essential factors in reducing the effect disasters have on the population. Our study indicates that phishing attacks could negatively affect these factors. As such, we suggest that organizations involved in reaction and recovery from disasters and emergencies consider including phishing education in the population awareness programs, at the same time, following 'good communication' rules in their interaction with the public.

2. Context-Aware Phishing Attacks[1]

Originally phishing attacks worked using the same principal that spam works on. Phishing is using social engineering and combining it with spam e-mails, sending the byproduct to unsuspecting victims, known as phish. The e-mails are disguised as, or "spoofed" to appear as they originated from legitimate corporations. The phishers goal is to "fish" for confidential information that

[1] Note, other sources, including [2] refer to Context-Aware attacks as "Spear-Phishing." In this paper, we will use the term "Context-Aware" attack, set forth by [3].

1-4244-0479-7/06/$20.00

the phishes have access too. This sensitive data can include bank account numbers, usernames and passwords, and social security numbers [4]. As many other technologies, both good and bad, phishing has and will evolve as time passes and phishing techniques are perfected.

With this in mind, we have seen studies that suggest that Context-Aware Phishing Attacks are the next phase in the refinement of phishing techniques [5] [6]. A context-aware attack consist of the phisher gaining knowledge of what sites and services the phish use and customizing an attack that appears to be from the target's service. [2] [3] Currently phishing attacks are carried out by sending tens of millions of e-mails out over the internet. 99% of the recipients might not even use the service targeted by the attack, but that one percent of the population that use the service have a high likelihood of taking the bait [4]. If that number of victims can be increased, while decreasing the total number of spammed accounts, then the chances of more people falling victim will increase. In short, decrease the total audience while increasing the total number of phish [3].

This creates a problem for vendors of antivirus, anti-spam and even firewall companies, because they gear their products to defend users from large-scale attacks. Meanwhile, smaller more focused attacks can slip through the cracks [7]. Using various techniques from browser recon to identity linking, phishers can target their victims in order to maximize their catch. For standard users and security experts, the problem comes when trying to defend from this kind of an attack. With a regular phishing attack many users, even those uneducated in phishing can identify the e-mail as fraudulent and delete it. A context-aware attack is harder to decipher than a regular attack, and can cause even more damage if a paranoid victim decides to delete legitimate e-mail [8].

2.1 Better Bait.

At first, one might wonder how a phisher can obtain personal information about potential phish. Two general ways that phishers can gather knowledge on their phish is by either data mining any of the social networks and databases available to the public, or retrieving the information from an end-user's own internet browser.

Social networks and public databases prove to be simple and efficient resources that are easily exploitable. There are a significant number of people who post private information in social networks. The social networks, listed in [5] provide phishers with desirable and reliable information about their targets. By using a script to mine information from anyone of these resources, one could easily construct a database of target's information [5].

Beyond the use of social networks, one's browser may also be a gold mine to phishers looking to create context-aware attacks. Web browsers including, Microsoft Internet Explorer (IE) and Mozilla Firefox, both store cache from website that the end-user has visited. This cache may contain, but is not limited to internet pages, media, form responses and login information [9]. As specified by both [9] and [3], the data from the browser can be easily collected from unsuspecting users that store their passwords and other login data using the autocomplete feature. The vulnerability of using the autocomplete feature of these web-browsers is illustrated in [10] with a script that attempts to grab sensitive information from the autocomplete feature. Of the respondents that executed the script created by [10], 2.7% of them were discovered to store their names within their web-browser. Approximately the same percentage of people had both their home and e-mail addresses retrieved by the script. The script also returned 0.7% of respondent's credit card numbers and passwords. These numbers might seem small, but on a large scale of a million users, the numbers approximate to 27,000 names and 7,000 credit card numbers that phishers can acquire. Phishers can also use the data stored in the end-user's browser history learn of the targets internet habits and develop a customized context-aware attack based on the acquired data on the phish [11].

2.2 Increased Catch

Two specific studies have been made analyzing the vulnerability of institutions [6] [5]. In the former study, the administrator at West Point created a phishing e-mail that he sent out to a select 512 cadets of the 4,200 student campus. This proof-of-concept experiment sent students a spoofed e-mail claiming to be from a nonexistent Colonel and asked them to confirm their grade reports online. The e-mail took advantage of the mentality at West Point where cadets must perform an order from a Colonel in spite of what their orders [6]. Over 80% of the cadets responded to the phishing e-mail. Of the results it is important to note that timing, as well as knowledge of the West Point mentality played a role in the success of the phishing e-mail. Timing was key in this experiment because of the subject of the phishing message. The message was sent at the end of the semester, when cadets would be most concerned about their grades. As seen in this experiment, they flooded the system, neglecting the obvious warnings, embedded in the e-mail, that the e-mail was fraudulent [6]. The paper also makes note that unbeknownst to the deployment team, the school sent seniors a legitimate e-mail three days before the deployment team sent out there e-mail. Therefore, there is

a high probability that the seniors associated the legitimate message with the fake one sent out later.

This trend was also noted in a phishing identification test conducted in [12]. As stated in that paper, the question on the administered test that received the least correct responses was one that claimed to be from the University Registrar. This question was incorrectly identified by 64% of the participants. At the time of the administration of the test, the University revealed that a large amount of their student data was inadvertently disclosed publicly, making the students more susceptible to identity theft. As with the aforementioned West Point experiment [6], the students in [12] associated the example presented to them, with what occurred on their campus, and believed it to be legitimate. Furthermore, this phishing identification test was administered a second time after the paper was published, and four months after the university sent out a legitimate version of the e-mail. The results were nearly identical, 67% of the students identified the message incorrectly.

The second aforementioned experiment, [5] took the concept of knowing something about the target in advance and used social networks commonly used to students at Indiana University to harvest information for their own personal phish database. This controlled context-aware phishing attack proved to be as successful as [6]. The study monitored both a random phishing attack from a source unbeknownst (the control case) to the test subject and a spoofed e-mail claiming to be from a source that the subject knows (context-aware attack). In the end, the control case had a success rate of 16% while the context-aware attack had a return rate of 72% [6]. An important conclusion to note about this experiment is that social and context-aware attacks appear to cause people to overlook vital clues that may otherwise alarm them that the e-mail they received is a phishing attack.

3. Effect on Legitimate Businesses

The most obvious harm caused to legitimate businesses and organizations is the monetary damage that phishing causes. In 2003 alone, it was estimated that phishing caused approximately $1.2 billion in direct financial loses to US Banks and credit card companies [15]. Indirect losses to businesses are much higher because they include customer service expenses, account replacement costs, and higher expenses from online services due to a decrease in use caused by lack of trust in data security [15]. This lack of trust towards online services provided by the organizations is understandable. After all, the standard phishing attack is delivered to victims through e-mail.

3.1. Promoting Bad Business Practice

A stereotypical phishing e-mail contains some sort of statement from the phisher, claiming to be a legitimate business asking the user to update or confirm their information in the system. Currently, millions, if not billions of e-mails use this guise. Therefore, a regular person would most likely consider an e-mail matching the description above to be a phishing attack. The problem arises when businesses do not follow good e-mail practices and actually request the information through an e-mail or provide links for the customers to click on. These e-mails may confuse customers and cause them to either delete a legitimate e-mail or get into a bad habit that will make users more likely to respond to a phishing attack. Many corporations and banks alike still have not changed their policies to be less confusing for their customers. At the time of publication of [16], American Express had developed a reputation for sending confusing e-mails to customers.

We have also personally received a similar e-mail in nature from a reputable bank was similar in nature and marked as having a 99% probability of being spam. In reality, after searching through the headers and examining the message, we determined that the e-mail was actually legitimate. In addition, during the process of authenticating the e-mail, we found a section on the bank's website that said they will not send customers any e-mails requesting personal information. This section of there website has since been removed.

In a different example, Expedia sent their customers' advertisements for special offers, but have the offers channel through a third party site that looks like a phishing attack. To make matters more interesting, the company sent the special offers through third party sites neglecting to check if the customer has disabled the send me special offer feature in their user preferences [17].

Bad business e-mail practices like the ones above risk companies losing customers. Figure 1 lists several important e-mail practices that businesses should follow to help reduce the confusion that phishing e-mails have created for their user-base. Although these

1. Do not request personal information directly through hyperlinks [13]
2. Refrain from "click here" hyperlinks [13]
3. Do not get customers in the habit of responding to e-mails in methods phishers use. [13]
4. When possible personalize e-mails [13] [14]
5. Keep URL's simple [13]
6. Make sure to use proper spelling and grammar in e-mails[13] [14]
7. Do not request delivery receipts [14]
8. Use meaningful subjects [14]
9. include e-mail disclaimers [14]
10. use bcc over cc when doing mailings [14]
11. Do not use third party sites or link redirection [9] [13]

Figure 1. List of recommended e-mail practices that businesses can follow to avoid looking like phishers.

recommendations may seem to be common sense advice, as seen above, many corporations and organizations do not follow these simple guidelines.

3.2. Training and False Identification

Educating users in dangers of phishing is a necessity that needs to be taken with caution. While a strong education of the dangers of phishing is important to computer user, [8] shows that as users receive more education, they become more likely to think that an e-mail is a phishing attack, instead of a legitimate message from a company that they do business with. Furthermore, confusing legitimate e-mails that are sent out by some companies, as listed in section 3.1, contribute to the added confusion that users face when reading their e-mail. Rather than risking irreparable financial damage, educated customers are more likely to delete these e-mails. This results in a decreased use of online services with the companies as discussed in [15]. Thus, electronic means of communication, for companies to consumers is hindered as more and more customers choose to ignore e-mail messages that were legitimately sent to people's inbox.

4. Impact on Disaster Reaction and Recovery

Disasters have the ability to bring out the best and worst in people. One only has to think back to the recent events of both the 2004 Tsunami and Hurricane Katrina. Each disaster caused an unimaginable amount of damage as well as large number of civilian causalities. These tragedies brought about a large amount of philanthropic donations from the public to help the victims. Unfortunately, with the generous flow of money towards charity, both phishers and scam artists alike have decided to divert some of the funds into their own pockets.

In the events of the Tsunami, one phisher was arrested with a database containing over 800,000 e-mail address that he had been phishing with e-mails disguised as if they were from Paypal(www.paypal.com) [19]. Figure 2 exemplifies a phishing e-mail sent out to take advantage of the misfortunes of the Tsunami victims.

In the case of Hurricane Katrina, images of the chaos seen in New Orleans as people looted the stores will forever be ingrained in the minds of this generation. Still, the cyber crimes that took place after the hurricane dissipated are far more damaging. Authorities shut down several phishing sites in the aftermath of Katrina that involved phishing scams. These websites contain legitimate sounding names, including katrinadonations.com, katrinarelief.com and katrinahelp.com [20] [21]. These sites in particular were

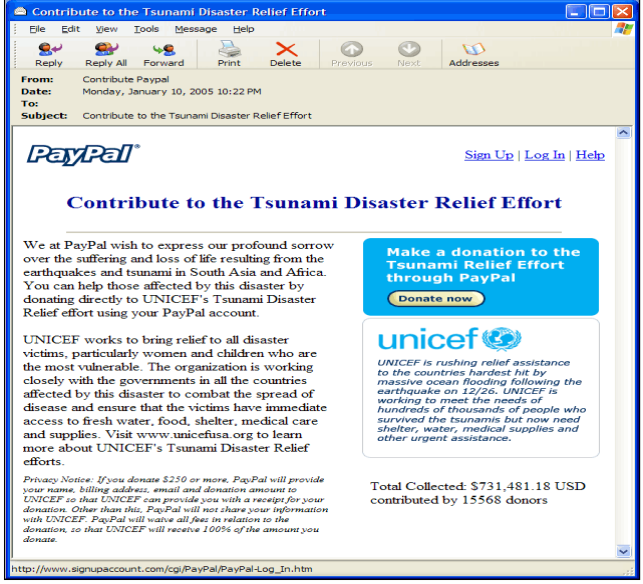

Figure 2. A Tsunami Phishing e-mail masked as it has been sent from Paypal [18]

registered to a P.O Box owned by a "Demon Moon." All of them appear to be construed to steal the passwords of sympathetic people who were trying to help out victims through the use of legitimate sites.

In any disaster, a fast response is crucial. With, this in mind public support is needed for a speedy recovery from damage. Phishers that use disasters to their advantage are basically creating a context aware attack. In the situation with disasters, phishers know that people are more likely to donate money to charity, and overlook obvious warning signs that the attack might display. Although the attack is not as fine-tuned as a context-aware attack described in section 2, phishing attacks masked as charity requests will continue to improve in quality as time moves on.

Similar to the effects in section 3, phishing can and will destroy the trust the public has in using the internet in disasters. Phishing, which has already received a large amount of media, due to the financial damage it causes, has already discouraged internet banking. It can significantly cut the relief aid that people were willing to give the victims through legitimate websites that belong to organizations like the Red Cross [21].

5. Conclusion

Trust, support and reliable communication are essential factors in curving the damaging effects from disasters. Phishing scams destroy all three of these elements. By receiving a phishing e-mail that claims to be a legitimate organization, such as the Red Cross, people question the authenticity of the message. As described in section 3, if people cannot validate the e-mail they received, because of bad e-mail practices by the charity organization, then they will most likely delete the e-mail due to lack of trust. By deleting the e-mail support for the

disaster is lost, because fewer donations are received as aid. Thus, unless a reliable means of communication is established elsewhere the recovery from disaster will become more drawn out than it should have been.

Charities, as well as businesses, need to practice good e-mail habits when dealing with public trust. By establishing good etiquette with e-mails as discussed in section 3.1, organizations can build trust. To reinforce this trust, organizations need to also keep in mind the problems that phishing presents to disaster recovery. By ignoring the problem trust can and will be destroyed, in addition to a much more prolonged recovery time. As phishing attacks continue to evolve with time, recovery plans that factor phishing need to be updated as well in order to not only stay ahead of the phishers, but also to preserve trust.

6. References

[1] Anti-Phishing Working Group, *Phishing Activity Trends December 2005 Report,* http://www.antiphishing.org/reports/apwg_report_DEC2005_FINAL.pdf, accessed 11 May 2006.

[2] Microsoft "What is spear phishing?," 2006, http://www.microsoft.com/athome/security/email/spear_phishing.mspx. accessed 20 Apr. 2006.

[3] M. Jakobsson "Modeling and Preventing Phishing Attacks," Phishing Panel in Financial Cryptography '05.

[4] J. Duntemann, *Degunking Your Email, Spam, And Viruses*, 2004.

[5] T. Jagatic, N. Johnson, M. Jakobsson and F. Mencezer "Social Phishing," 2005.

[6] A.J. Ferguson "Fostering E-mail Security Awareness: The West Point Carronade," *EDUCAUSE QUARTERLY*. pp. 54-57, 2005.

[7] J. Vijayan "Targeted Attacks Pose New Security Challenge," *Computerworld* pp. 1-16, 2005.

[8] A. Brandt "Phishing Anxiety May Make You Miss Messages," *PCWORLD* pp. 34 2005.

[9] C. Benniger "Finding Gold in Your Cache," 2006.

[10] F. Menczer "A Riddle," 2004. http://homer.informatics.indiana.edu/cgi-bin/riddle/riddle.cgi. accessed 29 Apr 2006.

[11] M. Jakobsson, T. Jagatic and S. Stamm "Phishing for clues: Inferring Context Using Cascading Style Sheets and Browser History," 2006, https://www.indiana.edu/~phishing/browser-recon/ accessed 18 Apr 2006.

[12] S.A. Robila and J.W. Ragucci "Don't be a Phish: Steps in User Education," *ITiCSE'06* 2006.

[13] K. Putnam "How Not to Look Like a Phish," TRUSTe 2005.

[14] "Email etiquette," 2004, http://www.emailreplies.com/ accessed 28 April 2006.

[15] A. Emigh "Online Identity Theft: Phishing Technology, Chokepoints and Countermeasures," pp. 1-58, 2005.

[16] L. James *Phishing Exposed: Uncover Secrets from the Dark Side,* Syngress Publishing, Rockland, MA, 2005.

[17] P.G. Neumann "Risks to the Public," *ACM SIGSOFT Software Engineering Notes* vol. 31, pp. 6-16, 2006.

[18] ""Paypal Tsunami" example," *MailFrontier*. 2004, http://www.mailfrontier.com/quiztest2/S2img/Q22_tsunami.gif accessed 3 Nov. 2005.

[19] J. McCarthy "Phishing scams and worms plague tsunami aid effort," *Infoworld Tech Watch* 2005, http://weblog.infoworld.com/techwatch/archives/000993.html accessed 29 Apr 2006.

[20] B. Krebs "Katrina Phishing Scams Begin," *Security Fix* 2005, http://blogs.washingtonpost.com/securityfix/2005/08/katrina_phishin.html accessed 09 Apr 2006.

[21] P.F. Roberts "Cyber-Looters capitalize on Katrina," *EWEEK* pp. 11-12, 2005.