Interscience Management Review

Volume 4 | Issue 1 Article 5

January 2011

Phishing: A Serious Threat to Online Banking

Subasish Mohanty
GMFC (Goa University), subasish.147@gmail.com

Biswajit Rout
Fakir Mohan University, mail4bishwa@gmail.com

Recommended Citation

Mohanty, Subasish and Rout, Biswajit (2011) "Phishing: A Serious Threat to Online Banking," *Interscience Management Review*: Vol. 4 : Iss. 1 , Article 5.
DOI: 10.47893/IMR.2011.1075
Available at: https://www.interscience.in/imr/vol4/iss1/5

Phishing: A Serious Threat to Online Banking

Subasish Mohanty[1] & Biswajit Rout[2]

[1]Asst. Professor & Head, Dept. of Business Administration, GMFC (Goa University)
Email: subasish.147@gmail.com
[2]Doctoral Research Scholar, Dept. of Business Management, Fakir Mohan University,
Email : mail4bishwa@gmail.com

Phishing:

Phishing is an attempt to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money) by masquerading as a trustworthy entity in an electronic communication. Communications purporting to be from popular social web sites, auction sites, banks, online payment processors or IT administrators are commonly used to lure unsuspecting public. Phishing emails may contain links to websites that are infected with malware. Phishing is typically carried out by email spoofing or instant messaging, and it often directs users to enter details at a fake website whose look and feel are almost identical to the legitimate one. Phishing is an example of social engineering techniques used to deceive users, and exploits the poor usability of current web security technologies. Attempts to deal with the growing number of reported phishing incidents include legislation, user training, public awareness, and technical security measures. Many websites have now created secondary tools for applications, like maps for games, but they should be clearly marked as to who wrote them, and you should not use the same passwords anywhere on the internet.

The concept of phishing has actually been around for years. The term "phishing" was first used by hackers to describe stealing America Online® (AOL) accounts by acquiring usernames and passwords. Phishing is a continual threat that keeps growing to this day. The risk grows even larger in social media such as Facebook, Twitter, Myspace etc. Hackers commonly use these sites to attack persons using these media sites in their workplace, homes, or public in order to take personal and security information that can affect the user and the company (if in a workplace environment). Phishing is used to portray trust in the user since the user may not be able to tell that the site being visited or program being used is not real, and when this occurs is when the hacker has the chance to access the personal information such as passwords, usernames, security codes, and credit card numbers among other things.

For example: You receive an e-mail from your credit card company informing you that your account has been deactivated because of suspicious activity. The message requests you to click a web link and log in to verify your account information. Following the instructions, you are directed to what appears to be the "Online Update" page of your credit card company. Here you are asked to enter your name, password, account number, social security number, and PIN. It all seems legitimate: the logos look proper, the web address of the page looks convincing, and the format of the site is the same as you remember. However, this is a scam; the e-mail is a fraud, and now a cyber-criminal has your personal information. He or she can now use or change your account or open new accounts in your name. You have become a victim of a growing crime called phishing.

The Anti-Phishing Working Group (APWG), states that the term phishing "comes from the analogy that Internet scammers are using e-mail lures to 'fish' for passwords and financial data from the sea of Internet users". Apparently, the "ph" was used as a tribute to the term "phone phreaking", a technique used in the early days of hacking to take advantage of security weaknesses in the phone systems. Phishing is defined as the use of "spoofed" (hoax) e-mails and fraudulent web sites for the purpose of fooling users into revealing personal data. Although e-mail is the primary channel for phishing attacks, some scams are using instant messaging (IM), fake news bulletins, and social communities such as MySpace™ to fool users into divulging personal information.

Treats from phishing:

One of the primary threats from phishing is identity theft. Consumers go to great lengths to protect their personal information, but a single breach of security can expose a person to a multitude of threats, including credit card fraud, damaged credit, having an identity used for criminal activity, stolen bank information, unauthorized use of accounts (online and otherwise), or stolen money. There are also intangible threats, such as damage to credibility, loss of trust, or embarrassment; having personal information stolen can cost a great deal more than lost cash. Terrorists are known to use phishing and other identity theft scams to gain employment, obtain fake identification as cover for attacks, and to finance their activities.

A threat that many experts have grown more concerned about is the level of trust consumers have in e-mail, online commerce, and the companies they deal with online. Many institutions have stopped communicating with customer's via e-mail altogether to help eliminate the possibility that the user may become a victim of phishing. This seems to point to a disturbing consequence of the increase in all forms of online fraud, not just phishing: if consumers become wary of using e-mail and the Internet, online commerce may begin to suffer, according to many experts.

ATTACK OF PHISHING:

Traditional Attack: Phishers play the odds when sending their mass-mailings. Of the thousands of messages sent, only a small percentage of the recipients may actually be a customer of the spoofed company. Still this can result in quite hefty profits for the scammers.

There have been many different variations of phishing scams, but the e-mail messages are usually structured to prey, ironically, on the computer user's fear of being a victim of fraud or hacking, or may be a message stating that the company needs to update their records. If the victim follows the link, their browser is directed to an address that might look very similar to the one they would expect. This is another ploy used by phishers: registering domain names with similar looking addresses or using character replacement (using the number "1" for the lowercase letter "L" for example) to disguise the fake address. Many people can be fooled since they may not notice the difference. The URL can also be displayed within the e-mail as the actual legitimate address, but another web address—the phony phisher address—has been embedded using deceptive techniques.

Spear Phishing:

Computer users have become more educated about the threats from online fraud and phishing, avoiding some of the more common schemes, so criminals have begun to change their tactics. An attack dubbed "spear phishing" has become more prevalent. Spear phishing, according to The APWG (Anti-Phishing Working Group), is a targeted attack on a certain individual, group, or organization. The phisher sends an email disguised to look like it came from within an organization, for example from the Human Resources department or the local area network (LAN) manager. Users are much more likely to open an email (and its attachments) if it appears it came from within. The message will often have an attachment, disguised, for example, as a Microsoft ® PowerPoint presentation, and entices the user to open the file. However, the file is in reality crimeware (software created expressly to steal financial information) created to infect the computer with a Trojan horse and open a backdoor into the system. Now the crooks have a route into the internal corporate network.

Vishing:

Traditional web-based phishing attacks are now evolving into sophisticated phone scams. Voice over Internet Protocol (VoIP) is becoming a popular alternative to traditional phone lines. Phishers use these VoIP numbers, available through retailers such as Skype, to setup a war dialer (software to sequentially dial phone numbers) to call numbers within a specific region. When a person answers, they are "alerted" to some type of fraudulent activity on their credit card account or that their bank account has been compromised. They are directed to call a phone number to confirm personal data. The phone number is in fact attached to the VoIP account of the scammer.

Botnets:

Botnets have become a major security issue in the last few years. Botnets—networks of compromised machines infected with malicious programs—have been identified as a leading cause of phishing. Some botnets can contain hundreds or even thousands of machines—

colloquially called "zombies". These networks are used to send spam, primarily, though they can be used for other criminal purposes.

Pharming :

Though not a phishing attack per se, pharming is used by the same criminals to redirect web users from legitimate commercial web sites to malicious sites, which can then be used to elicit information for identity theft. Pharming crimeware misdirects users to fraudulent sites or proxy servers, typically through DNS hijacking or poisoning. This technique is not new; however, the proliferation of online banking and commerce makes it attractive to phishers.

The "Phishing Kit"

According to an article on the Dark Reading Room web site, "this is an all-in- one package that provides the raw materials to launch sophisticated phishing exploits that appear to be operating on legitimate web sites. The kit lets buyers create man-in-the-middle attacks, in which the victims communicate with a legitimate web site via a fraudulent URL set up by the fraudster. This allows them to capture victims' personal information in real-time." A user must still be duped into clicking a URL, but they are interacting with the legitimate site (e.g., their bank's web site), yet using the fake URL, allowing the attacker to intercept any personal information entered by the user…in real-time! The kit also allows the attacker to impersonate multiple sites, without configuring or buying another kit.

Instant Messaging and Social Networks:

Phishers also use instant messaging (IM) technology and social communities such as MySpace™ for phishing scams. In the IM attack, users receive an IM message that often appears to be coming from a buddy-list contact [34]. The victim is lured into clicking a URL and, as in other phishing scams, is directed to a fraudulent web site. Fake MySpace login pages are also created to capture user's email and passwords, allowing the account to be compromised and used to spam other accounts. In addition, IM and social networks are often mediums for crimeware or malware.

REMEDIES OR RECOMMENDATIONS:

Many experts contend that phishing is less of a "technology problem" and more of a "user problem"; that the responsibility ultimately lies with the user being aware of where they are browsing, what information they are giving over the Internet, and to whom they are giving the information. Others are more concerned that the sophisticated techniques used by phishers are becoming more difficult to detect, even for experienced computer users; casual or less- technical users are much less likely to be able to discern a legitimate e-mail, web address, or web site from a fake one. Social engineering ploys can be very effective in these situations**.**

Education:

Education is a vital component of the phishing battle—as well as other online scams. The Federal Trade Commission suggests some things to remember:

- Don't reply to e-mails asking to confirm account information. Call or logon to the company's web site to confirm that the e-mail is legitimate.
- Don't e-mail personal information. When submitting information via a web site, make sure the security lock is displayed in the browser.
- Review credit card and bank account statements for suspicious activity
- Report suspicious activity.

The Department of Justice recommends that users Stop, Look, and Call:

- Stop: Don't react to phisher ploys of "upsetting" or "exciting" information
- Look: Look closely at the claims in the e-mail. Also look at the links and web addresses
- Call: Call or e-mail the company in question to verify if the e-mail is legitimate.

Computer users should make an effort to keep abreast of computer security issues in the news, and use common sense when giving information anywhere: online or otherwise. If an e- mail (or phone solicitor or web site, etc., etc.) asks for personal information, that should be an immediate red flag that something may not be legitimate and needs to be confirmed. Legitimate companies will generally not solicit personal information via e-mail. If personal information is requested via a web site, the user should make certain he

or she is connected to the proper site and that the communications are encrypted.

Technology:

Unfortunately, phishing usually involves social engineering tricks, and, thus, even the best defences that a company might have in place to combat outside threats are sometimes useless against these types of attacks. Although education is likely the best defence against phishing scams, there are technologies that make phishing harder to accomplish. When implemented with a defence-in-depth approach, software and hardware can be installed to slow the phishers down.

- Two-factor Authentication
- Firewalls
- Anti-virus Technology
- Browser Enhancements
- Digital Certificates
- Secure E-mail Protocols
- Communication with the customers
- Phish Feeding
- Defence-in-Depth

Litigation:

Framing and implementing various anti-phishing laws to provide varying levels of punishment for criminals who are caught committing phishing fraud is the need of the hour. The problem is, according to many security professionals, catching the crooks is difficult. It is very easy for them to hide their tracks, and many of the phishing sites are only operational for a few days or weeks before they are changed or moved.

Companies Need to be Prepared:

Regardless of education or technology put in place, companies need to be prepared for the impacts of phishing and other online fraud attacks. Costs related to reissuing credit cards, re- establishing accounts, reimbursing customers for losses, and possible litigation, are just a sampling of expenses a company may have to absorb. These costs could be quite significant, particularly if hundreds of accounts are compromised. Many experts suggest that companies need to have a disaster recovery plan in place to cover phishing attacks, similar to plans that cover any type of digital security breach or a natural disaster.

CONCLUSION:

Phishing scams can pose a significant threat to consumers and the companies they deal with. The number of online scams has increased significantly, and the techniques the criminals employ have become more and more sophisticated. These and other online cons show little sign of slowing. On the contrary, scams are on the rise, and companies and individuals need to be aware of the consequences.

No single technology can keep fraudsters at bay and keep our personal information completely safe. Thereare ways to make the crimes more difficult to accomplish, but a well-crafted phishing attack has a significant chance of being successful. There will have to be more done to stop the spread of these attacks and make them unprofitable and less appealing for the would-be phishers.

More research and development of anti-fraud technologies, more education of computer users, and aggressive prosecutions of the criminals who commit these crimes will go a long way to curb the threat, but these alone will most likely have little impact in the number of schemes.

Consumers need to become more educated concerning online threats and vulnerabilities. Companies need to make sure that online fraud and scams are reported and that their customers are kept apprised of scams that may affect them. The security community needs to work to find new ways to make e-mail and online commerce as bullet-proof as it can possibly be. If something is not done, the way we do business online will change, and almost certainly not for the better.

References:

1. The Anti-Phishing Working Group. “What is Phishing?” URL:http://www.antiphishing.org/ (March 2004).
2. The Anti-Phishing Working Group. “Origins of the Word Phishing.” URL: http://www.antiphishing.org/word_phish.htm (March 2004).
3. Wikipedia definition. “Phishing”. http:// en.wikipedia.org/wiki/phishing.
4. MadhusudhananChandrasekaran, Krishnan Narayanan, ShambhuUpadhyaya (March 2006). "Phishing E-mail Detection Based on Structural Properties". *NYS Cyber Security Symposium.*
5. Ghosh, Ayush (2013). "Seclayer: A plugin to prevent phishing attacks". *IUP Journal of Information Technology*, 9(4), 52–64

◈◈◈