Cybercrime and Business: How to *not* *Get Caught by the Online Phisherman*

Nick Nykodym, Ph.D**., Lisa Kahle-Piasecki,** M.B.A**.,** M.Ed.,[1] **Sonny Ariss,**
Ph.D. **and Tracey A Toussaint,** M.B.A.

Abstract. Throughout the history of modern business, management has dealt with the problem of theft. Businesses have a difficult time keeping money and information out of the wrong hands, due to external robberies and internal theft of both money and confidential information (Nykodym & Ariss, 2006). Apart from the ease of being able to reach customers anywhere in the world, the electronic media has created a new wave of worries for companies, since theft of information is becoming easier for criminals and harder to detect for businesses. Cyber crime, called "phishing," can be characterized by attackers using trusted Internet sites to lure information from unsuspecting consumers. It is now becoming a widespread problem for the business world. Phishing attacks are one of the major elements of cyber crime and companies have begun the arduous battle against phishers to keep their customers safe and their businesses afloat.

1 Introduction

Phishing is a scam to steal valuable information by sending out fake emails, or spam, written to appear as if they have been sent by banks or other reputable organizations with the intent of luring the recipient into revealing sensitive information such as usernames, passwords, social security numbers, account IDs, ATM PIN's or credit card details. Phishing can also come in the form of a pop-up message. Typically, phishing attacks will direct the recipient to a web page designed to mimic a target organization's own visual identity and to harvest the user's personal information, often leaving the victim unaware of the attack. Obtaining this type of personal data is attractive because it allows an attacker to impersonate their victims and make fraudulent financial transactions. Victims often suffer significant financial losses or have their entire identity stolen, usually for criminal purposes (Watson, Holz, & Mueller, 2005).

Phishing e-mails can be sent to people on selected lists or on any list, expecting that some percentage of recipients will actually have an account with the real organization (TechWeb, n.d., para. 1). Once the cybercriminals have gathered personal data, they have to decide how to use it. If the information comes from a business or financial institution, cybercriminals will research the best customers to attack. The best customers will have large assets, a good credit score, or other identifiers that make them a profitable victim. Cybercriminals will also research the types of transactions that get more scrutiny or will set off alarms and avoid those types of transactions (National Consumers League, 2006).

Phishing attacks use both social engineering and technical subterfuge to steal consumers' personal identity data and financial account credentials. Attacks using social engineering rely on using social skills through human interaction, to obtain information about a company or individual in order to gain access to sensitive information or personal data (United States Computer Emergency Readiness Team [US-CERT], 2009).

Social-engineering schemes use 'spoofed' e-mails to lead consumers to counterfeit websites designed to trick recipients into divulging financial data such as credit card numbers, account usernames, passwords and social security numbers. Hijacking brand names of banks, e-retailers and credit card companies, phishers often convince recipients to respond. Technical subterfuge schemes plant crimeware onto personal computers (PCs)

[1] Contact Author: Lisa Kahle-Piasecki, The University of Toledo, 2801 W. Bancroft Street, Toledo, Ohio 43606. E-mail: lisa.kahle@rockets.utoledo.edu

to steal credentials directly, often using Trojan keylogger spyware. Pharming crimeware, the latest version of online ID theft, misdirects users to fraudulent sites or proxy servers, typically through Domain Name System (DNS) hijacking or poisoning (e-Media Services, 2007).

2. History

The word *phishing* originated around 1996. The term was created with the analogy that cybercriminals used email as a fishing hook to "phish" usernames, passwords and other sensitive information from the "sea" of Internet users. The use of the letters "ph" is believed to come from the word "phreaking", which is a form of hacking telephone lines (Cybercrime, n.d., para. 2).

One of the early major phishing scams surfaced around 1996, when criminals stole American Online (AOL) accounts by phishing the passwords from AOL users (Cybercrime, n.d., para. 2). The attackers typically used either instant messages or email to trick users into divulging their AOL passwords. Victims would provide the attackers with this information, which the attackers would, in-turn, leverage to assume ownership of the victim's AOL account. Although this may not necessarily have been the first ever instance of phishing, it is the first well-known one and people first became aware of the dangers of the phishing hook.

Soon such hacked accounts were called "phish." By 1997, phish was traded and shared between cyber crooks as a form of currency. Often, these criminals used phish to obtain a particular hacking tool or a favor from fellow hackers.

Before 2003, most phishers employed emails as their main medium of fraud. They used text-based emails to trick their recipients into divulging their personal information to the phishers. These emails contained many spelling and grammatical mistakes, that tipped some cautious users off (Cybercrime, n.d, para. 5). Since then, the technique of phishing has evolved and expanded. While the original phishers usually obtained their data by sending fake emails, today various other techniques are used such as fake phish websites, Trojan horses and pharming. In this type of security breach, a virus is secretly planted in a user's computer to hijack the Web browser. The computer user then types in the address of a Web site and is taken to a fake copy of the Web site without realizing it. Once the user is at the phony site, usernames, passwords, social security numbers, account IDs, ATM PIN's or credit card details typed at the site are stolen and used (National Consumers League, 2006.)

3. How do you detect Phishing?

An entire phishing and hacker subculture has arisen, with phishing kits available online that include samples of messages, and instructions for building links (National Consumers League, 2006). A report by Symantec (2009) describes phishing toolkits as a method to professionalize fraud attacks with 25% of phishing attacks being generated using the toolkits. Rick Loomis (2009), director of information systems for the US Oklahoma Bar Association reports that Cybercriminals are also sharing information on the holes that exist in systems and how to attack different systems.

4. How to tell if an e-mail message is fraudulent

Microsoft Corporation (2009) encourages online safety in a guide that suggests a few phrases to look for if you think an e-mail message is a phishing scam.

"Verify your account."

Businesses should not ask you to send passwords, login names, Social Security numbers, or other personal information through e-mail.

"If you don't respond within 48 hours, your account will be closed."

These messages convey a sense of urgency so that you will respond immediately without thinking. Phishing e-mail might even claim that your response is required because your account might have been compromised.

"Dear Valued Customer."

Phishing e-mail messages are usually sent out in bulk and often do not contain your first or last name.

"Click the link below to gain access to your account."

HTML-formatted messages can contain links or forms that you can fill out just as you would fill out a form on a Web site.

The links that you are urged to click may contain all or part of a real company's name and are usually masked, meaning that the link you see does not take you to that address but somewhere different, usually a phony Web site

Con artists also use Uniform Resource Locators (URLs) that resemble the name of a well-known company but are slightly altered by adding, omitting, or transposing letters (Microsoft, 2009).

5. Rates of Phishing attacks

The monthly *Phishing Activity Trends Report* ("Anti-Phishing Working Group", 2009) analyzes phishing attacks reported to the Anti-Phishing Working Group (APWG) via its member company, Global Research Partners. The APWG phishing attack repository is the Internet's most comprehensive archive of email fraud and phishing activity. The APWG additionally measures the evolution, proliferation and propagation of crimeware drawing from the independent research of the member companies. The APWG also notes that more government agencies, such as US and UK tax authorities, are being phished along with more social networking websites. Latest attacks include phisherman going after log-ons to web mail and social networking accounts such as Facebook, Twitter and LinkedIn. The attacks have increased 200 % from May through September 2009 (Acohido, 2009). Access to social networking sites is increasingly banned in the workplace because of the threat not only to worker productivity but because of the potential for these sites to introduce malicious software from phishers into the corporate networks (Krebs, 2009). Recent warnings have been issued to Facebook users (Computer Fraud & Security, 2009) that several Facebook applications are designed to lure users to phishing sites. These attacks use social engineering to entice users to install applications and then using the Facebook user's friend's lists, the friends receive a false notification to encourage them to also install the application. Additionally, by installing these applications, Facebook users run the risk of possible identity theft if the applications are gaining access to the user's data (Computer Fraud & Security, 2009).

6. Statistical Highlights for the first half of 2009 from Symantec (2009)

- Unique phishing reports submitted to APWG recorded a high of 37,165 in May, around 7 per cent higher than last year's high of 34,758 in October.
- The number of unique phishing websites detected in June rose to 49,084, the highest recorded since April 2007's record of 55,643.
- Payment Services became phishing's most targeted sector, displacing Financial Services.
- Banking trojan/password-stealing crimeware infections detected increased during more than 186 percent between Q4, 2008 and Q2, 2009.
- The total number of infected computers rose more than 66 percent between Q4 2008 and the end of the half, 2009 to 11,937,944, representing more than 54 percent of the total sample of scanned computers.
- Sweden moved ahead of the United States as the nation hosting the most phish websites at the half's end.
- China hosted the most websites harbouring Trojans and Downloaders from March through June. ("Anti-Phishing Working Group", 2009)

7. Cost of phishing

When cybercriminals gain possession of a users Web mail user name and password, the results can be quite lucrative for the criminals. Using a victim's information, the criminals scan email folders for clues to online banks and social networks and then crack into those accounts. The phishers also sell this information to the cyber underground meeting a demand that leads to more attacks (Acohido, 2009).

According to the Javelin Strategy & Research 2008 Identity Fraud Survey Report, identity fraud and theft totalled $51 billion in the U.S. in 2008, after peaking at $58 billion in 2006. Internationally, one spam organization alone reportedly generated $40 million in a single year. "Stolen credit card data can sell for pretty cheap, like $5 to $10," says Derek Manky, security researcher at Fortinet, "but more targeted, sensitive data can bring in massive amounts. A coveted online gaming account can sell for up to $1,000." (Fong, 2008).

Research company Gartner Group reports that more than five million U.S. consumers lost money to phishing attacks in the 12 months ending in September 2008, a 39.8% increase from a year earlier (King, 2009) with 80% of the online adult population receiving e-mail that appeared to be part of a phishing attack. The cost of phishing not only stems from the actual monetary loss to consumers and business but the extra money being spent to develop ways in which to counteract phishing and this cost is passed on to consumers who purchase the products and services to protect themselves.

Another report detailing results of a survey of consumers conducted in 2006 (International Telecommunications Union, 2008), states US computer users paid over $7.5 billion over two years to repair and replace hardware that was damaged by viruses and spyware.

In a survey commissioned by the Messaging Anti-Abuse Working Group [MAAWG] (2009), 82 % of consumers are aware of malware threats but only 20 % believe their computers can become infected. When the computers need to be repaired, age is an important factor in determining how the computer is repaired. Users under 24 years old are more likely to take their computer to a repair service; users between 24 and 44 years old are more likely to repair their computers themselves. Users 45 and older look to a repair professional to fix their computers and users over 65 are more likely than other age groups to ask a professional to repair their computers (MAAWG, 2009).

Some companies however may not report losses to cyber crime of any type since they may fear a loss of confidence from consumers and investors, which could result in further losses such as major stock price declines or decreased sales for the company. In other cases, managers may not be aware that security breaches may have taken place until after the reporting of cyber crime findings.

8. Effects of phishing

Currently phishing has been creating havoc in the world of cyber space. Stealing credit card and other personal information from unsuspecting consumers, becoming a nuisance for those large companies with millions of customers who conduct all of their business online, and creating decline in online transactions because of increasing fear are just some of the negative impacts from phishing.

A recent phishing scam in Europe targeted businesses greenhouse gas emissions allowances (Spiegel, 2010). Under the European Union’s (EU) Emission Trading System, companies that are large emitters of greenhouse gases must have enough of an allowance or credit to cover the CO2 they release each year. The credits are issued by national authorities and the businesses are allowed to trade their credits to other businesses that need them. Cybercriminals sent e-mails to firms in Europe that appeared to come from the German Emissions Trading Authority and asked them to re-register on the agency’s Web site to avoid the threat of a hacker attack. Those firms that fell victim to the scam, mainly in Denmark and Britain, then purchased emissions allowances from the cybercriminals unaware that the emissions were illegally acquired (Spiegel, 2010).

Consumers have become more vigilant in their operations of online transactions and even though there may be an immediate pressure for companies to come up with ways to combat this cyber crime, in the long run this problem will definitely turn itself into a profitable enterprise for anti-phishing pioneers.

9. Fight against Phishing

European Efforts

Perhaps one of the most organized coordinated efforts to fight phishing and other related cybercrimes is through the Council of Europe. The Council of Europe is based in France and includes 47 member countries whose purpose is to develop common and democratic principles throughout Europe (Council of Europe, 2010). Specifically, this group formed the Council of Europe Convention on Cybercrime which is the only binding international treaty on the subject to have been adopted to date (Council of Europe, 2010). It establishes guidelines and a framework for all governments wishing to develop legislation against cybercrime and encourages international cooperation for cyber related crimes, including phishing. The Council of Europe considers phishing to be one of the major cybercrime threats that exists today (Council of Europe, 2009).

United States Efforts

The Federal Bureau of Investigation (FBI) feels that they are in a strong position and suitably equipped to deal with the problem of cyber crime. The FBI has the investigation skills, knowledge of forensics and international relations to make them excellent candidates for fighting cyber crime (Nykodym & Ariss, 2006). Likewise, legislation at the state, national, and international level will aid in the efforts against cyber crime (Nykodym & Taylor, 2004).

The FBI recently indicted over 50 people on charges of conducting financial fraud based on phishing (Stone, 2009). Operation Phish Phry caught the largest number of defendants charged in a cybercrime case. Defendants are reported to have stolen at least $2 million from victims with accounts at Bank of America and Wells Fargo over a period of the last several years. Customers of the banks clicked on e-mail messages that sent them to fake Web sites made to look like the actual banking site. Once there, victims typed in sensitive data such as usernames, passwords, social security numbers, account IDs, and ATM PIN’s. The cybercriminals used this information to transfer funds into their own accounts.

Global Efforts

Global law enforcement officials are recognizing the need to cooperate with each other in order to curtail cybercriminals in cross-border schemes. In two phishing-related crimes that were tied to organized crime worldwide, U.S. and Romania charged 38 people in both of the countries of defrauding thousands of individual victims and hundreds of financial institutions (Regan, 2008). In those crimes, U.S. Deputy Attorney General Mark R. Filip, stated that international organized crime was a serious threat to all nations and cooperation internationally must happen to disrupt and dismantle the cybercriminals enterprises (Regan, 2008).

Phishing Filter

Microsoft has a phishing filter for Internet Explorer to help protect users against phishing attacks. The phishing filter uses three methods to help protect users from phishing scams. First, it compares the addresses of websites visited against a list of sites reported to Microsoft as legitimate. This list is stored on a user’s computer. Second, it helps analyze the sites visited to see if they have the characteristics common to a phishing site. Third, with a user’s consent, the filter sends some website addresses to Microsoft to be further checked against a frequently updated list of reported phishing sites (Microsoft, 2009).

Training

Organizations should also make phishing awareness a necessary part of employee training and development. A service offered by Intrepidus offers companies help to test how susceptible their employees are to phishing attacks by sending workers fake phishing e-mails and recording how many employees fall for the fake phishing scam (Krebs, 2009). Of an approximately 100,000 employees in companies serviced by Intrepidus, 61% clicked links in mock phishing attacks that appeared to be from the popular social media sites LinkedIn, Facebook, and Twitter (Krebs, 2009). A game called Anti-Phishing Phil, created by researchers from Carnegie Mellon University (Sheng et. al., 2007), aims at teaching people how to detect phishing scams and protects themselves with the information they have gathered. The game can be used by businesses to train their employees and customers about phishing attacks and how to avoid them.

Improved communication has been shown to be a vital tool to combat cyber crime (Nykodym & Taylor, 2007). Likewise, phishing victims have shown cyber addiction tendencies so the dynamics of computer addiction and phishing should be explored (Nykodym, Ariss, & Kurtz, 2008). Strong training has been shown to decrease cyber crime (Nykodym, Taylor, & Vilela, 2005). One way to accomplish this is to make training in cyber crime a component of a formal organizational mentoring program. When an organization pairs an experienced employee or mentor with an inexperienced employee or mentee, the behaviors of the mentor are likely to be adopted by the mentee when that behavior is met with positive results in the organization (Kahle-Piasecki, 2010). Training programs can also help employees identify those situations where they feel apprehensive about whether or not they should comply with requests for sensitive information (Wright, Chakraborty, Basoglu, & Marett, 2009). Managers can be guided to understand, detect, and thwart computer crime (Nykodym, Kahle-Piasecki, & Marsilliac, 2010). Organizations that support efforts to combat cyber crime through employee training could notice a substantial decrease in this type of crime.

Reporting

Several outlets are available if you believe you have been a victim of phishing or received a phishing email. Phishing emails should be forwarded to the company, bank or organization impersonated in the email and in the US can be sent to spam@uce.gov and reportphishing@antiphishing.org .

10. Conclusion

On a global scale, cyber crime has skyrocketed with the advancement of the electronic medium. While progress is being made in combating cyber crime, particularly with the Council of Europe's Convention on Cybercrime, a large gap continues to exist in legislative compatibility across international borders (Nykodym & Ariss, 2006).

Countries need to become more educated with regard to Internet crime. Different laws in various countries and the enforcement of these laws influence the rate and nature of crime. Businesses in every sector also need to be acquainted with the technical details of cyber crime, as well as its relation to each individual employee (Nykodym & Ariss, 2006). Companies should consider a good mentoring program to train employees (Kahle-Piasecki, in press) and managers (Nykodym, Kahle-Piasecki, & Marsilliac, 2010) which will decrease the effects of phishing.

Cyber crime such as phishing, is no longer somebody else's problem, it is everyone's problem.

References

1. Acohido, B. (2009, October 27). Change passwords: Crooks want keys to your e-mail. *USA Today*. Retrieved from http://www.usatoday.com/tech/news/2009-10-27-cybercrime-phishing-account-passwords_N.htm
2. Anti-Phishing Working Group. *Phishing activity trends report 1st half 2009*. Retrieved from http://www.antiphishing.org/reports/apwg_report_h1_2009.pdf
3. Computer Fraud & Security. (2009, September). Hacking attacks target social networking.
4. Council of Europe. (2010). Who we are. Retrieved from http://www.coe.int/aboutCoe/index.asp?page=quisommesnous&l=en
5. Council of Europe. (2009, August). Fact Sheet. The Council of Europe and cybercrime. Retrieved from https://wcd.coe.int/ViewDoc.jsp?id=1496737
6. Cybercrime: Piercing the Darkness. (n.d.). *Origins of Phishing*. Retrieved from http://library.thinkquest.org/04oct/00460/phishingHistory.html
7. e-Media Services. (2007, January). Gone phishing: Internet identity theft. *Informant, 1*(2). Retrieved from http://www.e-mediaservices.com/Informant2005.pdf
8. Fong, C. (2008, May 9). Fighting the agents of organized cybercrime. *CNN*. Retrieved from http://www.cnn.com/2008/TECH/05/08/digitalbiz.cybercrime/index.html
9. International Telecommunications Union. (2008, July). *ITU study on the financial aspects of network security: Malware and Spam.* Retrieved from http://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-study-financial-aspects-of-malware-and-spam.pdf
10. Kahle-Piasecki, L. (in press). Making a mentoring relationship work: what is required for organizational success *Journal of Applied Business and Economics, 12(1).*
11. King, R. (2009, April 14). Phishing attacks surge amid recession. *BusinessWeek*. Retrieved from http://www.businessweek.com/print/technology/content/apr2009/tc20090413_894347.htm
12. Krebs, B. (2009, November 4). Spike in social media malware, phishing attacks. *The Washington Post*. Retrieved from http://voices.washingtonpost.com/securityfix/2009/11/spike_in_social_media_malware.html?wprss=securityfix
13. Loomis, R. (2009). It's 4:00 a.m. do you know if your computer system is safe? *Bar Leader, 34*(1), 12-13.
14. Messaging Anti-Abuse Working Group. (2009). A look at conusumers' awareness of e-mail security and practices or " Of course I never reply to spam- except sometimes." Retrieved from http://www.maawg.org/about/publishedDocuments/2009_MAAWG-Consumer_Survey-Part1.pdf
15. Microsoft Corporation. (2009). How to recognize phishing e-mails or links. *Microsoft Online Safety*. Retrieved from http://www.microsoft.com/protect/fraud/phishing/symptoms.aspx
16. Microsoft Corporation. (2009). Phishing filter: Frequently asked questions. Retrieved from http://windows.microsoft.com/en-US/windows-vista/Phishing-Filter-frequently-asked-questions
17. National Consumers League. (2006, March). A call for action: Report from the National Consumers League anti-phishing retreat. Retrieved from http://www.nclnet.org/news/2006/Final%20NCL%20Phishing%20Report.pdf
18. Nykodym, N., Ariss, S., & Kurtz, K. (2008). Computer addiction and cyber crime. *Journal of Leadership, Accountability and Ethics, 35,* 55-59.
19. Nykodym, N., & Ariss, S. (2006). Fighting cybercrime. *Journal of General Management*, 31, 63-70.
20. Nykodym, N., Kahle-Piasecki, L., & Marsillac, E. (2010, May). The managers guide to understanding, detecting and thwarting computer crime: An international performance issue**.** *Performance Improvement Journal*, *49*(5), 42-47.doi: 10.1002/pfi.20151
21. Nykodym, N., & Taylor, R. (2007). Communication: A vital tool to combat cyber crime. *CLSR Computer Law and Security Report, 2,* 185-189.
22. Nykodym, N., & Taylor, R. & Vilela, J. (2005). Criminal profiling and insider cyber crime. *CLSR Computer Law and Security Report, 21,* 408-414.
23. Nykodym, N., & Taylor, R. (2004). World's current legislation efforts against cyber crime. *CLSR Computer Law and Security Report, 20,* 390-395.
24. Regan, K. (2008, May 19). DOJ busts up global phishing ring, Charges 38. *E-Commerce Times.*

25. Sheng, S., Magnien, B., Kumugaru, P., Acquisti, A., Cranor, F., Hong, J., Nunge, E. (2007). Anti-phishing phil: The design and evaluation of a game that teaches people not to fall for phish. Retrieved from http://cups.cs.cmu.edu/soups/2007/proceedings/p88_sheng.pdf
26. Spiegel. (2010, February 3). Phishing scam cripples European emissions trading. *Spiegel Online*. Retrieved from http://www.spiegel.de/international/europe/0,1518,675725,00.html
27. Stone, B. (2009, October 8). F.B.I. indicts dozens in online bank fraud. *The New York Times*, p. B3.
28. Symantec. (2009, December). State of phishing: A monthly report, *26*, 1. Retrieved from http://eval.symantec.com/mktginfo/enterprise/other_resources/b-state_of_phishing_report_12-2009.en-us.pdf
29. TechWeb (n.d.). *TechEncyclopedia. Phishing*. Retrieved from
30. http://www.techweb.com/encyclopedia/defineterm.jhtml?term=phishing
31. U.S. Department of Homeland Security, U. S. Computer Emergency Readiness Team. (2009). *National cyber alert system: Cyber security tip ST04-014.* Retrieved from http://www.us-cert.gov/cas/tips/ST04-014.html
32. Watson, D., Holz, T., & Mueller, S. (2005, May 16). Know your enemy: Phishing. *The Honeynet Project*. Retrieved from http://www.honeynet.org/papers/phishing
33. Wright, R., Chakraborty, S., Basoglu, A., & Marett, K. (2009). Where did they go right? Understanding the deception in phishing communications. *Springer Science + Business Media B.V.*doi:10.1007/s10726-009-9167-9