Chapter 3: Threat and Magnitude of Problems

3.1 Introduction

According to the Anti-Phishing Working Group in Second Quarter (Q2) of 2008, the total number of unique phishing reports submitted was 28,151 in June 2008, an increase of from the previous month, 23,762. Q2 2008 saw a record high in reported hijacked brands to 294 in May 2008. The number of unique phishing websites detected by APWG was 18,509 in June 2008, a decrease of over 1,808 from the month of May. Financial Services continue to be the most targeted industry sector at 52% of all attacks in the Q2 2008, APWG is also seeing more phishing against some of the larger Internet retailers and the online job websites. The targeting of online job sites is likely linked to the massive identity theft cases that have involved these sites in recent months[30]. The United States and the United Kingdom tax authorities continued to be spoofed in phishing attacks against consumers. While in UK losses from phishing almost doubled to 23.2 million pounds in 2005, from 12.2 million pounds in 2004.[31] The BBC News on 13 December 2006 reported that the UK has seen an 8,000 percent increase in fake internet banking scams in the past two years[32].

A Report on phishing to the Minister of Public Safety and Emergency Preparedness Canada and the Attorney General of the United States, Binational Working Group on Cross-Border Mass Marketing Fraud October 2006,[33] phishing has **four distinct types** of impact, both domestically and internationally, that are of concern to the commercial and financial sectors and to law enforcement in both countries:

[30] See the APWG, "Second Quarter 2008 Phishing Trends Report", available at http://www.antiphishing.org/reports/ apwg_report_Q2_2008. pdf

[31] http://www.identitytheft.org.uk/

[32] BBC News, "Online Banking Fraud" up 8,000%

[33] See USA and Canada Report on Phishing, A Report to the Minister of Public Safety and Emergency Preparedness Canada and the Attorney General of the United States, Oct 2006

Direct Financial Loss. Depending on the type of fraud that a criminal commits with the aid of stolen identifying data, consumers and businesses may lose anywhere from a few hundred dollars to tens of thousands of dollars. Indeed, small e-commerce businesses may be particularly hard-hit by identity fraud. For example, because of credit card association policies, an online merchant who accepts a credit card number that later proves to have been acquired by identity theft may be liable for the full amount of the fraudulent transactions involving that card number.

Erosion of Public Trust in the Internet. Phishing also undermines the public's trust in the Internet. By making consumers uncertain about the integrity of commercial and financial websites, and even the Internet's addressing system, phishing can make them less likely to use the Internet for business transactions. People who cannot trust where they are on the World Wide Web are less likely to use it for legitimate commerce and communications.

This perspective finds support in a 2005 *Consumer Reports* survey, which showed declining confidence in the security of the Internet. Among several findings, the survey found that 9 out of 10 American adult Internet users have made changes to their Internet habits because of the threat of identity theft, and of those, 30 percent say that they reduced their overall usage. Furthermore, 25 percent say they have stopped shopping online, while 29 percent of those that still shop online say they have decreased the frequency of their purchases.

Difficulties in Law Enforcement Investigations.

Unlike certain other types of identity theft that law enforcement agencies can successfully investigate in a single geographic area (e.g., theft of wallets, purses, or mail), phishing – like other types of crime that exploit the Internet can be conducted from any location where phishers can obtain Internet access. This can include situations in which a phisher in one country takes control of a computer in another country, then uses that computer to host his phishing website or send his phishing e-mails to residents of still other countries. Moreover, online criminal activity in recent years has often reflected clear cut divisions of labor. For example, in an online fraud scheme, the tasks of writing code, locating hosts for phishing sites, spamming, and other components of a full-scale phishing operation may be divided among people in various locations. This means that in some phishing investigations, timely cooperation between law enforcement agencies in multiple countries may be necessary for tracing, identification, and apprehension of the criminals behind the scheme.

Incentives for Cross-Border Operations by Criminal Organizations. Law enforcement authorities in Canada and the United States are concerned that each of the preceding factors also creates incentives for members of full-fledged criminal organizations in various countries to conduct phishing schemes on a systematic basis. Law enforcement already has indications that criminal groups in Europe are hiring or contracting with hackers to produce phishing e-mails and websites and develop malicious code for use in phishing attacks.

The APWG reports that the leading geographic location for phishers is the United States, with 32 percent of the world's phishing sites.[34] As much as 81 percent of all phishing attempts made by January 2005 were targeted at customers of large financial institutions,

[34] Other top countries are China, 13 percent; Korea, 10 percent; Japan, 3.1 percent; Germany, 2.7 percent; Brazil, 2.7 percent; Romania, 2.2 percent; Canada, 2.1 percent; France, 2.7 percent; and Australia, 2.1 percent

although phishers prey on others as well.[35] Recent trends reveal that phishers are also targeting smaller financial institutions, such as community banks and credit unions. The smaller financial institutions tend to be more vulnerable to attacks because they have fewer resources to employ large security teams or implement effective security systems.

The financial loss to consumers and institutions can be tremendous. Gartner, Inc., a Stamford, Connecticut-based research and advisory firm, conducted a survey on phishing and identity theft in May 2005. The study revealed that 1.2 million Americans lost a total of $929 million in the previous year because of phishing.[36] And in his study "Phishing: A Growing Threat to Financial Institutions and E-Commerce," Frederick W. Stakelbeck, Jr., of Philadelphia's Federal Reserve Bank determined that a typical phishing attack can cost a financial institution between $50 and $60 per account compromised, or $50,000 per attack.[37] Those figures do not even cover the cost of time spent disabling the phishing sites, resetting legitimate user passwords, and installing software patches. In advising consumers, advocates should be careful that their warnings do not cause anyone to overreact and give up online transactions. Exaggerated perceptions of threats can undermine customer convenience, as well as being damaging to financial organizations. A Forrester Research study reveals, for example, that 26 percent of consumers have elected not to apply for a financial product online; 20 percent decided not to open e-mail from their financial providers; and 19 percent would not enroll in online banking or bill payment.[38]

Other than what had been mentioned above, Frederick W. Stakelbeck, Jr., in his article *"Phishing: A growing threat to financial institution and e-commerce*" stated the list of financial institutions victimized by phishing attacks in 2003 and 2004 reads like a "Who's

[35] See NW3C: National White Collar Crime Center, http://www.nw3c.org/.

[36] Gregg Keizer, "Phishing costs nearly $1 billion," *TechWeb News*, June 24, 2005.

[37] Frederick W. Stakelbeck, Jr., "Phishing: A growing threat to financial institutions and e-commerce," *SRC Insights*, fall 2004.

[38] Paul Gibler, "Phishing, pharming, spimming, and spoofing," *Credit Union Executive Newsletter*, April 18, 2005, p. 7.

Who," including Bank of America, Bank One, Citizens Bank, U.S. Bank, SunTrust, MBNA, Wells Fargo, and Visa, to name a few. And, the financial services sector continues to be the most targeted industry sector for phishing attacks. A May 2004 survey by Deloitte & Touche noted that attacks on information systems at some of the world's largest financial institutions have more than doubled in the past year; with 83 percent of those institutions surveyed saying their systems had been compromised, up from 39 percent in 2003.[39] In a recent report, software manufacturer Symantec estimated that U.S. banks and credit card issuers have lost almost $1.2 billion as a result of phishing attacks over the past year.[40]

Citibank, with its diverse product line, wide geographical reach, and emphasis on e-banking, reported 682 unique phishing attacks in the month of July 2004 alone, 34.5 percent of the total number of phishing attacks reported by the APWG that month. It's not only financial institutions that are coming under attack from online cyber crooks. AT&T, AOL, eBay, PayPal, Microsoft, Yahoo, the FDIC, the FBI, and the IRS have all been the victims of recent phishing assaults. No one, large or small, is immune. The U.S. military has also become a favorite target for phishers. In an August 26, 2004 press release, the United States Marine Corps' Judge Advocate Division advised all U.S. Marines stationed throughout the world to be cognizant of phishing attacks, further showing the magnitude of the phishing epidemic. The United States continues to host the greatest number of phishing web sites, with 35 percent of identified phishing sites located within U.S. borders. Other countries with a significant number of phishing sites include South Korea (16.0 percent), China (15.0 percent), Russia (7.0 percent), the United Kingdom (5.5 percent), Mexico (4.5 percent), and Taiwan (2.5 percent).[41]

[39] Thomas Vartanian, "Money Laundering Dominates Bank Enforcement Actions," *The American Banker*, September 24, 2004
[40] eMarketer, *Scary Stats: Internet Attacks Worldwide*, September 22, 2004, <www.emarketer.com/Article.aspx?1003053 >.
[41] Anti-Phishing Working Group, *Phishing Activity Trends Report,* July 2004.

3.2 Costs of Phishing

Today's phishers and hackers are no longer phishing and hacking for the resulting thrill, but for unadulterated financial gain. The resulting cost to victimized financial institutions and consumers, in both time and money, has the potential to be enormous. Cost estimates for identity theft for businesses, consumers and government organizations could reach $2 trillion by the end of 2005, according to market researcher Aberdeen Group. A typical phishing attack can cost a financial institution between $50 and $60 per account compromised, or $50,000 per attack. Furthermore, after a typical phishing attack, it takes approximately 160 hours for IT staff to disable a phishing site (once it has been identified), reset legitimate user passwords, and install software patches. In addition to tangible monetary losses, financial institutions suffer from reduced employee and IT productivity, loss of network resources, legal liability, and damage to their brand name and reputation.

From a customer perspective, phishing attacks have become a sober reminder of the vulnerability of the Internet and e-commerce. Trust in online payment systems and the ability of financial institutions to mitigate fraud are diminished by successful phishing attacks. According to Avivah Litan, vice president and research director at Gartner, Inc., the eventual impact of phishing attacks could slow e-commerce growth in the United States by one to two percent in 2005. "The whole promise of e-commerce—lower costs, increased revenue and quicker launches of marketing campaigns—all goes out the window if consumers cannot trust e-mail communications," says Litan. [42]

John Pescatore, Vice President for Internet Security at Gartner, Inc., a provider of research and analysis on the global information technology industry, recently told *Business Week*, "We expect a "flattening" of e-commerce because of consumer concerns about identity

[42] Alice Dragoon, "Fighting Phish, Fakes, and Frauds," *CIO*, September 7, 2004, <www.cio.com/archive/090104/phish.html>.

theft of financial and credit card information."[43] International Data Corp. (IDC), a provider of global market intelligence in the areas of information technology and telecommunications, released a report on October 18, 2004 noting that recent phishing attacks have hurt Asia Pacific e-commerce, forcing consumers to avoid making online purchases. Public statements and reports like Mr. Pescatore's and IDC's are reason for concern for financial institutions and e-commerce pundits around the world. There is little doubt that financial institutions and their customers are in the midst of a global epidemic of phishing attacks. Several phishing attacks in Asia and Europe during the past year demonstrate the severity of the problem. The Association for Payment Clearing Services (APACS) located in the United Kingdom, recently told BBC News Online that "it is worried by a surge in phishing scam e-mails."[44] In recent months, High Street banks such as Natwest, Barclays, and Lloyds TSB have come under fierce attack from cyber criminals. As a result, bank customers in the United Kingdom have been warned that they could be targets of future e-mail phishing scams. In May 2004, British police acted to end these threats by making one of the largest arrests of phishers to date. The arrest of 12 individuals accused of stealing hundreds of thousands of pounds from British bank accounts and depositing them into Russian accounts signaled only the beginning of law enforcement's involvement to curb phishing attacks.[45]

In *Germany*, two of the country's biggest banks, Postbank and Deutsche Bank AG, were victims of phishing attacks in late August 2004. In both cases, the e-mails requested that bank customers provide personal identification and transaction numbers to resolve fictitious account problems. The attacks apparently originated in the Far-East and Russia. Also in Russia, an individual known as "Robotector" recently sent out an e-mail virus with a

[43] eMarketer, *Scary Stats: Internet Attacks Worldwide*, September 22, 2004, <www.emarketer.com/Article.aspx?1003053 >.

[44] BBC News Online, *Britain Sees Surge in Phishing*, March 25, 2004

[45] "'Police arrest 12 for 'phishing'," *BBC News*, <newswww.bbc.net.uk/2/hi/uk_news/3687017.stm>.

subject line of "I Love You" to approximately 3 million bank customers throughout the world. The purpose of the e-mail was to secure user names and passwords, which would give cyber criminals located in Europe and South America access to customer bank accounts. One of Switzerland's largest regional banks, Basler Kantonalbank, recently warned its customers of suspicious e-mails requesting personal information claiming to originate from the bank. In Hong Kong, customers of the Hong Kong and Shanghai Banking Corporation became unknowing victims of a syndicate purporting to be a Hong Kong bank. From September 17, 2004 through October 6, 2004, bank customers received phishing e-mails asking them to click on an embedded hyperlink connected to a bogus web site. Eleven individuals ranging in ages from 21 to 58 were arrested in the case.

3.3 Scenario in Malaysia

In October 2006, thirteen people were arrested by the Malaysian police, including four university students, reported to be involved in phishing activities. The amount of losses on the part of the customers, according to the police, amounted to RM36, 000.[46] While the Association of Banks in Malaysia (ABM) states that a total of 159 online banking fraud cases mainly involving phishing were recorded in the first nine month of the year.[47] Former May bank's CEO Dato Amirsham A.Aziz asserts that customers should not shy from using Internet banking services as the fraud level recorded in the country is "not alarming".[48] Nevertheless the regulatory authority, the Bank Negara Malaysia (BNM) in its reaction, urges that both parties; the customers and financial institutions must take steps to ensure the security of the Internet banking. The BNM also states that all banks are required by the BNM to ensure that their Internet banking systems have appropriate security systems.[49]

[46] See Utusan Malaysia 10 October 2006

[47] Theedgeasia.com, available at http://www.theedgedaily.com/cms/contentPrint.jsp?id=om.tms.cms.article.

[48] Ibid

[49] Utusan Malaysia, 12 October 2006.

This is reiterated by the Deputy Prime Minister, when he reminds the banks to enhance the security of Internet banking services.[50] This matter will be discussed in the latter chapter.

In Malaysia, the reported incidences of fraudulent computer activity are on a rise as evident from the statistics reported by the Malaysian Computer Emergency Response Team or MyCERT. According to MyCERT[51], there were only 3 reported computer fraud incidences in 2000 but this number rose quickly in the subsequent years to 106 in 2004 and 364 in 2007. Phishing victims reported being deceived into visiting a fake website where perpetrators then stole their usernames and passwords and later used the information for the perpetrators' own advantage. This results in the breach of information security through the compromise of users' confidential data. Malaysian CERT (MyCERT), which is a unit within Malaysian Cyber Security Centre (MCSC), has been closely monitoring phishing activities in the country and even issued an advisory on possible phishing attacks on Internet banking users last month.   Their findings showed that 85 per cent of the phishing sites imitating local banks and other e-commerce Web sites reported were hosted overseas; those hosted in Malaysia mostly involved foreign banks. Through the interactions with other National Computer Emergency Response Teams in Australia, Japan and other countries, they are seeing that some cases involving large online payment gateways may involve organised groups with collaboration between spammers and hackers. For smaller-scale targets, they usually involve local players. Most of the banks targeted are not only in Malaysia; similar problems are faced in Europe and other countries.

[50] Ibid

[51] MyCERT, "Computer Crime Statistics," vol. 2008: MyCERT, 2008.

MyCERT acknowledged that the battle against phishing is far from over, but advised users not to be overly alarmed, saying that the problem is global and cases in Malaysia are relatively low compared to advanced countries[52].

The Association of Banks Malaysia (ABM) has reminded industry players, namely the commercial banks and users to be extra cautious and vigilant when conducting banking transactions online especially with the sharp increase in incidences involving scam emails.[53]

3.4 Technique and Variants of Phishing

Phishing is a particularly invidious attack on the Internet community because it almost always involves two separate acts of fraud.[54] The phisher first "steals" the identity of the business it is personating and then acquires the personal information of the unwitting customers who fall for the impersonation.[55] This has led commentators to refer to phishing as a "two-fold scam" and a "cybercrime double play".[56] Phishing involves sending customers a seemingly legitimate email request for account information, often under the guise of asking the customer to verify or reconfirm confidential personal information such as account numbers, social security numbers, passwords, and other sensitive information. In the email, the perpetrator uses various means to convince customers that they are receiving a legitimate message from someone whom the customer may already be doing business with, such as a bank.[57] Techniques such as a false "from" address or the use of seemingly legitimate bank logos, web links, and graphics may be employed to mislead the customer.

[52] Rozana Sani, "Phish in troubled water," in Computimes, Kuala Lumpur, Oct 2006

[53] Ahmad Nasir Mohd Zin and Zahri Yunos, "How to make online banking secure," in *The Star*. Kuala Lumpur, 2005.

[54] *See* Robert Louis B. Stevenson, "Plugging the Phishing Hole: Legislation versus Technology" (2005) Duke L. & Tech. Rev. 2.

[55] Ibid

[56] Ibid

[57] Comptroller of the Currency Administrator of National Banks, OCC Alert 2003-11.

After gaining the customer's trust, the perpetrator attempts to convince the customer to provide personal information and provides one or more methods for the customer to communicate that information back. For example, the email might include a link to the perpetrator's web site that contains a form for entering personal information.[58] Like the email, the web site is designed to trick the customer into believing that it belongs to the bank. Alternatively, the email might simply include an embedded form for the customer to complete.[59]

According to Aaron Emigh, phishing is perpetrated in many different ways[60]. Phishers are technically innovative, and can afford to invest in technology. It is a common misconception that phishers are amateurs. This is not the case for the most dangerous phishing attacks, which are carried out as professional organized crime. As financial institutions have increased their online presence, the economic value of compromising account information has increased dramatically. Criminals such as phishers can afford an investment in technology commensurate with the illegal benefits gained by their crimes. Given both the current sophistication and rapid evolution of phishing attacks, a comprehensive catalogue of technologies employed by phishers is not feasible.

Several types of attacks are discussed below. The distinctions between attack types are porous, as many phishing attacks are hybrid attacks employing multiple technologies. For example, a deceptive phishing email could direct a user to a site that has been compromised via content injection, which installs malware that poisons the user's hosts file. Subsequent attempts to reach legitimate web sites will be rerouted to phishing sites, where confidential information is compromised using a man-in-the-middle attack phishing.

[58] Ibid

[59] Ibid

[60] Aaron Emigh, "Online Identity Theft: Phishing Technology, Chokepoints and Countermeasures", (October 3, 2005), at 11

3.4.1 Deceptive Phishing

While the term “phishing” originated in AOL account theft using instant messaging, the most common vector for deceptive phishing today is email. [61] In a typical scenario, a phisher sends deceptive email, in bulk, with a “call to action” that demands the recipient click on a link. Examples of a “call to action” include:

a) A statement that there is a problem with the recipient’s account at a financial institution or other business. The email asks the recipient to visit a web site to correct the problem, using a deceptive link in the email.

b) A statement that the recipient’s account is at risk, and offering to enroll the recipient in an anti-fraud program.

c) A fictitious invoice for merchandise, often offensive merchandise, that the recipient did not order, with a link to “cancel” the fake order.

d) A fraudulent notice of an undesirable change made to the user’s account, with a link to “dispute” the unauthorized change.

e) A claim that a new service is being rolled out at a financial institution, and offering the recipient, as a current member, a limited-time opportunity to get the service for free.

In each case, the web site to which the user is directed collects the user’s confidential information. If a recipient enters confidential information into the fraudulent web site, the phisher can subsequently impersonate the victim to transfer funds from the victim’s account, purchase merchandise, take out a second mortgage on the victim’s home, file for unemployment benefits in the victim’s name, or inflict other damage.

[61] Ibid

In many cases, the phisher does not directly cause the economic damage, but resells the illicitly obtained information on a secondary market. Criminals participate in a variety of online brokering forums and chat channels where such information is bought and sold.

There are many variations on deception-based phishing schemes. With HTML email readers, it is possible to provide a replica of a login page directly in email, eliminating the need to click on a link and activate the user's web browser.

Sometimes, a numeric IP address is used instead of a host name in a link to a phishing site. In such cases, it is possible to use Javascript to take over the address bar of a browser or otherwise deceive the user into believing he or she is communicating with a legitimate site. A *cousin domain attack* avoids the need for such complexity by using a domain name controlled by a phisher that is deceptively similar to a legitimate domain name, such as www.commerceflowsecurity.com instead of www.commerceflow.com. Sometimes, an initial deception-based message leads to an installation of malware when a user visits the malicious site.

3.4.2 Malware-Based Phishing

Malware-based phishing refers generally to any type of phishing that involves running malicious software on the user's machine. Malware-based phishing can take many forms. The most prevalent forms are discussed below.[62]

In general, malware is spread either by social engineering or by exploiting security vulnerability. A typical social engineering attack is to convince a user to open an email attachment or download a file from a web site, often claiming the attachment has something to do with pornography, salacious celebrity photos or gossip. Some downloadable software can also contain malware. Malware is also spread by security exploits either by propagating

[62] See The Joint Report of the US Department of Homeland Security –SRI International Identity Theft Technology Council and the Anti-Phishing Working Group, "The Crimeware Landscape: Malware, Phishing, Identity Theft and Beyond" Oct 2006

a worm or virus that takes advantage of a security vulnerability to install the malware, or by making the malware available on a web site that exploits security vulnerability. Traffic may be driven to a malicious web site via social engineering such as spam messages promising some appealing content at the site, or by injecting malicious content into a legitimate web site by exploiting a security weakness such as a cross-site scripting vulnerability on the site.

3.4.3 Keyloggers and Screenloggers

Keyloggers are programs that install themselves either into a web browser or as a device driver, which monitor data being input and send relevant data to a phishing server. [63] Keyloggers use a number of different technologies, and may be implemented in many ways, including:

- A browser helper object that detects changes to the URL and logs

Information when a URL is at a designated credential collection site;

- A device driver that monitors keyboard and mouse inputs in conjunction with monitoring the user's activities; and
- A *screenlogger* that monitors both the user's inputs and the display to thwart alternate on-screen input security measures.

Keyloggers may collect credentials for a wide variety of sites. Keyloggers are often packaged to monitor the user's location and only transmit credentials for particular sites. Often, hundreds of such sites are targeted, including financial institutions, information portals, and corporate VPNs. Various secondary damage can be caused after a keylogger compromise. In one real-world example, the inclusion of a credit reporting agency in a keylogger spread via pornography spam led to the compromise of over 50 accounts with

[63] Ibid

access to the agency, which in turn were ultimately used to compromise over 310,000 sets of personal information from the credit reporting agency's database.

3.4.4 Session Hijackers

Session hijacking refers to an attack in which a user's activities are monitored, typically by a malicious browser component[64]. When the user logs into his or her account, or initiates a transaction, the malicious software "hijacks" the session to perform malicious actions once the user has legitimately established his or her credentials. Session hijacking can be performed on a user's local computer by malware, or can also be performed remotely as part of a man-in-the-middle attack, which will be discussed later. When performed locally by malware, session hijacking can look to the targeted site exactly like a legitimate user interaction, being initiated from the user's home computer **Web Trojans** Web Trojans are malicious programs that pop up over login screens to collect credentials. The user believes that he or she is entering information on a web site, while in fact the information is being entered locally, and then transmitted to the phisher for misuse.

3.4.5 Hosts File Poisoning

If a user types www.company.com into his or her URL bar, or uses a bookmark, the user's computer needs to translate that address into a numeric address before visiting the site[65]. Many operating systems, such as Windows, have a shortcut "hosts" file for looking up host names before a DNS (Domain Name System) lookup is performed. If this file is modified, then www.company.com can be made to refer to a malicious address. When the user goes there, he or she will see a legitimate-looking site and enter confidential information, which actually goes to the phisher instead of the intended legitimate site.

[64] See "Threat Centre" available at http://www.scansafe.com
[65] See "Types of Phishing Attacks" available at http:// http://tech.yahoo.com/gd/types-of-phishing-attacks

3.4.6 System Reconfiguration Attacks

System reconfiguration attacks modify settings on a user's computer to cause information to be compromised[66]. One type of system reconfiguration attack is to modify a user's DNS servers, so faulty DNS information can be provided to users as described below. Another type of system reconfiguration attack is to install a web proxy, through which the user's traffic will be passed. This is a form of a man-in-the-middle attack, which is discussed separately.

3.4.7 Data Theft

Once malicious code is running on a user's computer, it can directly steal confidential information stored on the computer[67]. Such information can include passwords, activation keys to software, sensitive email, and any other data that is stored on a victim's computer. By automatically filtering data looking for information that fits patterns such as a social security number, a great deal of sensitive information can be obtained. Data theft is also widely used for phishing attacks aimed at corporate espionage, based on the fact that personal computers often contain the same confidential information that is also stored on better protected enterprise computers. In addition to espionage for hire, confidential memos or design documents can be publicly leaked, causing economic damage or embarrassment.

3.4.8 DNS-Based Phishing ("Pharming")

DNS-based phishing also known as pharming is used here to refer generally to any form of phishing that interferes with the integrity of the lookup process for a domain name[68]. This includes hosts file poisoning, even though the hosts file is not properly part of the Domain Name System. Hosts file poisoning is discussed in the malware section since it involves changing a file on the user's computer. Another form of DNS-based phishing involves

[66] Aaron Emigh, "Online Identity Theft: Phishing Technology, Chokepoints and Countermeasures" supra n.63

[67] Ibid

[68] Abu Bakar Munir and Siti Hajar Mohd Yasin, "Would the Phishers get Hooked", (April 2007), Bileta p.5

polluting the user's DNS cache with incorrect information that will be used to direct the user to an incorrect location. If the user has a misconfigured DNS cache, this can be done directly. It can also be done with a system reconfiguration attack that changes the user's DNS server to a malicious server, by hacking a legitimate DNS server, or by polluting the cache of a misconfigured legitimate DNS server.

The U.S Federal Deposit Insurance Corporation (FDIC) describes pharming as the practice of redirecting Internet domain name requests to false websites in order to capture personal information, which may later be used to commit fraud and identity theft. It is the redirection of an individual to an illegitimate website through technical means.[69]

Pharming, like other types of phishing, aims to gather personal information from the unsuspecting victims; the difference is that pharming does not rely on email solicitation.

Instead, this attack method redirects the victims to a malicious website. Chris Risley said, "Phishing is to pharming what a guy with a rod and a reel is to a Russian trawler. Phishers have to approach their targets one by one. Pharmers can scoop up many victims in a single pass."[70]

Another commentator, distinguishing pharming from phishing, states, "Phishing is throwing the bait out and hoping to get a bite. Pharming is planting the seeds and not trusting to chance."[71]

Pharming can occur in four different ways. First, static domain name spoofing-the pharming attempts to take advantage of slight misspellings in the domain names to trick users into inadvertently visiting the pharmer's web site. Second, malicious software

[69] Federal Deposit Insurance Corporation, "Guidance on How Financial Institutions Can Protect Against Pharming Attacks," July 18, 2005, at 1.

[70] Cited in Michelle Delio, "Pharming Out-Scams Phishing", Wired News, available at http://www.wired.com/news/infostructure/1,66853-1.html

[71] Scott Chasin, cited in William Jackson, "Is a New ID Theft Scam in the Wings?", GCN, available at http://www.gcn.com/online/vo11-no1/34815-1.html

(malware) -viruses and Trojans on a consumer's personal computer may intercept the user's request to visit a particular site and redirect the user to the site that the pharmer has set up. Thirdly, domain hijacking –a hacker may steal or hijack a company's legitimate web site, allowing the hacker to redirect all legitimate traffic to an illegitimate site.[72] Fourthly, domain name server (DNS) poisoning - when a user types a name into the web browser's address bar, a Domain Name System server reads the name, finds the corresponding numeric address and directs the user to the official website. In a DNS poisoning scheme, a hacker will alter a company's IP address on a domain server so that when a user enters the correct web address, the server will direct the user to a different address that contains a bogus website, built to steal passwords and other data.

3.4.9 Content-Injection Phishing

Content-injection phishing refers to inserting malicious content into a legitimate site[73]. The malicious content can redirect to other sites, install malware on a user's computer, or insert a frame of content that will redirect data to a phishing server.

There are three primary types of content-injection phishing, with many variations of each:

1) Hackers can compromise a server through security vulnerability and replace or augment the legitimate content with malicious content.[74]

2) Malicious content can be inserted into a site through a cross-site scripting vulnerability. A cross-site scripting vulnerability is a programming flaw involving content coming from an external source, such as a blog, a user review of a product on an e-commerce site, an auction, a message in a discussion board, a search term or a web-based email. Such externally supplied content can be a malicious script or other

[72] Federal Deposit Insurance Corporation, "Guidance on How Financial Institutions Can Protect Against Pharming Attacks," July 18, 2005,

[73] See "How to Avoid the Internet Scam", available at http://www.associatedcontent.com/article/105088/_how_to_avoid_the_internet_scam.html

[74] Ibid

content that is not properly filtered out by software on the site's server, and runs in the web browser of a visitor to the site.[75]

2) Malicious actions can be performed on a site through SQL injection vulnerability. This is a way to cause database commands to be executed on a remote server that can cause information leakage. Like cross-site scripting vulnerabilities, SQL injection vulnerabilities are a result of improper filtering. Cross-site scripting and SQL injection are propagated through two different primary vectors. In one vector, malicious content is injected into data stored on a legitimate web server, such as an auction listing, product review or web-based email. In the other vector, malicious content is embedded into a URL that the user visits when he or she clicks on a link. This is commonly a URL that will be displayed on screen or used as part of a database query, such as an argument to a search function.[76]

3.4.10 Man-in-the-Middle Phishing

A man-in-the-middle[77] attack is a form of phishing in which the phisher positions himself between the user and the legitimate site.[78] Messages intended for the legitimate site are passed to the phisher instead, who saves valuable information, passes the messages to the legitimate site, and forwards the responses back to the user.[79] Man-in-the-middle attacks can also be used for session hijacking, with or without storing any compromised credentials. Man-in-the-middle attacks are difficult for a user to detect, because the site will work properly and there may be no external indication that anything is wrong.[80]

Man-in-the-middle attacks may be performed using many different types of phishing. Some forms of phishing, such as proxy attacks, are inherently man-in the- middle attacks. However, man-in-the-middle attacks may be used with many other types of phishing,

[75] Ibid
[76] Ibid
[77] Supra n.57
[78] See Abu Bakar Munir , supra n. 71
[79] See the Report Oct 2006, supra n.65
[80] See Aaron Emigh, supra n.63

including DNS-based phishing and deception-based phishing. Normally, SSL web traffic will not be vulnerable to a man in the middle. The handshake used by SSL ensures that the session is established with the party named in the server's certificate, and that an attacker cannot obtain the session key; and SSL traffic is encrypted using the session key so it cannot be decoded by an eavesdropper. Proxies have a provision for tunneling such encrypted traffic. However, a malware-based attack can modify a system configuration to install a new trusted certificate authority, in which case such a man in the middle can create its own certificates for any SSL-protected site, decrypt the traffic and extract confidential information, and re-encrypt the traffic to communicate with the other side. In practice, man-in-the-middle attacks simply do not use SSL, since users do not generally check for its presence.

Man-in-the-middle attacks can also compromise authentication credentials, such as one-time or time-varying pass codes generated by hardware devices. Such stolen credentials can be used by the phisher for authentication as long as they remain valid.

3.4.11 Search Engine Phishing

Another approach taken by phishers is to create web pages for fake products, get the pages indexed by search engines, and wait for users to enter their confidential information as part of an order, sign-up, or balance transfer[81]. Such pages typically offer products at a price slightly too good to be true. Scams involving fraudulent banks have been particularly successful. A phisher creates a page advertising an interest rate slightly higher than any real bank.

[81] Robert Ma, "Phishing Attack Detection by Using a Reputable Search Engine", University of Toronto, 2006

Victims find the online bank via a search engine, and enter their bank account credentials for a “balance transfer” to the new “account.” Greed is a powerful motivator that can cloud judgment. Some victims even provided their bank account numbers to “Flintstone National Bank,” of “Bedrock, Colorado.”

3.4.12 Voice Phishing (Vishing)

“Vishing” or “voice phishing” is relatively new tactic that phishers adapted to fish in the ocean of the Internet[82]. This has been described as follows; “Vishing can work in two different ways. In one version of the scam, the consumer receives an e-mail designed in the same way as a phishing email, usually indicating that there is a problem with the account. Instead of providing a fraudulent link to click on, the e-mail provides a customer service number that the client must call and then prompted to “log-in” using account numbers and passwords. The other version of the scam is to call consumers directly and tell them that they must call the fraudulent customer service number immediately in order to protect their account.”[83]

Vishing operate slightly differently. Rather than asking the receivers to reply by clicking on a link, the “visher” ask the receivers of the e-mail to call a number and provide confidential details over the phone. Victims call the number in the mistaken belief it belongs to their bank or Credit Card Company. Instead, they are connected to a Voice over Internet Protocol (VoIP) phone that can recognize, and record, telephone keystrokes.[84]

[82] See Abu Bakar Munir , “Would the Phishers get Hooked” pg 4, supra n.71

[83] NGS/NISR, “The Phishing Guide: Understanding & Preventing Phishing Attacks”

[84] *See* Privacy Commissioner of Canada, “Recognizing Threats to Personal Data: Four Ways That Personal Data Gets Hijacked Online’, p 3.

3.4.13 Spear Phishing

Spear phishing is a colloquial term that can be used to describe any highly targeted phishing attack.[85] Spear phishers send spurious e-mails that appear genuine to a specifically identified group of Internet users such as certain users of a particular product or service, online account holders, employees or members of a particular company, government agency, organization, group, or social networking website.[86] Much like a standard phishing e-mail, the message appears to come from a trusted source, such as employer or a colleague who would be likely to send e-mail message to everyone or a select group in the company.[87] Because it comes from a known and trusted source, the request for valuable data such as user names or passwords may appear more plausible.[88]

3.5 Conclusion

Phishing is online identity theft in which confidential information is obtained from an individual. Phishing includes deceptive attacks, in which users are tricked by fraudulent messages into giving out information; malware attacks, in which malicious software causes data compromises; and DNS-based attacks, in which the lookup of host names is altered to send users to a fraudulent server.

The problems of phishing causing billion dollar losses and indirect losses are much higher, including customer service expenses, account replacement costs, and higher expenses due to decreased use of online services in the face of widespread fear about the security of online financial transactions. Phishing also causes substantial hardship for victimized consumers, due to the difficulty of repairing credit damaged by fraudulent activity.

[85] USA and Canada Report on Phishing, A Report to the Minister of Public Safety and Emergency Preparedness Canada and the Attorney General of the United States, October 2006, 3.
[86] Ibid
[87] Ibid
[88] Ibid