PHISHING, PHARMING AND IDENTITY THEFT

Richard G. Brody, University of New Mexico
Elizabeth Mulig, University of South Florida St. Petersburg
Valerie Kimball, University of South Florida St. Petersburg

ABSTRACT

Identity theft is the fastest growing crime in America, occurring when the criminal obtains confidential information from an individual or business and uses it to access private financial accounts. In today's world of information technology, many thieves prey on their victims via the Internet. The level of disclosure of personal information in many of today's information age transactions is what leaves so many individuals and businesses open to identity theft.

Two of the most common ways that thieves acquire personal information to aid them in identity theft are phishing and pharming. Phishing utilizes bulk e-mail messages to entice recipients into revealing personal information. Pharmers, on the other hand, cast a wide net for the unwary. There is a huge potential reward for criminals who succeed in these malicious acts. In addition, now that organized crime has become involved, the money available to help thieves carry out the crimes is immense.

Information indicates that U.S. losses are approximately $52.6B per year. Approximately 90% of this total is being carried by businesses and financial institutions, and consumers' cost is the remaining 10%. Another huge cost of identity theft, to businesses is the loss of customer trust. Creating awareness is one of the most important tools in fighting identity theft via phishing and pharming schemes. However, it is not enough. Financial institutions and consumers need to work together to prevent future occurrences. Hopefully, with advanced technology and continued educational outreach by businesses, financial institutions and educational organizations, there will be a decline in the level of identity theft taking place on the Internet.

INTRODUCTION

The United States Postal Service, the Federal Bureau of Investigation, the National Crime Prevention Council, the Office of the Inspector General and others have all referred to identity theft as the fastest growing crime in America. Identity theft occurs when a criminal obtains confidential information from an individual or business and uses it to access private financial accounts. The personal information stolen from an individual in order to gain this access might include social security number (SSN), address, date of birth, or mother's maiden name. Once offenders have this

information, they have the ability to open bank accounts, make loans, rent homes, apartments or automobiles, set up utilities and a myriad of other things, all in another individual's name. Information stolen from a business might include bank account numbers, bank access codes, computer access codes or restricted employee records. Thus, just as with identity theft against an individual, the company's financial accounts, or perhaps those of individuals whose information was taken from the company, are then capable of being violated.

In today's world of information technology, many thieves prey on their victims via the Internet. The level of disclosure of personal information in many of today's information age transactions is what leaves so many individuals and businesses open to identity theft. Online purchases, credit card purchases at restaurants or gas stations, or ATM access all require personal information. When a thief gains access to this information, individuals and/or businesses can become potential victims of identity theft. It has been estimated that there were nearly 10 million cases of identity theft in 2005, which translates to 4.6% of the U.S. population annually (How Many…, 2006). Identity theft is not limited to the U.S. so when it is considered globally, the number of cases increases significantly.

At the recent Chief Securities Officer (CSO) Perspectives Conference, it was reported that: (1) 53 million identities have been stolen to date and 19,000 more are stolen every day and (2) Companies, on average, spend 1,600 work hours per incident at a cost of $40,000 to $92,000 per victim (Friedenberg, 2006). U.S. losses have stabilized (since 2003) at approximately $52.6 billion per year and that approximately 90% (or some $47.6 billion) of this total is being carried by businesses and financial institutions, with consumers' cost is the remaining 10%, or around $5 billion (How Many…, 2006). Focusing on these statistics on a per incident basis, the average cost has been stated as $10,200 for institutions and $1,180 for individuals.

Another huge cost of identity theft, to businesses, is the loss of customer trust, resulting in a loss of positive customer relations. According to Edward McNicholas, a partner in the law firm Sidley Austin, "if you experience a security breach [of customers' personal information], 20 percent of your affected customer base will no longer do business with you, 40 percent will consider ending the relationship, and 5 percent will be hiring lawyers!" (Friedenberg, 2006).

While there are many ways in which identities are stolen, this paper will focus on two: phishing and pharming. Each of these schemes relies on the Internet to gain the information necessary to acquire one's identity and while phishing is much more common, pharming is much more difficult to defend against as an individual. In a nutshell, phishing utilizes bulk e-mail messages to entice recipients into revealing personal information, while pharming secretly installs a virus or malicious program on a computer. As a result of the program, when the user types in legitimate web address, they are taken to an imitation of the site. Using these methods, identity thieves seek social security numbers, financial account numbers, credit card numbers, mothers' maiden names, and other personal information. The amount of personal data available on the Internet is amazing and criminals instigate huge amounts of fraud with this easily obtained information.

While phishing and pharming are opportunistic crimes, the level of criminal organization, motivation, and financing is escalating. The problem is directly related to the anonymity of the Internet and the amount of the money that can be quickly stolen. For instance, an e-mail that appeared to be from the security division of e-gold.com was sent to members to update their configuration settings. Authorized users of e-gold.com buy and sell title to gold deposits held in London and the United Arab Emirates. Opening the official-looking e-mail instantly downloaded a keylogger virus. The malicious program opened a hidden web session in the background draining the user's account while they were connected to the e-gold.com official web site. According to Paul Stamp, a Forrester Research computer security analyst, the amount of money stolen this way is unknown (Cyber crime…, 2005). This is only one example of phishing; however, it demonstrates how powerful and dangerous a tool for fraud it is, when employed by the "right" user.

In order to minimize the risk of being victims of identity theft, individuals and businesses must take measures to protect against theft of their private information. Some of these measures involve simply using common sense about giving out private data or providing it online, others involve technical security measures.

PHISHING

As stated previously, phishing is initiated through bulk emails. The sender of the email somehow persuades the recipient to voluntarily giving personal information. Phishing is much more insidious than spam e-mail messages selling products. The average time for spammers to target e-mail addresses is 29.5 days. Identity criminals, on the other hand, typically act on victims' responses within 14 hours of receipt. The difference in speed may be due to the operating structure of the crime. Typically there is a division of labor between the harvesters of e-mail addresses and the actual spam senders. Phishing is a serious solitary criminal activity according to Matthew Prince, co-creator of Project Honey Pot a spam tracking service (Mindlin, 2005).

Phishing e-mails are lures cast into cyberspace in an attempt to hook the unwary. For example, a criminal may send out one million e-mails that appear to be from SunTrust Bank. By chance, some recipients will actually be SunTrust customers. This does not mean that a list of SunTrust customers is circulating on the Internet. Still, in some instances, financial institutions may have disclosed customers' information. Privacy notices warn individuals that their information may be shared unless the customer follows specific instructions (Huntley, 2005).

Even the Internal Revenue Service is not immune to phishers. In November, 2005 the IRS issued a consumer alert about e-mails from taxrefunds@irs.gov (IRS Warns…, 2005). The e-mail directs readers to a link that requests social security and credit card numbers. Stolen identity can be used in multiple ways, for example, to open new credit accounts, apply for loans or benefits, or to file a fraudulent tax return (Palmer, 2006). Identity thieves select companies that are likely to appear

relevant to its potential victims. In addition to various banks, other popular companies used in the phishing emails are eBay and paypal, high volume Internet sites.

Consumers are enticed into revealing their personal identification and financial information on fraudulent web sites, also known as spoofed web sites. The victim may receive a phishing e-mail describing a plausible problem that appears serious. To correct the supposed issue, the consumer will be provided with a link to a sophisticated imitation of the bank's web site in order for the victim to confirm account information. The phisher can then use the stolen PIN numbers, passwords, and identity to empty bank accounts.

The phisher has another option: he or she can sell the information. Despite years of security improvements and improved law enforcement, stolen consumer information can be easily found for sale on the Internet. The black market for this data is well organized. Buyers, sellers, intermediaries and even service industries meet in cyberspace, frequently on web sites that are run from computer servers in the former Soviet Union. In fact, traders earn titles, ratings and reputations for the quality of the stolen goods. Malicious-code writers advertise their services to phishers who in turn contract with spammers to send out millions of increasingly sophisticated phony e-mails to lure victims (Zeller, 2005b).

The logic behind every phishing campaign is that someone, somewhere, will always take the bait. True, phishing e-mails and web sites have improved significantly. In addition, new computer users along with a portion of the population are simply gullible and get tricked by implausible offers. Over twenty years ago, J. Barton Bowyer proposed that deception follows two basic strategies, hiding the real or showing the false. To hide the real, a criminal might use masking: concealing critical characteristics, repackaging: adding or subtracting components, or dazzling: obscuring the truth. To show the false a thief might use mimicking: false imitations, inventing: lies made out of a portion of the truth, or decoying: distracting from the truth (Zeller, 2005a).

Twenty years later researchers at the University of Virginia and the University of Texas at Austin suggested that these same basic categories transfer into the virtual world. There are few barriers to enter online crime. Moreover, the Internet provides an incredible opportunity to reach millions of potential victims at the same time. In other words, for criminals, phishing continues to pay (Grazioli and Jarvenpaa, 2003).

A potentially more lethal version of phishing, spear-phishing, is raising alarms among the digital world's watchdogs. This hybrid form of phishing casts lures for specific victims instead of casting a net across cyberspace to catch hordes of unknown prey. Security specialists say that spear-phishing is much harder to detect than phishing. Messages appear to be legitimately sent from well-known organizations with a twist, the e-mails are targeted at people known to have an established relationship with the imitated sender. Software, for example a keylogger, is used to monitor the web access by victims and it starts recording information when the user enters the sites of interest to the fraud perpetrator, enabling them to directly target those persons. In addition, spear-phishing is more

likely to be linked to sophisticated groups seeking financial gain, trade secrets or military information. It is one of the most insidious cyber crimes encountered (O'Brien, 2005).

Alan Paller, research director at the SANS Institute, a group that trains and certifies computer security professionals, believes that there has never been a better attack method than spear-phishing (O'Brien, 2005). There is little data about actual incidents of spear-phishing because victims are hesitant to come forward. In June 2005, the National Infrastructure Security Coordination Centre, a government agency that monitors computer security in the United Kingdom, issued a rare public warning about a spear-phishing campaign aimed at industrial and government computer networks. "Files used by the attackers are often publicly available on the Web or have been sent to distribution lists," the warning said. "The attackers are able to receive, trojanise and resend a document within 120 minutes of its release, indicating a high level of sophistication" (Targeted Trojan..., 2005). The warning reported that the phishing e-mail messages appear to come from a trusted sender. In addition, antivirus software and firewalls did not protect receivers, and worse, there was no way to completely protect any computer connected to the Internet from the attack once the recipient opened the spear-phishing e-mail. The files used by the criminals are often publicly available on the Internet or have been sent to distribution lists.

Cyber crime is cost effective for spear-phishers. CipherTrust, a computer security firm, reports that a spear-phisher can rent a server for as little as $300 a month after paying a $100 set-up fee. Spam-sending software on the server is approximately $1,200 a month and for another $1,900 a month the spear-phisher obtains spam-sending proxies, a database of e-mail addresses, and other add-ons. The relatively low-cost endeavor can reap lucrative rewards depending on the number of victims hooked (A Little Fraud…, 2006).

Johannes Ullrich at the SANS Institute's Internet Storm Center believes that phishing and spear-phishing will merge so that company logos can be stolen from web sites to build customized databases of corporate logos. After all, the goal of all attacks is automation, getting the largest effect with the least amount of effort (O'Brien, 2005).

PHARMING

Pharming is a more technologically advanced form of phishing in which a virus or malicious program is secretly installed on a computer. Typing in a legitimate web address takes the computer user to an imitation of the site. As a result, any information provided at the fake web site, such as account numbers or passwords, can be stolen (ID thieves preying…, 2005). Thus, even though the computer screen displays the desired web address, the domain-name server system has redirected the traffic to a fraudulent location (Biersdorfer, 2005).

Computer users unintentionally download the malicious program without clicking on a link or opening an attachment. Opening a pharmer's e-mail message is all that is required to install the stealth application redirecting the browser to a counterfeit web site. Moreover, the newest form of

pharming does not even require e-mail. A virus can attack through Microsoft Messenger using a keylogger. This type of virus tracks a user's keystrokes on legitimate web sites and captures passwords. Consequently, consumers who use the same password on numerous sites expose themselves to multiple frauds (Hicks, 2005).

Pharmers cast a wide net across the Internet to catch prey. Redirecting Internet traffic to fraudulent web sites can be done several ways. For instance, pharmers often take advantage of spelling mistakes in domain names. The pharmer builds a web site with one letter missing from the legitimate address to trick the unwary into believing the address is genuine. Another popular mode of pharming is malware, malicious software. This type of virus alters the code of a consumer's computer causing a correctly typed address to be redirected to a fraudulent web site. Slamming is an additional method utilized by pharmers to redirect Internet traffic. Slamming takes place when a domain transfer request is submitted to move the domain name to a different registrar. The pharmer, who is also the account holder at the new registrar, then controls where the web address sends computer users (Swann, 2005).

Domain name server poisoning is still another avenue available to pharmers. Domain name servers (DNS) convert web addresses into Internet Protocol addresses and routes the computer user to the correct location. Thirteen root DNS servers cover the entire Internet along with a number of local servers. Once reconfigured, the DNS can send users to any number of web sites and seriously compromise the entire Internet system (Swann, 2005). To illustrate, once a web URL address is typed into a browser, it accesses a DNS server to retrieve a numeric Internet Protocol (IP) address corresponding to that URL address in order to display the requested web page. A pharming mode of operation is to alter the list of addresses in a DNS server so that a legitimate URL address points to an illegitimate Internet Protocol address, the fraudulent web site (Buckler, 2005).

Pharming attacks usually target small local servers operated by Internet service providers (ISP). However, these attacks can be aimed higher, specifically, upon the 13 servers on which all other DNS servers rely. DNS security extensions (DNSsec) is designed to guard against these types of threats by encrypting addresses with a procedure similar to the IP security protocol used to protect e-commerce transactions. DNSsec offers the ability to verify that the address returned by a DNS server has not been altered (Buckler, 2005).

Unfortunately, DNSsec is rarely utilized because it is only effective in a tight community where information is sent back and forth between itself. It is simply not practical to secure sub-domains one at a time due to the number of security keys involved. Ronald Aitchison, author of Pro DNS and Bind, a book on DNS systems, believes that DNSsec would be much more effective if applied to top-level domains such as dot-com, dot-org and dot-edu along with country code domains like Canada's dot-ca. Still, adoption of DNSsec is not enough. Computers reading Internet Protocol addresses must request security data from the secured servers for verification that the web address returned is legitimate (Buckler, 2005).

To date, Sweden is the only country to publicize DNSsec implementation. The transition for that country began in mid-September 2005. Due to the critical nature of the entire DNS system, some countries are hesitant to follow Sweden's lead. The Canadian Internet Registration Authority is studying the issue and expects to learn from Sweden's experience to ensure that Canada's own implantation of DNSsec goes smoothly (Buckler, 2005).

SOURCE COUNTRIES

While reports of phishing and pharming scams may appear to indicate Eastern European and Asian countries as the top source, surprisingly, the United States is the biggest phisher with 34.1 percent of the total. China and Korea fall way behind in second and third place with 15 percent and 8.17 percent, respectively (Phishing Activity…, 2006). Despite the fact that the United Kingdom does not appear as a top source on the phishing list, pharming is one of the top Internet crimes in the United Kingdom (Britt, 2005).

Although the United States is indeed the top source of phishing scams, the English-speaking criminals, especially Americans, are often the lowest members of the organization. According to Gregory Crabb, an investigator with the United States Postal Inspection Service and the economic crimes division of Interpol, American phishers are "a dime a dozen" and easy to track down (Zeller, 2006). Crabb also indicates, however, that low members of the organization often lead to recruiters in Eastern Europe and Russia.

Unfortunately, due to privacy rights and political treaties, stopping international crime is a challenge. It is extremely difficult to entice the cooperation of foreign investigators. Indeed, former Eastern Bloc countries have more immediate local crime issues to tackle shuffling American banks and consumers to the bottom of their priority list. In some countries the problem is compounded since law enforcement officials in charge of fighting online crime may not have ever owned a credit card themselves. These investigators do not clearly understand how credit cards work. Even more discouraging, once a top Eastern European is caught, he or she is often quietly released while awaiting trial (Zeller, 2006).

Whitfield Diffie, the chief security officer of Sun Microsystems, points to a basic flaw in most e-mail systems: the failure to reveal the history of an e-mail. He notes that a message that appears to be from a recognizable company like Amazon.com could have actually originated in the Ukraine, Romania, Bulgaria, Poland, Russia, or any other country that is a favorite place for phishing scams. Some computer security specialists agree that including that basic information would allow software programs to warn Internet users that the 'from' address is not consistent with the path history (O'Brien, 2005).

THE VICTIMS AND THE COSTS

These fraudulent Internet scams pose a dangerous threat to both the financial sectors and consumers. Phishing and Pharming schemes are on the rise, and according to studies, this is a problem that will continue to burden Internet users for years to come. For the past two years, there has been a tremendous growth in the number of cases reported. In 2005, the Gartner Phishing Study showed that 73 million Americans who used the Internet had received an average of 50 phishing e-mails in the last year (Gartner survey…, 2005). In the nine months ended February 2005, the monthly growth in phishing sites rose by approximately 26 percent (Phishing Activity…, 2005).

The creativity and savvy of hackers has grown, and consequently, so has the number of phishing reports submitted. In January 2006, there were 17,877 cases reported. This is the largest number ever recorded and that figure is 50 percent higher than the previous year. Even more worrying is the number of phishing sites that are appearing on the Internet. The Anti-Phishing Working Group recorded 9,715 sites in January 2006, up from just 4,630 in November 2005 (Malone, 2006).

Technology experts say there are a number of factors contributing to the growth of these attacks. Hackers are better motivated and better financed than ever, compared to the mid-1990's when criminal hacking was just getting off the ground. The hacker community is becoming more dangerous (Cyber Crime.., 2005). Their prevalent skill in disguising scam attacks to trick end users is ever growing. What is worse is that most people do not even realize they are being taken and by the time they do become aware, it is too late.

According to the Anti-Phishing Act of 2005 (New Leahy Bill…, 2005), organized crime is now allegedly involved, and is using sophisticated methods to escalate attacks in new, hard-to-detect ways. Organized crime bosses are "catching on" to the potential this type of activity provides. There are piles of cash to be made through these scams and they are willing to pay big bucks to someone who can perpetrate this sort of cyber attack (Cyber Crime, 2005). Also, perpetrators of these crimes typically use a decentralized approach, with one party holding customer information, another originating the initial message, and still another handling the cash that is illegally obtained. Consequently, the financial sector is finding itself up against not one, but perhaps 20 people orchestrating an attack (Sturgeon, 2005).

Not surprisingly, the most spoofed sites are in the financial sector, with 92 percent of recorded phishing and pharming attempts targeting banks and other financial institutions (Malone 2006). However, in 2005, there has been a huge increase (633%) in the number of credit unions, regional and mid-sized to small-sized banks attacked by fraudsters. This movement could be a result of larger banks implementing stronger security measures; leaving the smaller banks vulnerable to attacks (PSECU Battles…, 2005).

Both consumers and institutions face a tremendous amount of financial loss if confronted with this type of fraud. In May 2005, a Connecticut-based research and advisory firm conducted a study

on phishing and found that 1.2 million Americans lost a total of $929 million in the previous year due to phishing scams (Gartner Survey…, 2005). They also established that a typical phishing attack could cost a financial institution between $50 and $60 per account compromised, or $50,000 per attack. Institutions also need to be concerned with the costs associated with disabling the phishing sites, resetting legitimate passwords, and installing software patches (Hicks, 2005).

Security measures need to be implemented within financial organizations to prevent phishing and pharming attacks from ever taking place. Huge costs can also stem from creating secure systems that can detect this type of fraud. It is likely that over the next several years, banks will spend millions of dollars enhancing information security in response to the recent Federal Financial Institutions Examination Council (FFIEC) guidelines. FFIEC guidelines were updated in response to the increased threats from phishing and pharming scams. These new guidelines suggest that financial institutions assess the risk associated with their Internet banking applications, identify mitigating actions and adjust their information security programs to implement those actions. Theoretically, the FFIEC does not consider an identification name and password alone as a sufficient security measure for Internet-based banking. This current practice of using an identification name and password is extremely susceptible to fraud. Therefore, the FFIEC guidelines state that additional controls need to be implemented, especially in high-risk areas.

Processes such as multi-factor authentication and mutual authentication are just two examples of additional security measures that can deter future fraudulent activity from occurring in Internet-based banking. Multi-factor authentication refers to the use of more than one factor to verify a user's identity. Passwords and pin numbers can still be used to confirm a user's identity, but with multi-factor authentication, they would be used in conjunction with other types of identity proof, such as a finger print or retinal scan. Mutual authentication allows the user and financial institution to authenticate each other (Baker, 2005).

Modern day threats, like phishing and pharming, are forcing corporate executive officers to continuously reassess the emerging dangers of the Internet and re-evaluate what they are doing to protect the company, employees and customers. Focusing on security needs to be a priority to everyone within an organization. Otherwise, companies are in effect opening their cash registers to hackers and thieves. However, organizations must realize that security is not the real cost. Rather, the real cost is not having the proper security measures in place. The expense associated with the actual fraud, cleanup and potential loss of customers is a cost that can put these institutions out of business (Mitchell, 2005).

Financial losses are not the only cost impacting businesses. The non-financial losses that businesses face can be just as horrific, if not worse. If an institution's systems are infected, the cost and disruption are immense. The Internet has changed the way in which everyone conducts business. Therefore, if customers sense that the Internet cannot be trusted, they will spend less money buying products online, which perhaps, means not buying those particular products at all. Also, if customers feel that their information is not secure, they will discontinue use of the medium altogether.

Businesses also face the consequence of the security issue being publicized, leading customers to believe that the business cannot be trusted. The cost of lost customers is so extreme that it can even cause a business to go bankrupt (Mitchell, 2005).

HOW TO AVOID THESE ATTACKS

Many technology analysts expect that the number of reported cases will continue to increase before falling off. However, there are several ways that a company can protect itself and its customers. Experts declare that technology has the most impact over the short term, but it should be used in conjunction with internal and external security efforts (Britt, 2005). Financial institutions can take several steps to protect themselves from pharming attacks. For example, setting up a digital certificate can differentiate a legitimate Web page from a pharming site (Swann, 2005).

Banks should renew their domain names frequently and investigate any similar domain names to prevent phishing or pharming attacks from occurring. Banks should also have its card processors set parameters to automatically decline authorization if the card verification value (CW) or card verification code (CVC) is missing or does not match. The use of a neutral network that performs antifraud functions based on cardholder use patterns can also be effective. Any suspicious use of the card will alert the network and temporarily block the account or contact the cardholder (Garrett, 2005).

Software vendors, like Symantec, are urging banks to take proactive steps to protect their customers' personal computers. Symantec actually works with several banks that allow customers to check their computers' protection level and even download a Symantec product at a discount, right through the on-line banking site. Browser plug-ins, such as "Netcraft" or "SpoofStick" can also be installed into a user's computer and each product will alert the user of suspected spoof sites (Grebb, 2005). Institutions have started taking steps to protect customers from phishers and pharmers. In 2005, Bank of America initiated SiteKey, a web site authentication service that makes it easier for users to determine whether they are on the real Bank of America site. They have also implemented a personal digital-image system. Customers choose a secret image for logging onto the web site and if the secret image does not appear when he or she logs on, then it is a fake site (Hicks, 2005). Institutions and consumers need to continue taking these steps to prevent phishing and pharming attacks from occurring.

Consumer education is essential in preventing phishing and pharming. Increasing education by financial institutions for these crimes is required. Consumers need education about the differences between legitimate sites and "spoofed" or fraudulent sites (Swann, 2005). For example, Boston Private Bank & Trust recently hired two full-time staff members dedicated to fraud detection and prevention. In addition, the bank formed a committee to coordinate consumer-education efforts. As people begin losing confidence in the Internet, it will deter them from banking on-line. Consequently, it is crucial that banks educate its consumers in order to protect themselves (Grebb, 2005).

According to Beth Robertson, a senior analyst at a research and consulting firm, one of the most important ways to deter the effectiveness of national or local attacks is to educate consumers about these crimes and teach them to protect themselves. For instance, several financial institutions have already informed their customers that they will not ask for personal or account information via e-mail. Any account discrepancies will be handled through traditional mail. As a result, consumers should be wary of any e-mails sent from their financial institutions asking for any personal information. If a consumer does receive an e-mail that seems fraudulent or suspicious, he or she should contact the institution directly (Britt, 2005).

LAWS/ENFORCEMENT

In February 2005, Senator Patrick Leahy introduced the Anti-Phishing Act of 2005. This bill was specifically created to outlaw the practice of phishing and/or pharming. The act adds two new laws to the U.S. Code. The first law prohibits "the creation or procurement of a web site that represents itself to be that of a legitimate business, and that attempts to induce the disclosure of personal information, with the intent to commit a crime of fraud or identity theft." The second law prohibits "the creation or procurement of an e-mail that represents itself to be that of a legitimate business, and that attempts to induce the disclosure of personal information, with the intent to commit a crime of fraud or identity theft." The bill allows for a five-year jail term and a fine of up to $250,000 for anyone convicted of phishing or the related practice of pharming (New Leahy…, 2005).

Phishing may have appeared to be covered by the pre-existing fraud laws, but asking for credit card numbers was, in itself, not illegal. Some phishers and pharmers can be prosecuted under wire fraud or identity theft statutes, but often these prosecutions take place only after someone has been defrauded. Fraudulent e-mails are now sufficient for prosecution, whereas previous laws only allowed phishers to be prosecuted if the crime had taken place and was reported.

There is also the problem of enforceability. Many of these attacks, if they can be traced at all, originate overseas where there is no proper enforcement to give laws any strength. However, there was one notable exception in Brazil last year, where a gang was arrested after allegedly stealing an estimated $37 billion from online bank accounts by recording and transmitting the victims' passwords and login numbers to their own accounts. Still, this was an exception, and not the rule. However, even though law enforcement might not be able to shut down a phishing site due lack of jurisdiction, authorities should still be notified as soon any attacks are identified (Britt, 2005).

CONCLUSIONS

The extent of identity theft by use of phishing and pharming scams is staggering. It is imperative that individuals protect themselves and that businesses protect themselves and their customers. Not only is the immediate monetary cost incredible for breaches of security concerning

private data, but the future costs associated with loss of confidence in the company is immeasurable and potentially dramatic in terms of public relations and dollars.

Phishing and pharming are not merely esoteric fraud schemes that appear in the news and seem mildly interesting. Businesses and individuals can suffer greatly if they are the victims of an attack. The number of phishing and pharming scams has grown tremendously over the past few years. There is a huge potential reward for criminals who succeed in these malicious acts. These crimes will continue to grow unless consumers and financial institutions work together to stop phishing and pharming from occurring.

Creating awareness is one of the most important tools in fighting identity theft via phishing and pharming schemes. However, it is not enough. Financial institutions and consumers need to work together to prevent future occurrences. Multi-factor authentication and mutual authentication should be implemented to provide assurance that the communication between customers and financial institutions is authentic. Also, various other business practices may need to be changed to protect identity data.

No one is perhaps more aware of the pitfalls of identity theft scams than ChoicePoint, the Alpharetta, Ga.-based company fined $15 million by the Federal Trade Commission for the disclosures of information. The company was fooled into selling personal information on 163,000 people to fake companies set up by Nigerian criminals. Other companies have also suffered enormously from not having proper safeguards set up to keep their customer data secure.

The role of company fraud examiners (whether internal employees or consultants) and accountants should be significant. They can use their skills to not only identify schemes already in place in the company's system but also recognize weaknesses in data security and online access and define changes the company should implement.

Some suggestions for changes, which the fraud examiner could also help implement, are: blocking access by foreign address to all company networks, screening customers more thoroughly, encrypting data feeds, and making passwords and user ids more protected. Institutions should also continue to send correspondence through the mail, informing customers about cyber crimes and instructing them not to give out personal information if they are prompted via e-mail. eBay's procedure on email is a prime example of this safeguard in action. The company sends email warnings to customers that indicate they will not contact them via email and ask for private information; they provide a number/email address to check with before doing anything that may turn out to be from a fake/"spoof" email.

Hopefully, with advanced technology and continued educational outreach by businesses, financial institutions and educational organizations, there will be a decline in the amount of identity theft taking place on the Internet. Unfortunately, Internet users (individuals and businesses alike), in order to protect their identities, pay the costs associated with stopping phishing, pharming, and other types of cyber crimes. Higher costs will continue to be incurred, though, if private information is not properly secured.

REFERENCES

A Little Fraud among Friends (2006, April 4). Retrieved July 11, 2006, from http://www.tbrnews.org/Archives/a2316.htm

Baker, D. (2005, December 1). Banks Need to Take FFIEC Mandate to Heart. *Bank Technology News*. Retrieved April 9, 2006 from ProQuest database.

Biersdorfer, J.D. (2005, November 3). As with phishing, shun pharming. *New York Times*. Retrieved January 17, 2006, from ProQuest database.

Britt, P. (2005 June). No Phishing Allowed. *Information Today*. Retrieved March 10, 2006, from ProQuest database.

Buckler, G. (2005, November 10). Do DNS gatekeepers provide safety? *Computing Canada*. Retrieved January 24, 2006, from ABI Inform database.

Cyber crime: Black-hat hacker problems worsen (2005, August 23). *Electronic Payments Week*. Retrieved January 24, 2006, from ABI Inform database.

Friedenberg, M. (2006). The coming pandemic: No, not bird flu. Identity theft. CIO, 19(15), Retrieved May 28, 2006, from ProQuest database.

Garrett, J. (2005, December). Best practices for card fraud prevention. *Credit Union Magazine*. Retrieved March 10, 2006, from ProQuest database.

Gartner survey shows frequent data security lapses and increased cyber attacks damage consumer trust in online commerce (2005, June). Retrieved May 16, 2006, from http://www.gartner.com/press_releases/asset_129754_11.html

Grebb, M. (2005, March 1). Crime: Crooks get behind plow; 'pharming' harvests a new crop of thieves. *Bank Technology News*. Retrieved March 10, 2006, from ProQuest database.

Grazioli, S. and Jarvenpaa, S. (2003, Volume 46, Number 12). Deceived: Under Target Online. *Communications of the ACM*.

Hicks, D. (2005, Fall). Phishing and pharming: Helping consumers avoid Internet fraud. *Communities & Banking*. Retrieved January 24, 2006, from ABI Inform database.

How Many Identity Theft Victims Are There? What IS the Impact on Victims? (2006, February). Retrieved July 10, 2006 http://www.privacyrights.org/ar/idtheftsurveys.htm#FTC

Huntley, H. (2005, November 13). Is your info out there, or are they just guessing? *St. Petersburg Times*. Retrieved January 17, 2006, from ProQuest database.

ID thieves preying on consumers with new phishing scam called pharming (2005). Retrieved January 17, 2006 from www.nclnet.org/news/2005/phishing_10132005.htm

IRS Warns of e-Mail Scam about Tax Refunds (2005, November). Retrieved July 10, 2006, http://www.irs.gov/newsroom/article/0,,id=151065,00.html

Malone, St. (2006, March 31). Phishing sites reach all time high. PC Pro: News. Retrieved April 1, 2006, from http://www.pcpro.co.uk/news/85698/phishing-sites-reach-all-time-high.html.

Mindlin, A. (2005, May 16). E-mail irritants act at different speeds. *New York Times*. Retrieved January 17, 2006, from ProQuest database.

Mitchell, C. (2005, December). Taking Internet security off the backburner. *Chief Executive*. Retrieved March 26, 2006, from ProQuest database.

New Leahy Bill Targets Internet "PHISHING" and "PHARMING" That Steal Billions Of Dollars Annually From Consumers (2005, February). Retrieved June 15, 2006 from http://leahy.senate.gov/press/200503/030105.html

O'Brien, T. L. (2005, December 4). For a new breed of hackers, this time it's personal. *New York Times.* Retrieved January 17, 2006, from ProQuest database.

Palmer, S. (2006, January 10). IRS warns consumers of e-mail scam. *St. Petersburg Times*. Retrieved January 17, 2006, from ProQuest database.

Phishing Activity Trends Report (2005, February). Retrieved June 15, 2006, from http://www.antiphishing.org/reports/APWG_Phishing_Activity_Report_Feb05.pdf

Phishing Activity Trends Report (2006, May). Retrieved June 15, 2006, from http://www.antiphishing.org/reports/apwg_report_May2006.pdf

PSECU Battles Phishing, Pharming and Online Fraud with Cyota's FraudAction Service (2005, June 13). Retrieved June 15, 2006 from http://www.rsasecurity.com/press_release.asp?doc_id=6809&id=1034

Sturgeon, J. (2005, November). Byte out of Crime. *Independent Banker*. Retrieved March 10, 2006, from ProQuest database.

Swann, J. (2005, September). Banks need to protect themselves against pharming, says FDIC. *Community Banker*. Retrieved January 24, 2006, from ABI Inform database.

Targeted Trojan Email Attacks (2005, June 16). Retrieved March 10, 2006 from http://www.niscc.gov.uk/niscc/docs/ttea.pdf

Zeller, T., Jr. (2005a, June 6). You've been scammed again? Maybe the problem isn't your computer. *New York Times*. Retrieved January 17, 2006, from ProQuest database.

Zeller, T., Jr. (2005b, June 21). Black market in credit cards thrives on web. *New York Times*. Retrieved January 17, 2006, from ProQuest database.

Zeller, T., Jr. (2006, April 3). Countless dens of uncatchable thieves. *New York Times*. Retrieved May 4, 2006, from ProQuest database.