Interested in learning more about security?

SANS Institute InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

Phishing and Pharming - The Evil Twins

Phishing and Pharming are two of the most organized crimes of the 21st century requiring very little skill on the part of the fraudster. These result in identity theft and financial fraud when the fraudster tricks the online users into giving their confidential information.

Copyright SANS Institute

Author Retains Full Rights

AD

© SANS Institute 2007, Author retains full rights.

Phishing and Pharming – The Deadly Duo

GIAC *Gold Certification*

Author: Tushar Vishesh Srivastava, tushar.vs@gmail.com

Adviser: Jim Purcell

Accepted: January 29, 2007

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Outline

1. Introduction 4

2. You've Got Mail – The Phish Saga 5

2.1. Evolution of the Phishing Attack 6

2.2. The Drive to Phish 7

2.3. The new Offensive – Personalized Phishing 8

2.4. Anatomy of a Phish Attack 9

2.5. Other Phishing Attacks 14

3. Something Phishy – Opening the Pandora's Box 15

3.1 Enterprise 15

3.2 Customers 16

3.3 Government Authority 16

4. Pharming – Phishing sans the Bait 17

4.1 The Anatomy of a Pharming Attack 18

4.2 Pharming Techniques 19

4.3 The Pharming Impact 21

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

5. Defense against the Dark Acts 22

5.1 Employee/Customer Education and Awareness 22

5.2 Technology 24

5.3 Law Enforcement 27

6. United We Stand 28

7. The Road Ahead 29

8. References 31

9. Footnotes 32

10. Glossary 34

11. List of Figures 35

© SANS Institute 2007, Author retains full rights.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

1. Introduction

Phishing and Pharming are two of the most organized crimes of the 21st century requiring very little skill on the part of the fraudster. These result in identity theft and financial fraud when the fraudster tricks the online users into giving their confidential information like ***Passwords, Social Security Numbers, Credit Card Numbers, CVV Numbers,*** and personal information such as ***birthdates*** and ***mothers' maiden names*** *etc*. This information is then either used by fraudsters for their own needs such as impersonate the victim to transfer funds from the victim's account, purchase merchandise etc., or is sold in a variety of online brokering forums and chat channels for a profit.

The **Anti-Phishing Working Group** (APWG)[1] study indicates that 26,877 phishing attacks were reported in October 2006, a 21 percent increase over September's 22,136 attacks and an increase of 70% as compared to October 2005. Through these attacks the fraudsters **hijacked 176 brands** resulting in huge financial losses and loss of reputation to enterprises. The **Gartner** study reported that more than **2 million Americans** have had their **checking accounts raided** by criminals in 2004, the average **loss per incident** being **$1,200**[2].

With phishers developing evermore sophisticated attacks, these numbers are bound to increase in the near future. Hence, battling these attacks has become a high priority for Governments and Industry Groups.

This paper discusses the ways and means of defending the integrity of online business by foiling such attempts using a three pronged approach:

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

1. **Employee / Customer education and awareness**

2. **Technology**

3. **Law enforcement**

2. You've Got Mail – The Phish Saga

The United States Department of Justice defines phishing as 'Criminals' creation and use of e-mails and websites – designed to look like e-mails and websites of well-known legitimate businesses, financial institutions, and government agencies – in order to deceive Internet users into disclosing their bank and financial account information or other personal data such as usernames and passwords'[3].

Phishing is both a **social engineering** and **technical deception** type of attack. Social-engineering attacks use 'counterfeit' e-mails to lead users to fake websites designed to trick them into divulging their personal information. In addition, technical subterfuge schemes plant **malicious software (malware)** e.g. virus, trojans etc. onto users' computers to steal their credentials. This is usually done by monitoring and intercepting consumers' keystrokes or grabbing screens to steal off their personal details.

Social engineering attacks are the most common method to conduct phishing with e-mails being the most used technique. The figure below depicts the number of unique phishing e-mail reports submitted to APWG in October 2006.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

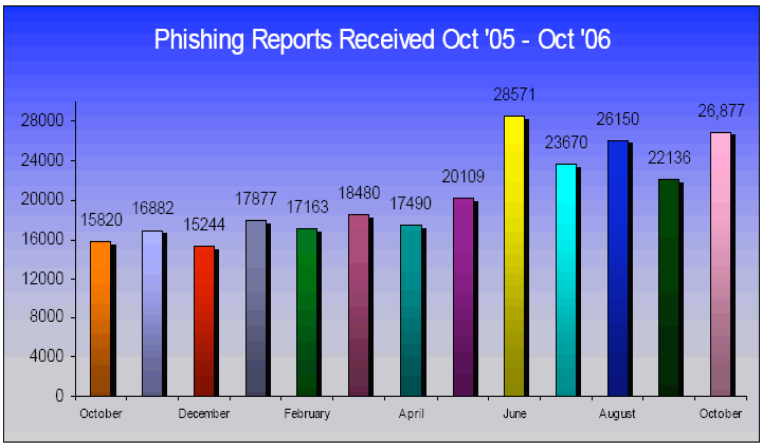

Figure 1: Phishing Reports Received Oct '05 – Oct '06

2.1. Evolution of the Phishing Attack

The term "phishing" originated in AOL account theft using instant messaging[4]. However, nowadays e-mails are used by phishers as the most common attack vector. Moreover, what started as poorly written e-mails sent to the users, with bad sentence structure and spelling error, phishing has evolved into something much more difficult to identify, even to a discerning user.

The e-mails are now better written and more convincing with few or no spelling mistakes, incorporating the required logos and graphics. The deceptive websites are **identical** in their **'look and feel'** to that of the real organization's, making differentiation impossible.

All of this 'originality' has resulted in a phenomenal increase in the number of new phishing sites over the past year. Moreover, the ease of carrying out phishing is making it one of the most organized online crimes. The figure below depicts this phenomenal increase.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

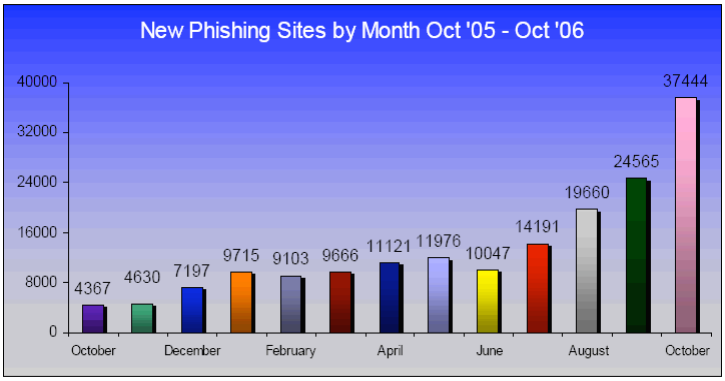

Figure 2: New Phishing Sites by Month Oct '05 – Oct '06

2.2. The Drive to Phish

The motive behind the phishing attack is usually financial. Even if a small percentage of the users, who received the spoofed mail, divulge their confidential details such as logon credentials, passwords etc. the attack is a huge success. These credentials can then be used by phishers for personal gain or sold online for a huge profit.

It is due to the simplicity of these attacks and resultant monetary gains that the Banking and Financial Services sector find themselves bearing the brunt of these attacks i.e. 93% of attacks.

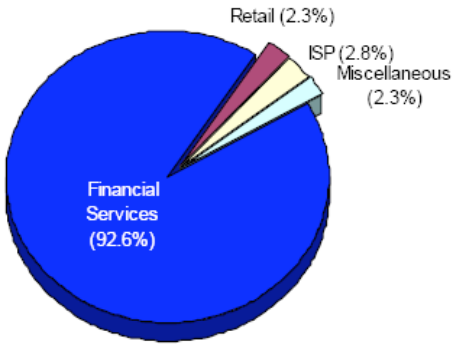

Figure 3: Most Targeted Industry Sectors – APWG study

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

2.3. The new Offensive – Personalized Phishing

Contrary to a typical phishing attack, where fraudsters send out thousands of e-mails to arbitrary e-mail addresses, in personalized phishing phishers usually pick a business that the potential victim actually does business with, such as a bank or a financial institution, or a credit card company. The phishers then tell the e-mail recipients that they need to "update" or "validate" their credit card details or the billing information in order to keep their accounts active. To set the bait and make things look authentic, they direct their potential victims to a web site that mimics the look and feel of the target organizations' legitimate web site – with same graphics, color combinations etc. The unsuspecting users submit their personal information to the fraudster and the crime is conveniently committed.

In addition to the creation of fake websites, the phishers also utilize the latest techniques such as Spyware, Key loggers, Mouse loggers, and Screen grabbers in an attempt to steal a user's credentials. For these techniques to result in a success, malicious software (malware) needs to be executed on the victim's machine. This malware is delivered to them using the commonly used communication channels such as:-

- Internet Messenger (Yahoo, MSN, ICQ etc.)
- E-mail based worms/virus

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

2.4. Anatomy of a Phish Attack

The anatomy of the phishing attack is as follows:

Stage 1 – Initiation

This includes the Phisher preparing for the attack in order to steal the personal information of the Internet users. This can be accomplished by the following:

- The Phisher can register a similar sounding or cousin domain which is extremely similar to the legitimate domain name. For example the phisher can register and control a domain name called www.xyzbank-verysecure.com instead of www.xyzbank.com.

- The Phishers may also create websites offering counterfeit products at a discounted rate wherein the user may be asked to input his user credentials, other confidential details or do an amount transfer using credit card. These fraudsters can also get their sites indexed by commonly used search engines such as Google, Yahoo. MSN etc. to dupe a wider audience.

  Sites could also be created with fake address and status bar resembling the actual sites which ask for confidential and sensitive information from the user.

- The phisher can also establish servers using either his machine or a 'Zombie'[5]. Zombie's are computers attached to a network that have had their security compromised by hacking or malware and are remotely controlled by a fraudster for

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

another purpose. This purpose may be to use it as a launch pad for another attack, or for the distribution of SPAM. Usually zombies are used to send malicious mails to millions of internet users or for hosting spoofed web sites (resembling the real website).

The phishing server is then configured to obtain personal information entered by the users either through web based interfaces or by malwares installed on user's systems which transmit such information to the server.

Stage II – Execution

In this stage the phisher tries to lure the victim to accept the bait he/she sends through different attack vectors. The vectors are as follows:

- The most common and popular technique to commit phishing is through malicious e-mails. The 'phisher' sends an email to thousands of online users asking them to re-enter or update their personal details as their "Account is about to expire" or "Multiple log-ins have been detected" etc. He does this to lure the victims in clicking a particular link provided in the e-mail and disclose their personal information.

- In other cases, a phisher can entice the internet users using social engineering techniques, a non-technical kind of intrusion that relies heavily on human interaction and often involves tricking other people to break normal security procedures[6], to open an e-mail attachment, download a file on a system etc. These attachments when downloaded can exploit

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

the security vulnerabilities of the system and can install malwares on it.

Some of the commonly used malwares used by phishers are Key Loggers and Screen Grabbers. Key loggers are programs designed to record which keys are pressed on a computer keyboard most commonly used to record passwords for later use by another person. Screen grabbers, on the other hand, monitors and captures all user data inputs on the screen and sends it to the phishing server.

Another kind of a malware based attack is the Web Trojan attack which uses pop up windows over the login screens of the organization's websites to collect user credentials. The user will think that he's transmitting information of the organization's webpage where in reality the confidential information entered by him is transmitted to the phishing server.

- Other ways of Phishing could include methods like Man in the Middle attacks wherein the Phisher sits between the user's machine and the legitimate site, silently observes the communication between them and collect the data that is transmitted for his own usage. This attack is difficult to detect as the phisher is sitting as a proxy between the user and the website and the communication is totally legitimate.

- In another popular technique of phishing, the phisher uses the organization's own web scripts or webpage against the user. This attack, known as cross-site scripting, is very difficult to identify by the unaware user as everything from

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

the web address to the security certificates of the organization seems correct.

In this attack the user is brought to a Web page running on the victim's site (e.g. www.xyzbank.com), but it includes elements from the attacker site which can be malicious in nature. The phisher could therefore use this security vulnerability of improper input filtering by the developers of the web pages to convince a user to provide personal information. This content is then redirected to a phishing server.

Stage III – User Action

This includes any action from the user which makes him vulnerable towards the loss of his user credentials, account balance and his other sensitive information. This action could be any one of the following:

- The user clicking on a link sent to him by the phisher in a deceptive e-mail.
- The user goes to a counterfeit website with a fake address and status bar and enters his personal information on the site without taking any precautionary measures.
- In other attacks like Host file modification, DNS cache poisoning, Malware usage, Domain Hijacking and Static Domain Name spoofing (discussed in the Pharming section), the user tries to go to a legitimate site but is redirected to a fake

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

website wherein he/she is asked to enter his personal details.

Stage IV – Completion

The scam is completed when the 'phisher' receives the personal information entered by the user either through a Key Logger/Screen Grabber/Web Trojan attack, the DNS spoofing attacks (discussed later), Man in the middle/ Proxy attack or the Cross-Site Scripting attack.

The phisher, after receiving this information, can then use these details for money transfer, committing identity fraud or selling it online, for a profit.

Typical Phishing Attack

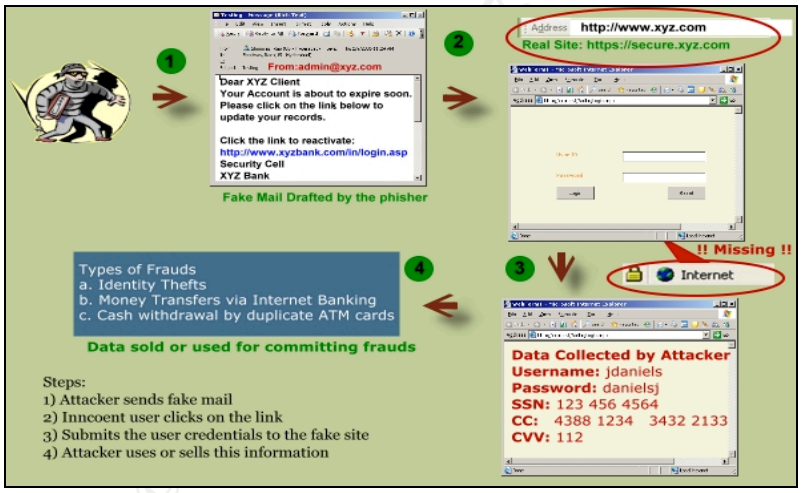

Figure 4: Typical Phishing Attack

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

1. The phisher uses any kind of attacks mentioned above or a combination of them to launch an attack against the victim. Common technique is the use of fraudulent e-mails sent to online users.

2. Attack is perpetrated with an email which contains an embedded link, which most often in case of a phishing attacks takes the user to a spoofed site.

3. If the customer falls for the 'bait', by clicking on the link, and submits his/her personal data or other sensitive information on the spoofed site, these details are recorded and sent to the 'phisher'.

4. The scam is completed when the 'phisher' either personally uses these details for money transfer or sells it online, for a profit.

2.5. Other Phishing Attacks

In other kinds of Phishing attacks, a flaw in the URLs have been found while handling the Internationalized Domain Names (IDN) in web browsers. This flaw known as IDN spoofing or a homograph attack can allow visually identical web addresses to lead to fake, possibly malicious, websites.

The point to ponder here is that not all phishing attacks require a fake website or the technique of IDN spoofing / homograph attack. Incident has been reported wherein messages that claimed to be from a bank told users to dial a phone number regarding a problem with their bank account. Once the phone number was dialed, prompts told users to enter their account numbers and PIN. The number was

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

provided by a Voice over IP provider.

In addition to the above, SMiShing is another emerging threat vector wherein some cell phone users have started receiving SMS messages that call them to visit various web sites that have fake confirmation about signing to various online services. This is version of phishing by SMS and yet another indicator that cell phones and mobile devices are becoming increasingly used by perpetrators of malware, viruses and scams.

3. Something Phishy – Opening the Pandora's Box

The impacts of the phishing attacks have been huge. Losses can be viewed from three angles:

1. Enterprise
2. Customer
3. Government Authority

3.1 Enterprise

According to Gartner, between May 2004 and May 2005, **2.42 million** US citizens have taken the phishing bait; losses amounting to **$929 million** for Enterprises[7]. In another survey it was found that U.S. businesses lose an estimated **$2 billion USD**[8] a year as their clients become victims. In the United Kingdom losses from web banking fraud – mostly from phishing – almost doubled to **£23.2m in 2005,** from **£12.2m in 2004,** while **1 in 20** users claimed to have lost out to phishing in 2005[9]. In addition, the APACS study of 2006 found that

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

U.K losses from phishing, which were approximately **$27.7 million** in the first half of 2005, rose to almost **$43 million** in the first half of 2006[10].

Other than the huge financial losses, the enterprises are also facing **loss of reputation** and **brand image**, and losses due to reimbursement of the fraudulent transactions to maintain **customer loyalty.** All the losses amount to increased capital charge on the organization for conducting its business.

Per law, once the victim reports the loss or theft of a credit card he/she has no further responsibility for the unauthorized charges on his/her card. The maximum liability under federal law is $50[11] per card. This makes the Enterprise bear the rest of the losses, which in some cases could be huge.

3.2 Customers

Customers, on the other hand, are losing trust in conducting their financial transactions online. According to Gartner, the annual e-commerce growth could be reduced by 10% if adequate phishing defenses are not implemented.

3.3 Government Authority

In December 2005, a security glitch enabled phishers to usurp government sites. The phishers disguised themselves as Internal Revenue Service agents (IRS) agents and mislead users into revealing their sensitive information. This showed that the phishers are now implementing the attacks against government authorities' too[12].

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

What makes the situation worse is the fact that the authorities are almost helpless in combating these attacks. The average time window between being alerted and the phisher moving from one server to another is 4.5 days[13]. This makes phishing an online 'hit and run attack' wherein the phisher hides his/her identity so that he/she cannot be found.

Sadly, industry experts on phishing like APWG believe that the increase in phishing incidents are just the beginning and the worst is yet to come. APWG has based their findings on the fact that most incidents are not reported due to the:

- Users being unaware of the fact that they are being phished
- Enterprises feeling that it would lose its reputation if they report an incident.

4. Pharming – Phishing sans the Bait

The worst arrives! Pharming is the evil cousin of phishing which doesn't rely on sending e-mails to thousands of online users in order to trap them. What makes pharming dangerous is that the attack is unrecognizable to even an alert user. Pharming leverages malicious code such as viruses, worms, trojans and spyware to carry out sophisticated attacks such as hosts file modification, DNS cache poisoning etc. Pharmers can even hijack domains or spoof static domain names in order to fool users by redirecting them to malicious websites.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

4.1 The Anatomy of a Pharming Attack

The most common method of Pharming attacks is described below:

1. The user types in the address of their bank (e.g. www.xyzbank.com) into the address bar of their browser.

2. The request passes to a DNS name server. This server maps www.xyzbank.com to a number say 210.10.10.3 (IP address) which is understandable to the computers.

3. In a normal scenario, the browser will connect the user to the authentication site of xyzbank. However, in pharming, the attacker modifies the mapping in the DNS service. Now DNS service maps www.xyzbank.com to 230.10.10.3 – the IP address of attacker's fake site.

4. For example: the customer thinks that they are interacting with http://www.xyzbank.com, because it so indicates this in the browser's address bar, but actually they are connected to the deceptive site of the attacker.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Pharming – Anatomy of the Attack

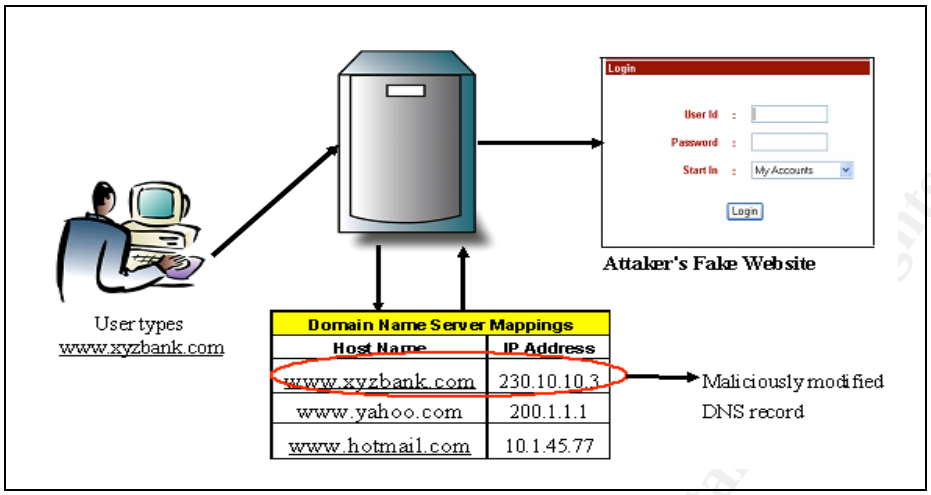

Figure 5: Anatomy of the Pharming Attack

4.2 Pharming Techniques

Pharming, as mentioned earlier, relies on changing the DNS entries of the organization's website. There are multiple ways to accomplish this. These are:

- ***Hosts file modification***

Most OS store files locally which consist of a mapping between the domain name and the corresponding IP address e.g. www.xyzbank.com maps to say 210.10.10.3

Phishers can benefit from this OS vulnerability by modifying these host lookup files with malicious mapping e.g. they can map www.xyzbank.com to say 230.10.10.3 which is actually the IP address of the malicious website.

- ***DNS cache poisoning***

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

DNS servers, for a limited amount of time, cache the queries made by the users. Caching is done to speed up the user response times for frequently used domains in order to enhance the user experience. Phishers can poison the DNS cache itself, which contains the alias to IP address mapping, by inserting malicious content to lead users to fake where they are asked to update their personal information, such as passwords and credit cards, social security and bank account numbers.

- ***Usage of Malwares***

Usage of malwares have become very common with pharmers deploying Viruses and Trojans on the user's system which intercept user requests to visit a particular site or webpage, such as **xyzbank.com**, and redirects him/her to the site the pharmer has set up.

- ***Domain Hijacking***

The pharmer may hijack or steal an organization's website, by techniques like Domain Slamming and Domain Expiration, which allow them to redirect all legitimate Internet traffic to an illegitimate site.

In Domain slamming a pharmer can submit domain transfer requests and switch a domain from one registrar to another. The account holder at the new registrar can then alter routing instructions to point to a different, illegitimate server.

In Domain expiration the domain names are leased for fixed periods and failure to manage the leasing process properly could

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

result in a legitimate ownership transfer possibly to a pharmer.

- ***Static domain name spoofing***

The pharmer may attempt to take advantage of slight misspellings in domain names to trick users into accidentally visiting the malicious website e.g. a pharmer may redirect a user to **xyzbnk.com** instead of **xyzbank.com**, the site the user actually wanted to access.

4.3 The Pharming Impact

In March 2005 SANS Institute reported a DNS poisoning incident where the users were directed to several fake web servers which tried to install malware onto the user's machines.

Another pharming incident which happened during the last quarter of 2004 was due to a worm named Troj/Banker-AJ[14]. The worm looked for users visiting certain bank sites such as Abbey, Barclays, Egg, HSBC, Lloyds TSB, Nationwide, and NatWest etc and redirected them to phishing sites. The Trojan monitored the user's internet transactions in an attempt to steal passwords and other data related to online banking and other financial transactions.

The fact that the reported incidents of pharming have been few does not mean that this threat is not important. The incidents of hacking, online fraud, and identity theft are increasing in number everyday. Furthermore, with increasing technical sophistication the chances are high that these attacks will only get worse.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

5. Defense against the Dark Acts

To prevent e-commerce firms from loosing its charm, due to the phishing and pharming attacks, a three pronged approach can be adopted:

1. Employee/Customer Education and Awareness
2. Technology
3. Law Enforcement

5.1 Employee/Customer Education and Awareness

Prevention is always better than recovery. Hence, the success of a phishing attack may be reduced by enabling employees and customers to recognize the attempted fraud. This can be achieved by increasing the awareness of the users to do the following:

- Check the grammar, content and quality of the graphics in the e-mail
- Verify whether the "https" word, is present at the beginning of the URL
- Double click on the yellow lock icon at the bottom of the pages served using "https" to see the certificate details and verifying the same
- Call the organization's help desk whenever in doubt of the authenticity of the e-mail or website

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

- Read the online privacy statement of the organization carefully

- Review credit card and account statements as soon as it is received to determine whether there are unauthorized charges.

- If the statement is late by more than a couple of days, call the Credit Card Company or financial institution to confirm the billing address and account balances.

- Report suspicious activity to the FTC – send the actual spam e-mail to uce@ftc.gov or file complaint at www.ftc.gov, and then visit the FTC's identity theft web site at www.ftc.gov/idtheft to learn how to minimize the risk of damage from identity theft.

It is now imperative for the banks and other organizations to train their users on the following to make them aware about these attacks:

- Identification of genuine emails and web sites

- Appropriate usage of Instant Messenger (IM), and Peer to Peer (P2P) software.

In addition to this, guidelines should be issued to the customers to inform them about the way the organizations would communicate to them. These Guidelines should include that the:-

- Customers would never be asked to provide their username, password, credit card number, full name, bank account number etc by e-mail.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

- E-mails sent by the organization would not contain any embedded links or ask the users to fill personal information online.

- Users should be suspicious and not act upon any e-mail/ pop up messages with urgent requests for personal information. For further confirmation, they could contact the help desk.

5.2 Technology

Technology can always complement education but it will never be a substitute. Implementing the following solutions at the enterprise and customer level will serve as preventive controls against such attacks:

Enterprise Level

Proactive Measures

o Adopt Standards that could help promote trust, e.g. sender e-mail authentication.

o Implement URL blocking, filtering rules either on the host or gateway.

o Implement stronger authentication, such as two factor authentication (hardware tokens or client certificates) or mutual authentication between client and server.

o Prevent cross-site scripting vulnerabilities in the website by implementing central input data validation for malicious characters

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

- Have an agreement with the Internet service providers to quickly shut down malicious websites

- Implement active site monitoring using Inbound and outbound filters

- Deploy logging software to look for particular events such as spikes in DNS traffic or spikes in e-mail traffic from a single user

- Apply system and software patches and upgrades on a timely basis. Place controls on DNS servers, such as host-based intrusion detection systems, to prevent pharming attacks

- Follow developments such as the progress of the DNSSEC Standards, and ensure that the organization's ISPs have the proper controls on their DNS directories and servers

- Use downloadable tools for web browsers that rate websites based on Secure Sockets Layer (SSL) technology, an internet protocol for sharing sensitive information. Most software options check against an updated database of blacklisted phishing sites and IPs.

- Use security features like SiteKey as implemented by Bank of America. This feature uses personal digital images and allows the user to choose an image he would like to appear on the login page whenever he logs on. If the secret image does not appear, it means that he has logged on to the wrong place.

Reactive Measures

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

o Make incident response teams aware of the phishing and pharming threat and educate them regarding handling these types of attacks

Customer Level

- Two Stage Passwords – one password during entering 'Login' credentials and other password during the 'Transaction'

- Implementing Multi-factor Authentication Mechanism – Something the user knows (Account PIN / Password) and something the user has (Security Token/Digital Certificate/Smart Card)

- Email Authentication with Sender Validation - Using S/MIME digital signatures, PGP etc.

- Pop-up blocker – to help stop automatic execution of malicious code

- Verifying digital card number – A process wherein the user is asked the 4th, 7th, 15th digit etc. on their debit card

- Anti-Virus and Anti-Spyware Software / Desktop Firewalls – prevent attacks by malicious agents

- Browser Security - Install security toolbar inside web browsers to help mitigate phishing and pharming attacks by reporting security information about visited websites.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

5.3 Law Enforcement

Various federal and state laws in the United States address phishing attacks which state that whoever[15]

- creates a website or domain name that seems like a legitimate online business, without the authority or approval of the owner of the real website or domain name of the legitimate online business

- uses it to ask, induce, request, or solicit any person to transmit, submit, or provide any means of identification to another

- falsely represents itself as being a legitimate online business

- includes an Internet information location tool that refers or links users to an online location that pretends to belong to or be associated with a legitimate online business

- induces, requests, asks, or solicits a recipient of the electronic mail message directly or indirectly to provide, submit, or relate any means of identification to another

Shall be fined or imprisoned up to five years, or both.

In addition, rulings have already been established on identity theft, wire fraud, mail fraud, computer fraud and abuse such as the July 2004 Identify Theft Penalty Enhancement Act, Identity Theft and Assumption Deterrence Act of 1998, Fair and Accurate Credit Transactions Act of 2003, USA PATRIOT Act, Anti-Phishing Act of 2004 and Gramm-Leach Bliley Act – all of which contain provisions related

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

to identity theft and/or fraud.

Regulations are also becoming stricter as evidenced with the **Identity Theft Penalty Enhancement Act of 2004**, which includes a two-year prison sentence for the convicted fraudster, and the **Anti-Phishing Act of 2004**, which not just takes action against successful attacks – it criminalizes the bait itself (the e-mail sent or exploiting Web server or DNS vulnerabilities). The Anti-Phishing Act includes five-years in prison and up to $250,000 in fines for each scam.

6. United We Stand

Even with legislation in place, phishing incidents are on a rise and the phishers are roaming scot-free. Phishers and pharmers usually pack up and leave before the victim can discover the scam, making it difficult for authorities to prosecute.

There is a strong need for Government authorities, financial institutions, Internet Service Providers (ISP), and technology vendors to form working groups to share information and techniques to address this problem. Some industry associations mentioned below focus on the ways and means to prevent the phishing, spoofing and identity theft scams.

- ***Anti-Phishing Working Group*** – APWG (www.antiphishing.org)
- ***Digital PhishNet*** (www.digitalphishnet.org)
- ***Financial Services Technology Consortium*** – FSTC (www.fstc.org)

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

- ***Trusted Electronic Communications Forum*** – TECF (www.tecf.org)
- ***National Cyber-Forensics & Training Alliance*** (www.ncfta.net)

7. The Road Ahead

The revenue model for many companies such as Amazon, eBay and Yahoo and other financial institutions etc. is solely based on the transactions performed online. Phishing and pharming attacks are real and are damaging the relationship between the company and their customers. These damages could be large financial losses to the company/customers or diminished reputation with their customers.

Time has come for the organizations to take this threat head on and raise the bar to effectively implement security and privacy of data. This may not make the company 100% secure but it will help their customers trust the Internet and thus preventing the e-commerce wave from receding.

A good defense will need to include three key elements – Education, Technology and Law Enforcement. Education provides a solid defensive foundation and should include educating management and end users as well as communication mechanisms between IT and the business.

The use of emerging detection tools and technology solutions add an additional layer of defense. Software solutions such as Spoofguard / Fraudeliminator which, when plugged in to the user's browser warn them that they are surfing a spoofed site.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Finally, law enforcement provides the third key element of the defense. Companies will need to continue working in the industry groups / forums to provide current information and bring about a sense of urgency in the proper regulatory bodies.

© SANS Institute 2007, Author retains full rights.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

8. References

1. Emigh, Aaron: Online Identity Theft: Phishing Technology, Chokepoints and Countermeasures, October 3, 2005

   www.anti**phishing**.org/**Phishing**-dhs-report.pdf

2. Stevenson, Robert Louis B.: Plugging the "Phishing" Hole: Legislation versus Technology, Duke Law & Technology Review (2005)

3. Cybercrime: Piercing the darkness, Purging Cybercrime – Laws against Phishing

   http://library.thinkquest.org/04oct/00460/law.html

4. Anti-Phishing Working Group (APWG). Phishing Activity Trends Report. Combined Report for September and October, 2006

   http://www.antiphishing.org/reports/apwg_report_september_october_2006.pdf

5. Ollmann, Gunter: The Pharming Guide, Understanding and Preventing DNS-related Attacks by Phishers, July 2005

6. AT&T Knowledge Ventures, Fighting the Phishers: Suggested Countermeasures for the Phishing Phenomena, 19 Oct, 2006

7. Green, Theodore: Phishing – Past, Present and Future. Greenview Data, Inc. (2005)

8. Chaudhary, Nilesh: Pharming on the Net, March 2006

   http://palisade.plynt.com/issues/2006Mar/pharming/

9. Phishing From Wikipedia, the free encyclopedia

   http://en.wikipedia.org/wiki/Phishing

10. Verghese, Jose: Anti-Phishing Techniques - Protection

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Measures, August 2006

http://palisade.plynt.com/issues/2006Aug/phishing-protection/

11. Wilson, Tim: Phishing Continues Meteoric Rise, November 10, 2006

http://www.darkreading.com/document.asp?doc_id=110384

12. Litan, Avivah: "Increased Phishing and Online Attacks Cause Dip in Consumer Confidence," 22 June 2005, © 2005 by Gartner, Inc.

9. Footnotes

1. Anti-Phishing Working Group (APWG). Phishing Activity Trends Report. Combined Report for September and October, 2006, p. 2 (2006) http://www.antiphishing.org/reports/apwg_report_september_october_2006.pdf
2. Sullivan, Bob: Survey - 2 million bank accounts robbed. Criminals taking advantage of online banking, Gartner says. 14 June, 2004 http://www.msnbc.msn.com/id/5184077/
3. United States Dept. of Justice, Special Report on "Phishing" p.1 (2004) http://www.usdoj.gov/criminal/fraud/Phishing.pdf
4. Emigh, Aaron: Online Identity Theft: Phishing Technology, Chokepoints and Countermeasures, October 3, 2005

   www.anti**phishing**.org/**Phishing**-dhs-report.pdf

5. Glossary, Scrutiny of Acts and Regulations Committee Victorian

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Electronic Democracy, Final Report, May 2005
www.parliament.vic.gov.au/sarc/E-Democracy/Final_Report/Glossary.htm

6. What is social Engineering? - a definition from Whatis.com
http://searchsecurity.techtarget.com/sDefinition/0,,sid14_gci531120,00.html
7. Musgove, Mike: 'Phishing' Keeps Luring Victims. October 22, 2005; Page D01
http://www.washingtonpost.com/wp-dyn/content/article/2005/10/21/AR2005102102113.html
8. Kerstein, Paul: How Can We Stop Phishing and Pharming Scams?" July 19, 2005.
http://www.csoonline.com/talkback/071905.html
9. UK phishing fraud losses double, Finextra, March 07, 2006.
http://www.finextra.com/fullstory.asp?id=15013
10. Phishing Continues Meteoric Rise, Mondomedesuah, November 23, 2006
http://mondomedeusah.typepad.com/mondomedeusah/2006/11/index.html
11. Credit, ATM and Debit Cards: What to do if They're Lost or Stolen, Federal Trade Commission for the Consumer
http://www.ftc.gov/bcp/conline/pubs/credit/atmcard.htm
12. McMillan, Robert: Phishers Pose as IRS Agents, IDG News Service, Dec 1, 2005
http://www.pcworld.com/article/id,123765-page,1/article.html
13. Anti-Phishing Working Group (APWG). Phishing Activity Trends Report. Combined Report for September and October, 2006, p. (2006)
http://www.antiphishing.org/reports/apwg_report_september_october_2006.pdf

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

14. Troj/Banker-AJ, Spyware Trojan, Sophos
http://www.sophos.com/virusinfo/analyses/trojbankeraj.html
15. Cybercrime: Piercing the Darkness, Laws against Phishing
http://library.thinkquest.org/04oct/00460/law.html

10. Glossary

Malware: Software designed to infiltrate or damage a computer system and includes computer viruses, Trojan horses, and spyware.

Spyware: Software that performs certain tasks on the computer like collecting a user's personal information.

Keylogger: A Keylogger observes and records all keys pressed on the computer – in particular, when they enter their authentication information.

Mouselogger: A Mouselogger collects information on mouse use statistics.

Screen grabbing: Software designed to take a screen shot of data displayed on the screen.

Trojans: A malicious program that masquerades as a benign application.

Virus: A computer program with the ability to modify other programs usually to harm the computer system.

IM: An Instant Messenger is a client which allows instant communication between two or more people through a network such as the Internet.

P2P: Peer to Peer is an application that runs on a personal computer and shares files with other users across the network.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Worm: A program or algorithm that replicates itself over a computer network and usually performs malicious actions.

Padlock: Usually a yellow lock icon at the bottom of a page served over secured channel. Double clicking on the icon shows the SSL certificate.

11. List of Figures

Figure 1: Phishing Reports Received Oct '05 – Oct '06

Figure 2: New Phishing Sites by Month Oct '05 – Oct '06

Figure 3: Most Targeted Industry Sectors – APWG study

Figure 4: Typical Phishing Attack

Figure 5: Anatomy of the Pharming Attack

© SANS Institute 2007, Author retains full rights.

© SANS Institute 2007, As part of the Information Security Reading Room Author retains full rights.

Last Updated: September 4th, 2015

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Crystal City 2015	Crystal City, VAUS	Sep 08, 2015 - Sep 13, 2015	Live Event
SANS Network Security 2015	Las Vegas, NVUS	Sep 12, 2015 - Sep 21, 2015	Live Event
SANS Seoul 2015	Seoul, KR	Sep 14, 2015 - Sep 19, 2015	Live Event
SANS Tallinn 2015	Tallinn, EE	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Baltimore 2015	Baltimore, MDUS	Sep 21, 2015 - Sep 26, 2015	Live Event
Data Breach Investigation Summit & Training	Dallas, TXUS	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS Perth 2015	Perth, AU	Sep 21, 2015 - Sep 26, 2015	Live Event
SANS ICS Amsterdam 2015	Amsterdam, NL	Sep 22, 2015 - Sep 28, 2015	Live Event
SANS Bangalore 2015	Bangalore, IN	Sep 28, 2015 - Oct 17, 2015	Live Event
SANS Seattle 2015	Seattle, WAUS	Oct 05, 2015 - Oct 10, 2015	Live Event
SANS DFIR Prague 2015	Prague, CZ	Oct 05, 2015 - Oct 17, 2015	Live Event
SOS: SANS October Singapore 2015	Singapore, SG	Oct 12, 2015 - Oct 24, 2015	Live Event
SANS Tysons Corner 2015	Tysons Corner, VAUS	Oct 12, 2015 - Oct 17, 2015	Live Event
SANS Gulf Region 2015	Dubai, AE	Oct 17, 2015 - Oct 29, 2015	Live Event
SANS Tokyo Autumn 2015	Tokyo, JP	Oct 19, 2015 - Oct 31, 2015	Live Event
SANS Cyber Defense San Diego 2015	San Diego, CAUS	Oct 19, 2015 - Oct 24, 2015	Live Event
SANS Sydney 2015	Sydney, AU	Nov 09, 2015 - Nov 21, 2015	Live Event
SANS South Florida 2015	Fort Lauderdale, FLUS	Nov 09, 2015 - Nov 14, 2015	Live Event
SANS London 2015	London, GB	Nov 14, 2015 - Nov 23, 2015	Live Event
Pen Test Hackfest Summit & Training	Alexandria, VAUS	Nov 16, 2015 - Nov 23, 2015	Live Event
SANS Hyderabad 2015	Hyderabad, IN	Nov 24, 2015 - Dec 04, 2015	Live Event
SANS Cape Town 2015	Cape Town, ZA	Nov 30, 2015 - Dec 05, 2015	Live Event
SANS San Francisco 2015	San Francisco, CAUS	Nov 30, 2015 - Dec 05, 2015	Live Event
Security Leadership Summit & Training	Dallas, TXUS	Dec 03, 2015 - Dec 10, 2015	Live Event
SANS Milan 2015	OnlineIT	Sep 07, 2015 - Sep 12, 2015	Live Event
SANS OnDemand	Books & MP3s OnlyUS	Anytime	Self Paced