GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

Phishing for Banks

A Timely Analysis on Identity Theft & Fraud in the Financial Sector

GIAC Security Essentials
Certification (GSEC)
Practical Assignment
Version 1.4c

Option 1 - Research on Topics
in Information Security

Submitted by: Tony UcedaVelez
Location: Atlanta, GA
Date: December 7, 2004

© SANS Institute 2000 - 2005

© SANS Institute 2000 - 2005 Author retains full rights.

Table of Contents

Abstract/Summary 1
Introduction – Defining Phishing 2
Section One 3
Section Two 5
Section Three 11
Conclusion 20
References 1

List of Figures

Figure 1 4
Figure 2 5
Figure 3 9
Figure 4 14

© SANS Institute 2000 - 2005, Author retains full rights.

Abstract/Summary

This paper focuses on addressing one of the largest threats currently plaguing the financial industry - Phishing. The research provided herein attempts to define this ever-changing phenomenon and explores the past, present, and future components that have consisted of this form of identity theft.

Phishing is the act of deception via the Internet communication channels for the sole purpose of extracting confidential information that leads to some undeterminable financial gain. Although the primary vehicles used in such attacks are mail and web related, other methods have been known to conduct phishing attempts and should not be overlooked.

This advance form of identity theft and financial fraud is a serious and credible threat to online financial services. As those services are projected to grow, it is vital for financial organizations to take a serious look into providing a high level of assurance to their online consumers. Failing to do so will minimize growth and discredit online banking services as a reliable and extended arm of banking services.

Phishing attacks are evolving rapidly. They employ no standard tool or technology as a trademark and transcend many forms of Internet use. For this reason, it is imperative for both end-users and suppliers of Internet services to be aware of up to date and future tactics employed by phishing artists. In order to provide a timely and effective response to this threat, members of the financial sector, as well as their clients, must be aware of the latest trends pertaining to this ongoing menace.

This dissertation identifies current and future trends pertaining to this form of social engineering via the Internet. On the offensive end, a look at some of the current techniques, tools, and processes utilized by these modern day criminals will be examined. On the defensive end, we'll examine some common security shortcomings committed by both users and financial institutions. Lastly, a recommendation will be made on how to implement and maintain security procedures that defend banks/ credit unions and their respective clients from phishing baits.

© SANS Institute 2000 - 2005, Author retains full rights.

© SANS Institute 2000 - 2005 Author retains full rights.

Introduction – Defining Phishing

In the world of banking and Internet security, phishing is simply a form of modern day social engineering that employs both technical and non-technical methods for the purpose of extracting personal, confidential information. As you can tell, this definition is both broad and vague. It offers no specifics as to the type of tactics or tools employed by this attack. However, as vast as this definition may be, the sole purpose of phishing, regardless of the channel in which it travels nor the exploit it attacks, remains the same: to obtain confidential information for the purpose of monetary gain by the attacker. Confidential information in this case revolves around bank information such as account number, login id, password, and/or any information needed to assume control of a bank account.

In order to better understand phishing's definition, we look to the definition of different establishments in order to compare commonalities and distinguishing terms.

The Federal Deposit Insurance Corporation (FDIC) plays a vital role in sustaining the confidence in the U.S financial system. Part of its responsibility is to mitigate risks existent in the current financial environment, specifically pertaining to deposited funds. Phishing would constitute a risk to those funds and the FDIC, addressing this threat on its website, has provided the following definition:

> The term "phishing" – as in fishing for confidential information - refers to a scam that encompasses fraudulently obtaining and using an individual's personal or financial information.[1]

As you can see, the FDIC also provides some ambiguity by using the word 'scams' to potentially encompass many methods in obtaining private information from an individual.

An alternate definition from the United States Computer Emergency Readiness Team (US-CERT), defines phishing in a two-step process. First it defines social engineering and then it defines phishing to be simply 'a form of social engineering'. It thereafter specifies e-mails and web sites as the source of these types of attacks.[2]

Overall, most would define phishing to be a combination of both of the aforementioned examples. Such a definition would most likely resemble one currently provided by webopedia:

> (fish´ing) **(n.)** The act of sending an e-mail to a user falsely claiming to be

[1] http://www.fdic.gov/consumers/consumer/alerts/index.html
[2] http://www.us-cert.gov/cas/tips/ST04-014.html

© SANS Institute 2000 - 2005

Author retains full rights.

> an established legitimate enterprise in an attempt to scam the user into surrendering private information that will be used for identity theft. The e-mail directs the user to visit a web site where they are asked to update personal information, such as passwords and credit card, social security, and bank account numbers that the legitimate organization already has. [3]

This definition is accepted and shared by many other institutions in the security and banking industry. The Anti-Phishing Working Group (APWG), an organization whose existence is built upon the foundation of eradicating fraud over the Internet, defines phishing similar to that of Webopedia. Once again, e-mails and websites are referenced as the double dose of deception in this attack definition. Although both e-mails and websites have consistently accounted for the primary vector for delivering these attacks, it's important to not associate these terms as the sole manners in which phishing can target end users. Doing so creates a false sense of security for those who are only wary of phishing scams via their e-mail and the referenced html links contained within. A false sense of security can unknowingly be established as end users ultimately lower their guard towards other phishing vectors, addressed later on in this paper.

In summary, defining phishing is best achieved by realizing that it is a modern day ploy of social engineering that is not limited to the technical channels of e-mail and phony web sites. The non-technical portion of the attacks exploits personal fear, trust, and interest in luring users to their bait. The technical component to the attack today encompasses e-mails and websites, with more advanced phishing tactics employing Trojans, worms, and embedded scripts. The technical component is and will continue to be varied and not concentrated to a single source of technology. In response, security professionals and banking establishments must keep stride to new developments.

Section One – How Big is Big?

A press release issued by Gartner in May of 2004 quantifies the problem that phishing poses to the U.S financial sector:

> Direct losses from identity theft fraud against these phishing attack victims cost U.S. banks and credit card issuers about $1.2 billion last year[4].

The study also points out that roughly 57 million Americans have received e-mails that pertained to a phishing attack. Of that amount, it is projected that 30 million have genuinely been targeted with phishing e-mail, while an estimated 27 million believe that they may have received an e-mail that resembled a phishing scam. Of this alarming amount, only a fraction is needed to respond to

[3] http://www.webopedia.com/TERM/p/phishing.html
[4] http://www4.gartner.com/5_about/press_releases/asset_71087_11.jsp

the phishing bait in order for the ploy to be deemed a success by attackers. It is estimated that roughly five percent of all phishing e-mails are returned with confidential account information that could easily compromise a client's account funds.

The impact associated with phishing attacks extends beyond direct monetary losses. Threatened account holders may steer away from online banking services altogether. Confronted with the fear that they might not be visiting their banks website or truly corresponding with their bank via e-mail, bank customers may opt to return to paper statements thereby electing security over convenience. Although this scenario in its entirety is improbable, it does not negate the fact that the credibility of online banking services is in jeopardy if this problem continues to escalate. Long-term effects may include a slower growth of companies' online services. Along with benefiting online banking consumers, these online services have been pivotal to financial institutions in facilitating data processing, transaction processing and billing. No hard numbers exist supporting a decline in online services; however, most analysts contend that phishing is likely to reduce traffic in that area. Currently, it is estimated that more than 30 percent of bank consumers do some degree of online banking.

This point is furthered by David Jevans, chairman and one of the originating members of APWG. In a spring 2004 interview with Bank Technology News, Jevan explains that 'branding is everything' in a banking world where online services are like essential commodities. Banks and Credit Unions risk their reputation of being a secure banking establishment when their name, logos, and other identifying trademarks are represented in a phishing e-mail or fictitious website. As a result, financial institutions may witness diminished growth numbers of their online banking services. Untapped market share of potential online users will remain skeptical of these services and will continue to dismiss online services as a risky amenity for the brave at heart.

Phishing is mostly a banking problem. Of all the industries affected by the phishing epidemic, banking establishments have been the hardest hit. The below data visualizes the number of unique phishing attacks during June 2004.

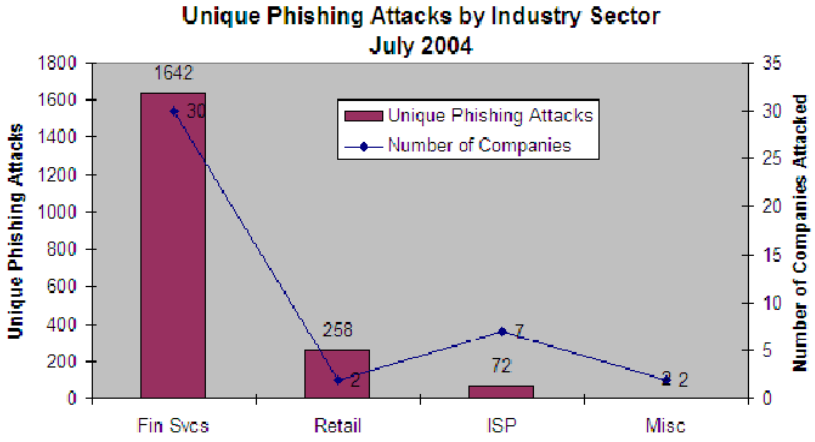


Figure 1

Source: APWG Phishing Attack Report-Jul2004

Being the primary target of these attacks, banks and other financial organizations will have to take a hard look in addressing what defensive measures are best to retain the credibility with their customers as well as control the surmounting costs associated with these attacks. The below table[5] summarizes some of the overall costs associated with phishing in the banking industry that was discussed in this section.

Figure 2

The Costs of Phishing
▫ **Per-attack costs:** Incurred from going after and shutting down rogue sites, cleaning up and law enforcement.
▫ **Per-affected-customer costs:** Increased support, handling compromised accounts and dealing with actual fraud.
▫ **Prevention costs:** Incurred independent of number of attacks or number of affected customers.
▫ **Long-term costs:** Loss of transaction volumes, loss of Internet channel and loss of customers.
Source: Financial Services Technology Consortium, New York

Phishing is a problem that will continue to escalate for both consumers and banking institutions. The APWG reports that phishing attacks will average at least 50 percent growth each month this year with an already 2 million dollar tab for U.S banks[6]. Having understood the magnitude of the problem and its scope, we look onward to diagnosing the technical aspects of phishing and what solutions to implement now and in the future.

Section Two – Dissecting the Phish

Again we reiterate that phishing is a form of social engineering. Phishing traverses across the Internet (via mail transfer agents, web servers) and exploits both human and technical vulnerabilities. As a result, phishing is both a technical and non-technical attack to diagnose. Arguments can be made that the solution in defending against these attacks is technical in nature. Others may contend that the lack of consumer awareness fosters a ripe environment for phishing to thrive upon. In reality and in good security practice, it's both. Adhering to the 'defense in depth' creed of Internet security, we adopt this best practice strategy in defending networks via a layered defense model. In this section we look at phishing's targeted vulnerabilities and technical makeup.

[5] http://www.computerworld.com/industrytopics/financial/story/0,10801,96549,00.html
[6] http://msnbc.msn.com/id/6416723/

© SANS Institute 2000 - 2005

Author retains full rights.

Trust and fear are the primary non-technical vulnerabilities that phishing attackers look to exploit. Falsely representing a banking website instantaneously gains the trust of that online user. Company logos, client specific information, and online banking paraphernalia prevents banking consumers from ever thinking twice about the legitimacy of the bank's online service. Whether online or off-line, the authentication has always been the responsibility of the consumer and not the financial institution. A banking consumer has never had to question whether their frequented bank is truly the same building, personnel, and establishment that it was the week before. Similarly, consumers using online services believe that the banking website they visited today will be the same tomorrow. The elements of deceit included in phishing attacks include fake logos, bogus banners ads, e-mail content that appears real, spoofed e-mails (e-mails with a falsified user@domain.com), and spoofed URLs (redirecting the user to the attacker's website and not the banks). The body of the e-mail often times instills fear or demands immediate action to be taken by the consumer. By stirring these emotions, attackers seek to blur the deceitfulness of their scam. This was the case with one of the better-known phishing attacks that targeted Citibank customers.

Having looked at how phishing undermines consumer confidence, we now look at how these attacks have propagated themselves via the Internet with such ease. Since e-mails have been the primary vector for which phishing has targeted its victims, we begin by examining mail servers as well as mail clients and how they've fallen short of detecting these frauds.

E-MAIL

E-mail is simply one form of transport for phishing. Thus far, it's been phishing's preferred way of traveling. While e-mail itself is simply the bait, it's the misleading contents or attached malware that poses the actual threat to the user. Adhering to the timeless suggestion of never opening mail from unknown individuals or that seem suspicious would make the risk negligible. However, because most users do not strictly follow this policy, the threat is real.

Deciphering what is suspicious or not is becoming increasingly difficult as e-mails become more and more authentic to that of a trusted banking institution. Current vulnerabilities within the SMTP protocol facilitate a phisher's disguise by not enforcing strict rules on editing the 'Mail From' and 'RCPT TO' fields. As a result e-mail originators can easily spoof addresses in the e-mail header and create authentic looking e-mails from victim's banks or credit card companies.

HTML formatted e-mails also add an extra layer of deception as they can obfuscate target URLs and veil hidden data in the actual body of the e-mail. Using simple HTML, such an embedded link would look like the following:

```
<a
href=http://www.phonybank.com:6666/fake/index.html>https://legitimatebank.co
```

m/id/default.asp

The above link would be displayed to the user within the anchor tags. Visiting the site would take the user to the illegitimate site where they would be prompted for banking information. Upon successfully filling out and submitting the disguised form, the user is generally directed to either an error page or redirected to their bank's true web page.

HTML based e-mails can be crafted to appear like text based e-mails, making it difficult to decipher for an end-user. Hidden html code camouflaged in the body of the e-mail can be inserted for the sole purpose of inserting legitimate key phrases that would fool certain spamming software products.

Vulnerabilities obviously exist with mail clients for their inability to contain these exploits to some degree. Additionally, exploits with Internet browsers offer added vulnerabilities for phishers to exploit. A recent phishing attack discovered by Panda Software details a phishing scam that is propagated by either an HTML based e-mail or web page. In the case of the e-mail, the embedded link appears to reference a bank's web page. When opened with Microsoft Internet Explorer, the link attacks an old vulnerability in the browser's code that prevents it from correctly displaying the URL of the web site. The process that is broken down is called canonicalization and occurs when visiting web servers using SSL/TLS 3.0 with a specific configuration. Since February of 2004, Microsoft has since provided information and a patch for this vulnerability. Browsers that have not been patched would not be able to know the true site they were visiting. Patched IE browsers would still be directed to the phishing page, however, the true source of the URL would be disclosed.

More disturbing and advanced mutations of phishing e-mails have recently been cited by e-mail filtering firm MessageLabs. Analysis from the firm shows that new phishing e-mails are actually becoming phishing-virus hybrids. The essence of these attacks is to rely less on a consumer action and more on malicious code that could extract and upload confidential information without user intervention. The attack occurs once a consumer's computer has been infected with the malicious code. From then on, when a user opens their browser to visit their online banking page, they are seamlessly redirected to the attacker's website. Regardless whether the bank URL is bookmarked or directly entered, the redirect is inevitable and the user unknowingly conduct their banking needs without knowing their presence on the attacker's webpage. The technique employed here involves a simple edit to an infected computer's local host file. The local host file is used to resolve hostnames with IP addresses on the Internet prior to referencing table values on DNS servers. Despite the fact that most computers reference DNS servers to resolve hostnames on the Internet, the use of the local host file has not been phased out, creating an unnecessary vulnerability for banking consumers.

© SANS Institute 2000 - 2005

Author retains full rights.

Instant Messaging/ IRC Chat Rooms

Chat rooms offer phishers easier forums to exercise their social engineering techniques. Instant Messaging allows for a different channel to gain access to personal or private information from IM victims (i.e – credit card information, personal information, etc). The phishing technique can either be strictly non-technical or technical. Through the use of lying, coaxing, or luring victims to unknowingly generate personal information, phishers can accomplish successful reconnaissance. Technically, it serves as another means to introduce malicious scripts or code to IM correspondents via transmitted links, corrupt images, or file transfers. Although banks and credit unions are discovering more efficient ways to curtail the use of messaging clients at work, it is one of the more difficult security loopholes to control due to the wide range of proxy servers that can are used to relay IM traffic and the use of non-standard ports.

TROJAN HORSES

A Trojan Horse is a seemingly legitimate software product that contains malicious embedded code. While Trojan horses do not exclusively aid phishers in furthering their efforts, they have been discovered to relay phishing emails throughout the Internet.

Trojan horses are utilized by many other malicious programs and for various other reasons besides obtaining confidential financial information. Specifically related to phishing attacks are the hijacked hosts that are part of a wide network of computers that record, share, and hold monitored information as part of large fraudulent framework. Most of these victimized computers have minimal security settings and un-patched software vulnerabilities making it a primo nesting cell for propagating phishing ploys.

One of the more infamous Trojan Horses that terrified banks and their online users was the key-logger Trojan. Spread via HTML based e-mails or compromised websites, the Trojan was introduced to a victim's computer if their browser settings had been insufficiently restricted. The downloaded software would then log keystrokes when window title frames included the names of popular banks and retail sites. Targeted banks included those such as Bank of America, Citibank, and Bank West.

WWW.FAKEBANK.COM

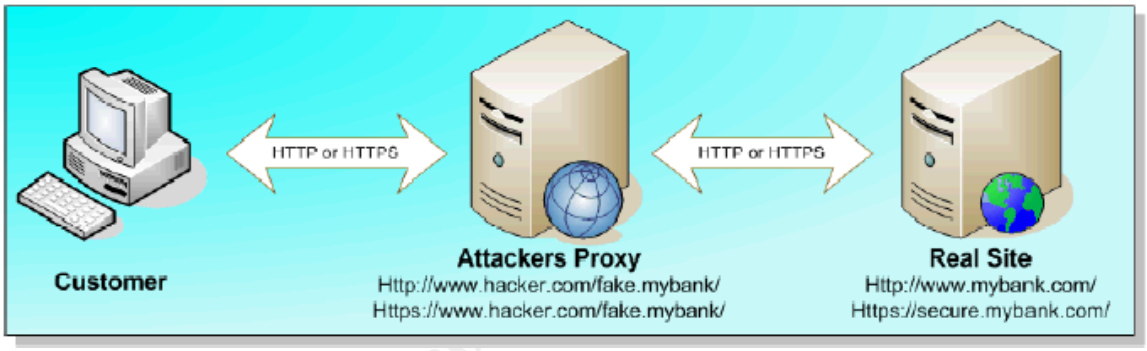
As previously mentioned, phishing attacks ultimately employ the use of a phony banking website to collect bank data from a user. In prior examples, misled consumers visited the perpetrated bank website mostly via e-mail and in some cases via introduced mal-ware. In those examples, the user ultimately was lured into visiting the bogus site. In the following section we examine how some phishing artists are able assume a less conspicuous role yet accomplish their social engineering through more covert operations.

© SANS Institute 2000 - 2005, Author retains full rights.

One of the more advanced phishing techniques used to deceive online bank users is through the use of proxies. Often times referred to as man-in-the-middle attacks, the attacker sits in between the banking institution and the bank on-online user. All communication amongst the three parties occurs in real time. It is believed by some security experts that these attacks will be more prevalent in the future. According to Dr. Johnathan Tuliani, UK Technical Manager for Cryptomathic Ltd, man-in-the-middle attacks position the attacker to conceal his presence while recording all of the bank related information from users. He adds these highly orchestrated attacks bypass even multiple layers of authentication since the attacker does not interfere with the bank login process.

Man-in-the-middle attacks operate with an intermediary server or proxy that handles the http/https request and thereafter hands the traffic off to the bank's web server. The below diagram illustrates the attack channel while in progress:

Figure 3



Source: The Phishing Guide by Guntar Ollman

A well designed man-in-the-middle attack serving falsified bank web pages can easily fool even the most paranoid online users. The technical exploits targeted by the attacker will directly affect the outcome of the online scam. Below we address some of the opportunities that the phisher may exploit:

- Transparent Proxies – Positioned in the direct path of the consumer's http/https request, this type of proxy achieves a stealth and seemingly benign profile. An attacker's stealthy profile is achieved by obtaining an IP address belonging to the same public IP space as the bank's web server. Alternatively, an attacker's web server, hosted by an intermediary ISP, can be part of a network 'hop' to the true banking web server. Once the attacker has successfully intercepted the user's web request to their true bank server, submitted data is snatched, logged, and forwarded to the true banking web server by the transparent proxy server.

- DNS Cache Poisoning – Domain Name Servers have historically provided vulnerabilities for hackers to exploit, particularly in the last decade. DNS Cache Poisoning is achieved by altering the entries in the cache of a

© SANS Institute 2000 - 2005

Author retains full rights.

DNS server. The cache is used to expedite lookup requests and serves as a table, matching IP values to hostnames. The cache is 'poisoned' when a hostname resolves to a false IP. In a corporate environment, DNS servers are the principal targets while attacks on individual users affect the local hosts. In either case, a banking institution's hostname may resolve to the attacker's web server.

A brief historical look back at DNS vulnerabilities reveals the viability and reality of DNS cache poisoning today. Banks need to review DNS server configurations seriously in order to avoid these covert attacks. Christopher Schuba discovered one of the early DNS vulnerabilities, which was detailed in a security paper he authored while attending Purdue. His discoveries essentially detailed how the DNS daemon was able to receive a reply packet that remained cached and could be later referenced by a future DNS request[7]. Other discovered vulnerabilities pertained to the BIND (Berkeley Internet Name Domain) software, which was discovered to use a sequential transaction ids that were assigned to new requests. In this case, simply sending a spoofed query to the DNS server and logging the transaction id of the request, the attacker could thereafter send a spoofed reply using the sequential transaction id.

- URL Obfuscation – This technique is commonly used by phishers because of its simplicity in implementation (e-mail, pop-up, IM, etc). Attackers rely on the fact that most users disregard checking the authenticity of a URL or its format. Many online bank users may never have observed the URL of their banks visited web site and can therefore not provide a valid comparable basis when confronted with an obfuscated banking URL.

  Obfuscated URLs are accomplished in many ways. Some of the more simpler smokescreens created by phishers include simply bad URLs missing a letter in the domain name or substituting an ASCII character with an international character that looks similar. (simple example: http://www.legitimatebanking.com and http://www.legitimatbanking.com).

  Third party sites facilitate URL obfuscation by concealing long, confusing URLs with short ones. Phishers have the convenience of intentionally referencing long URLs in an e-mail which when clicked result in a short URL in the browser window via this third party service.

  While there are other methods to URL obfuscation, encoding schemes are one of the more advanced forms of accomplishing this phishing technique. Of the various encoding schemes available, Unicode UTF-8 encoding is one of the more widely utilized formats since it preserves the entire range of the US-ASCII character range. As a result, various

[7] http://ftp.cerias.purdue.edu/pub/papers/christoph-schuba/schuba-DNS-msthesis.pdf

© SANS Institute 2000 - 2005, Author retains full rights.

> characters can be represented in different character sets allowing phishers to register their sites using different character sets.

Authentic Web Certificates

Attackers have also found ways to fabricate certificates and perpetrate a trusted banking source. Most users are familiar with the lock icon displayed at the bottom of a web browser. The lock icon serves as a visual indication to a secure website, however, with false certificates the icon is still visible to online users and provides them with a false sense of security. Exploiting this vulnerability, attackers issuing fake certificates can visibly fool bank consumers that the site they're visiting is a legitimate secure site. In a published NetCraft article, this technique known, as visual spoofing is further illustrated:

> The technique alters the user interface of the web browser, substituting images for parts of the browser interface that would normally help users detect the fraud. JavaScript links launch a new browser window without scrollbars, menu bars, toolbars and the status bar - which allows the scam artists to substitute a fake status bar containing the URL for a legitimate site, along with an image of a "lock" indicating a secure SSL site.[8]

As a result of these visual spoofing techniques, bank users are forced to become more vigilant when banking online. Users need to validate the URL address, the security icon at the bottom of the page, and validate the certificate by clicking on the lock icon.

As ways to mask malicious web sites become increasingly sophisticated, it is imperative that banks, credit unions, and other financial establishments maintain themselves current with the latest online scamming techniques. Phishing is evolving and mutating continuously. During the holiday seasons, phishers look to e-mail and pop-ups as main vectors in conducting targeted holiday hoaxes. As reported in a November 2004 PC Magazine article, phishers look to cash in on some 'un-holiday' spirit from online users via e-mail. The article details how to win a Mercedes Benz over the holiday by responding to an e-mail. As expected, personal information is required in order to be a part of the holiday drawing[9].

Upon having reviewed some of the vulnerabilities present on various servers, applications, and protocols, the next section provides solutions geared towards minimizing the increasing level of risk currently affecting financial institutions, their clients, and the banking industry.

Section Three – Securing Banking

[8] http://news.netcraft.com/archives/2004/03/08/ssls_credibility_as_phishing_defense_is_tested.html
[9] http://www.pcmag.com/article2/0,1759,1573372,00.asp

Overall, it is important that a bank or credit union establish a formal security policy that adheres to a standard best practice and defense in depth philosophy. Such a policy serves as primary foundation for which technologies, training, and communication help support. A formal security policy should become a 'living document' – always evolving and changing to address new threats and vulnerabilities. Investing and supporting such a policy demonstrates a financial institution's sincerity to provide assurance to confidential data.

TECHNICAL CONSIDERATIONS

Discovering where to begin tightening down on vulnerability loopholes in a financial institution can be a daunting and aggravating job. It's vital to perform a comprehensive audit of any networked device; its usage, OS and application specifications, and security vulnerabilities. A walk-through may be needed through a bank or credit union in order to ensure that no 'rogue' network devices are present. If unaccounted for network devices are present after implementing a formal security policy and tightening down known network devices, the entire accomplishment can easily be undermined by the rogue host sitting on your network and serving as a gateway to shared resources.

Upon completing a successful audit of all network equipment, an examination of each device is essential in order to evaluate its individual vulnerability to attacks, viruses, or worms. Assessing the security level of each host can be cumulatively accomplished through the use of an internal or external scan. Third party managed services usually conduct such vulnerability assessments, however, if an initial audit has never been performed, it is preferable for a bank's IT Manager to perform a preliminary assessment by which other future third party assessments can be compared against.

Segregating the network of a financial institution into various sections facilitates the security audit. The same security risks do not apply to workstations as they apply to DNS or Mail servers. Upon obtaining an inventory list of connected network devices, these devices must be classified as a server resource, workstation resource, or company-wide resource.

Securing the Workstation

One of the more time consuming responsibilities for an IT manager is in tightening security at the workstation level. Auditing a vast number of workstations on a network is time consuming, but relatively simple if an IT Manager creates a list on what to check. The following should be the principal areas in workstation security. Since the majority of banks and credit unions use some version of Microsoft Windows as their operating system, the following points will pertain to such.

- Patch Management/ Updates – Generally available every 2nd Tuesday of a month, Microsoft publishes security bulletins revealing flaws or vulnerabilities in either the OS or one of its many software products. The

© SANS Institute 2000 - 2005

Author retains full rights.

benefit is that IT Managers are briefed about these vulnerabilities, however, hackers and virus authors are also informed to these new 'weak spots' to target. It is crucial to implement patches as soon as they become available by Microsoft.

Automatic Updates for Windows 2000, XP facilitates updates to software and OS vulnerabilities. This service can be configured to various degrees so that updates are applied automatically or at the discretion of the IT Manager. If budgetary constraints allow, previous versions of Windows (i.e. – Windows 95, 98, or ME) need to be upgraded to more secure OS versions or protected by other means. Those means can include AV software, limited Internet and e-mail access, and limited running services. This level of automatic updates can be set according to the degree of control desired during the update process.

Windows Automatic Update serves as a simple and efficient method for protecting work stations in a small banking environment, however, for larger financial institutions, a more robust patch management system is required for better control and distribution of updates. Ideally, a localized patch management system for workstations is worth the investment by larger banks. Such a system would be willing to conduct updates locally from a centralized network server. Some Windows patch management products include BigFix's Enterprise Suite Gravity, Storm Software's Service Pack Manager 2000, PatchLink's Update and Shavlik Technologies' HfNetChk Pro.

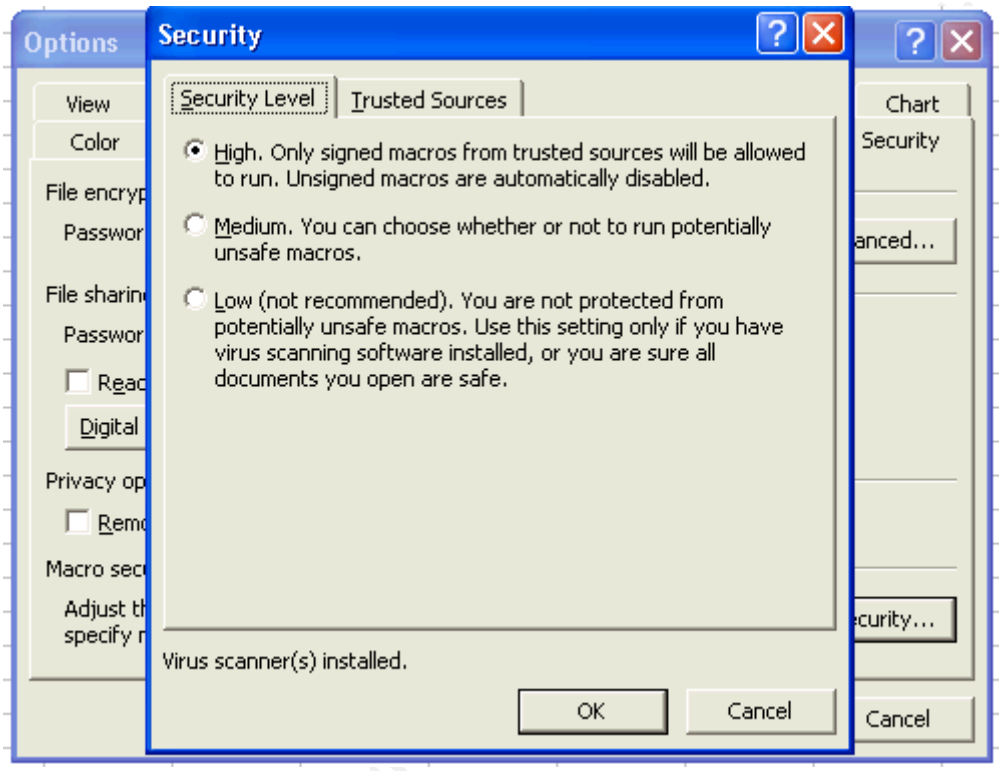
- Software Customization – Despite a tightly patched workstation, there are additional pre-cautionary measures that can be conducted. Aside from e-mail clients and web browsers, tightening word processing and spreadsheets with security loopholes is a perfect adherence to the defense in depth philosophy. Recently discovered security flaws in MS Word and MS Excel provide another channel for an attacker to introduce malicious code. Using flaws in the mail merge function in Microsoft Word, attackers can send a maliciously crafted mail merge document saved as an HTML link. The link would run code in another Microsoft product, MS Access and allow for an attacker to completely take over your machine[10]. Similarly, damaging code, introduced by the same vector, can be embedded in MS Excel spreadsheets that have malicious macros.

  MS Word, Access, and Excel are extremely popular and useful tools employed at financial institutions. Advanced phishers with excellent social engineering techniques could easily craft a seemingly legitimate e-mail attachment that appears legitimate. By enabling Word and Excel to only accept signed macros or those from trusted sources, hedges this

[10] http://pcworld.about.com/magazine/2010p055id103757.htm

threat. Below is a snapshot of where to enable additional precautionary measures to prevent macro based attacks:

Figure 4



- User Privileges/ Workgroups – Defining user privileges across network resources protects from both external and internal attacks. Viruses introduced by phishing sites may affect that particular host, however because of the inherited rights of that user pertaining to its network group; the damage can be contained and logged. Disabling guest accounts or accounts on hosts that are no longer in use is also proper security measures to tighten up a workstation.

- Standard Services/ Port Management – Open ports and gratuitous services running on Windows 2000 or WinXP installations are two important areas that IT managers need to assess when auditing their workstations. Determining a standard template as to what services and ports are permitted should be established. Future violations can be compared against this standard workstation configuration. Ensuring that these services are disabled and not running at startup further prevents attackers from exploiting workstation resources. Unfortunately, earlier versions of Windows including 95, 98, ME, and NT do not have this functionality.

- E-mail/ Browser Security – As mentioned throughout this exposition, e-

© SANS Institute 2000 - 2005

Author retains full rights.

mail and web sites are the primary proliferators of phishing acts. At a high level, e-mail and web browsing policies should serve as guidelines for usage. A strict e-mail and web browsing policy can sometimes trump some protective technical measures. However, most organizations have moderate rules pertaining to e-mail and web browsing thereby creating the need for technical security measures.

In June 2004, the United States Computer Emergency Readiness Team (US-CERT) recommended users to stop using Microsoft's Internet Explorer for web browsing due to major security flaws associated with the software[11]. In regards to banking operations, Internet Explorer and its features are not irreplaceable for banking online operations. Other available low-thrill browsers are just as functional for most banking web apps, yet devoid of many of IE's security flaws.

In general, it's important to ensure that any browser has the ability to prevent the following: pop-up ads, Active X Scripts, and Java run-time support. Additional customization may be needed to prevent the storage of cookies and cached Internet pages and the automatic play of multi-media files. A cross examination of any internal financial web app must be assessed prior to implementing these steps in order to prevent that legitimate internal banking applications be adversely affected.

Although there is a range of e-mail clients that banks or credit unions can choose, most use some edition of Microsoft Outlook or Outlook Express. Patches and hot-fixes for versions of Outlook are critical in fighting phishing attacks. Historical virus attacks have proven to be successful through the exploitation of various MIME vulnerabilities. Most of these MIME vulnerabilities have been addressed in newer versions of the Outlook client. Evaluating outdated versions and their vulnerabilities can be cumbersome. If budgetary constraints allow, an enterprise wide upgrade to Outlook should be considered.

Three important 'lockdown' recommendations for Outlook include disenabling HTML functionality, disenabling MS Word or Rich-text formats for mail editing, and attachment blocking. Disenabling HTML formatting and advanced e-mail editing typically do not interfere with day-to-day banking operations. Blocking attachments, if done correctly, would prove the same as well. Allowing should be examined on a host that has the ability to scan the attachment for viruses before becoming accessible to users on the network.

Securing the Server

Mail.

[11] http://www.pcworld.com/news/article/0,aid,116848,00.asp

© SANS Institute 2000 - 2005

Author retains full rights.

Publicly visible from the watchful eyes of the *world wide phish-net,* mail, web, and FTP servers are directly vulnerable to the attacks of Trojan horses, viruses or worms. Due to its elusive nature, phishing is difficult to defend against since phishing tactics can take the form of an e-mail, a superimposed browser image over a bank's website, or a misleading bank pop-up ad. These camouflaged phishing attacks penetrate banking networks if counter phishing measures are not in place.

A banking mail server's risk level is directly related to the frequency of mail server upgrades/ security patches, the use of AV or spam filtering software, and defending against known SMTP exploits. For example, known exploits in Microsoft Exchange 5.5 allow attackers to introduce malicious code that affects those using the Outlook's Web Access interface. Patches for this popular version of Microsoft's mail server have been deployed and upgrades to 2000 and 2003 do not have this vulnerability. The issue that most banks need to address is *when* the upgrade should take place, not *if.* A bank's shortcoming to minimize the time frame between a newly publicized exploit and the solution's implementation will only augment the risk. In the above example, an Exchange 5.5 mail server left un-patched could ultimately lead to cross-site scripting attacks.

No patch or hot-fixes exist to heal SMTP's naivety. SMTP mistakenly allows anyone to forge a sender's FROM and MAIL FROM address. Unfortunately, the protocol lacks any built in authentication functionality that could be used by mail client software to authenticate the source of the e-mail. However, e-mail authentication tools do exist to validate the address against additional sender information. Below is a list of four of the more prevalent and leading solutions for e-mail authentication, followed by a brief description of each:

- SPF (Sender Policy Framework): validates the MAIL FROM address from the e-mail message by querying the domain of that IP for a list of valid addresses. The resulting list of valid IP addresses is returned and compared to that shown in the TCP/IP header of the inbound mail message.
- Caller-ID: similar to SPF, however, queries the DNS of the domain shown in the FROM address rather the MAIL FROM field. Does similar DNS-to-IP comparison shown above with SPF.
- DomainKeys: uses asymmetric cryptography to authenticate the domain name listed in the FROM field of the e-mail header. Digital signature is verified against the DNS server of the domain name shown in the FROM address.
- S/MIME Digital Signature: employs asymmetric cryptography to authenticate both the sender and the domain shown in the FROM address; widely deployed e-mail signatures, security measure protocol used to encrypt e-mail.

Source:Using Digital Signatures to Secure E-mail and Stop Phishing Attacks [12]

© SANS Institute 2000 - 2005, Author retains full rights.

The above authentication measures would have the most benefit on internal e-mail usage and not adequately resolve correspondence between banks and their consumers. It is debatable whether or not banking consumers should be expected to be more vigilant when they conduct their online banking activities. Additional complexity will simply add to the fear of online banking and ultimate curve the usage altogether. Widely publicized phishing articles provide little reasonable technical solutions to defending consumers from phishing scams sent via e-mail. Ultimately, repeatedly informing banking consumers on what type of email correspondence to expect via bank posters, bulletins, etc provides the best form of foiling phishers from tricking consumers into sharing their account information. The aforementioned details regarding mail authentication is however an excellent and effective measure for destroying phishing attacks targeting bank sites or business accounts for which e-mail correspondence is more prevalent.

Web.
Providing a more direct impact to phishing attacks towards banking consumers is security changes to web servers. A banking website is a consumer's online representation as to where they bank. Most consumers authenticate their bank's webpage by the logos, information, and tools that are provided via that web site. Establishing credibility is done in a matter of seconds. For this reason, a bank must secure some of the previously mentioned web server vulnerabilities that a phishing attack may exploit.

Fighting URL obfuscation is one of the many battles that bank's face. Unfortunately, this is a battle in which banks rarely know the site of the attacker that is perpetrating the bank's online business. Structuring a bank's URL to be simple, easy to recognize, and always including the domain name (e.g. – www.mybank.com/apps/loans/form1.php) trains customers to become accustomed to the format of their bank's URL. A bank or credit union should also avoid having redirects in their web pages or URLs that show or redirect to IP addresses. Registering other variants of a bank's domain name is also good assurance in evading future phishing attacks. By not leaving too many other look-a-like domains, a phishing artist's choice for domains is limited. Renewing existing domain names is also highly important so attackers aren't given the opportunity to design and publish a phishing site.

Content recycling is a simple but effective tool in establishing authenticity with consumers. Phishing web sites mirror a bank's online pages by replicating the content of a bank's website in a certain point in time. As a result, most phishing sites contain only static content. Through the insertion of new images or rotating images on a bank's website on a period basis, banks and credit unions can coach their consumers on what to be wary of when ensuring that they are

[12] http://cnscenter.future.co.kr/resource/security/application/0304_tmwd_wp_digital_signatures.pdf

banking at the right site. Providing dynamic images, ads, and banners makes a banking site more difficult to spoof.

A more effective method for online validation is adopting a multi-channel authentication model where both parties authenticate. Two-way authentication enables both banks and consumers to validate who is on the other end of the network line. This level of authentication is more effective than a layered authentication approach, which is one-way. Passwords and token-based authentication are two examples of one-way authentication methods commonly used today. However, these methods are useless in man-in-the-middle or proxy attacks. An attacker could position themselves between the bank server and the end user, collecting login ids, passwords, and token information transmitted en route to the genuine banking server. Dr. Jonathan Tuliani, UK Technical Manager for Cryptomathic Ltd. further elaborates on how multi-factor authentication fails in more elaborate attacks:

> My firm belief is that the next few years will see the emergence of Internet man-in-the-middle attacks. Here, the user is tricked exactly as described above, except that instead of just the user communicating with the attacker, the attacker is also communicating in real-time with the bank. Two (or even ten) factor authentication is of no help, since the attacker doesn't interfere with the login process. Both the user and the bank are unaware of the presence of the attacker, and believe they have a secure connection directly from one to the other.[13]

Going beyond multi-factor authentication is two-way authentication which establishes credibility between both the user and the bank, each having to prove their credibility. Authentication can occur over the same network traffic, or preferably through another channel. Many larger financial institutions, vulnerable to more advanced phishing schemes, have implemented two-way authentication over two different channels, one being the Internet and the other being an SMS network. In this case an attacker would have to intercept confidential data over two different networks, making it extremely difficult for them to be successful.

Security banking experts will recommend the implementation of transaction-based security versus session-based security. Session based security only authenticates the beginning of an online banking session. Once token and password information is submitted, the entire web session is authenticated and transactions are authorized without question of credibility. Conversely, transaction based security authenticates each transaction made during the banking session. For example, the bank can confirm a transfer made between two banking accounts by confirming the transfer details and supplying a one-time password via an SMS channel. In this scenario, the banking consumer establishes credibility as the account holder each time and the bank establishes

[13] http://www.net-security.org/article.php?id=672

© SANS Institute 2000 - 2005

Author retains full rights.

credibility that it is the banking institution executing the transfer request.

Securing the Corporate Environment

External and internal perimeter defense systems such as firewalls, Intrusion Detection Systems, Intrusion Prevention Systems, or anti-virus scanning enterprise servers are the front lines of network security for financial institutions. Some peripheral systems are not well equipped to address phishing attacks since those attacks appear to be benign network traffic. Those that due have built in phishing defense mechanisms must always maintain their software updated in order to address new phishing techniques. Some effective perimeter defense mechanisms phishing attacks include the following:

- Anti-Virus Scanning – detects malicious attachments, embedded HTML, or hidden binary code to a bank's network
- Anti-Spam Filtering – rule based inspection of email to prevent successful delivery of spam
- Content Filtering – inspecting content of communication channels (IM, HTTP, FTP, etc)
- Proxy Services - assisting in the management of forms of Internet communication into a banking network

Phishing targets both consumers and employees of a financial institution. In regards to bank's employees, these aforementioned perimeter defenses can help substantially. However, the negative effects of phishing mostly target a bank's customers. In order to preserve the credibility of the bank or credit union, it's imperative that a bank monitor the performance and use of their mail, web, and DNS servers, which are common exploitable resources used in phishing attacks. Active vigilance on behalf of the bank or a third party managed service is extremely useful. The cost savings and efficiency delivered by managed security companies is very beneficial for smaller banks and credit unions that may not have the resources or the time to employ permanent resources.

It's important to note that if a bank or credit union does administer their own perimeter systems (mail, DNS, web, router, switches, proxies, etc.), it's important to not use the default configuration settings that were provided by the manufacturer. Doing so allows hackers or phishing artists to learn these base configurations and exploit their weaknesses. A detailed customization of enterprise wide systems will prevent some of the more common attacks from exploiting overlooked or poorly configured network systems. Case and point comes from a recent article detailing Microsoft's disclosure of server side vulnerabilities with its ISA 2000 Server and Proxy Server 2.0 products. By default, the cache in these servers is not set to zero which can allow attackers to spoof stored URLs in the server's cached pages. Setting the cache size to zero effectively disables DNS caching on those servers. Adhering to these and

© SANS Institute 2000 - 2005, Author retains full rights.

other manufacturer security alerts will further aid banks in creating a fortified anti-phishing network.

NON-TECHNICAL CONSIDERATION

As in most serious crimes, education serves as one of the primary weapons in fighting phishing attacks. Banking consumers need to be aware that they are the intended targets for phishing scams. Educating consumers in a professional and non-sensationalistic manner will allow them to be vigilant when conducting their online banking needs. Although the issue of phishing attacks is difficult to discuss while not instigating worry, doubt, and fear, the alternative of not communicating to banking consumers is far worse. Identity theft has been on the rise and is a growing issue. Phishing is simply another vehicle for which this crime is being committed. Maintaining customers aware of new trends in security and what procedures their bank or credit union is taking to defend against these attacks will create a more informed, aware, and less vulnerable group of banking consumers. Communication, however, should not be the only form of defense. A combination of both public relations and technical security changes to a bank's network serves as a good foundation for defense.

Conclusion

As the number of online banking services continues to grow in the U.S, phishing attacks look to profit from simply a handful of those online transactions. The payoff is tremendous for the attacker and the damage is likewise great for the financial institution. The amount of damage from phishing attacks will only continue to grow if precautionary measures are not put into place by financial institutions and stricter regulations are not created. Banks and credit unions need to provide assurance to their consumers by taking the necessary steps to secure their internal and external banking resources. A combination of both technical security measures and effective communication to consumers greatly minimizes the risk associated with these social engineering attacks.

Authentication is the ethereal victim for banks throughout the war on phishing. Discovering new channels and methods to successfully authenticate consumers with banks and vice versa is the key in addressing future phishing attacks. Consumers have historically been responsible for establishing credibility to the bank. Now banks too must find ways in which they can prove their authenticity to consumers via the Internet.

Banking security measures should not be regarded as an implemented change but rather an on-going process of formation and reformation. As phishing attacks become more sophisticated in nature, security measures must be continuously re-addressed in order to ensure that current techniques and defense mechanisms are adequately capable of addressing these new attacks. It is certain that phishing artists will look to thwart new security measures. In response, banks must be proactive in finding ways in which these criminals will

© SANS Institute 2000 - 2005, Author retains full rights.

cast their next form of bait.

© SANS Institute 2000 - 2005, Author retains full rights.

References

1. Johnson, J. Stuart. “Plug Dangerous Holes in Word, Excel.” http://pcworld.about.com/magazine/2010p055id103757.htm.
2. “Internet Explorer HTML Elements Buffer Overflow Vulnerability.” http://secunia.com/advisories/12959/.
3. Policht, Marcin. “Windows Patch Management.” http://www.serverwatch.com/tutorials/article.phpr/3299831. January 15,2004.
4. LURHQ Threat Intelligence Group. “DNS Cache Poisoning - The Next Generation.” http://www.lurhq.com/cachepoisoning.html.
5. Krebsbach, Karen. “Goin' Phishing.” http://www.onlinesecurity.com/links/links925.php.
6. Vijayan, Jaikumar. “Companies Fight Back Against Phishing Scams.” http://www.computerworld.com/securitytopics/security/story/0,10801,96549,00.html. October 11, 2004.
7. Rosencrance, Linda. ”TECF aims to fight online fraud.” http://www.thestandard.com/article.php?story=20040617173836939. June 17, 2004.
8. McCall, Tom. “Gartner Study Finds Significant Increase in E-Mail Phishing Attacks.” http://www4.gartner.com/5_about/press_releases/asset_71087_11.jsp. May 6, 2004.
9. Ollman, Guntar. “The Phishing Guide.” http://www.nextgenss.com/papers/NISR-WP-Phishing.pdf.
10. Jacques, Robert. “Microsfot flaw leaves PCs open to phishing.” http://nl2.vnunet.com/news/1159305. November 10, 2004
11. FDIC. “FDIC Consumer Alerts – Phishing Scams.” http://www.fdic.gov/consumers/consumer/alerts/index.html.
12. US-CERT. “Avoiding Social Engineering and Phishing Attacks.” http://www.us-cert.gov/cas/tips/ST04-014.html. 2004.
13. Webopedia. “phishing.” http://www.webopedia.com/TERM/p/phishing.html.
14. Sullivan, Bob. “A new, more sneaky phishing attack.” http://msnbc.msn.com/id/6416723/. November 5, 2004.
15. Schuba, Christopher. “Addressing Weaknesses in the Domain Name System Protocol.” http://ftp.cerias.purdue.edu/pub/papers/christoph-schuba/schuba-DNS-msthesis.pdf. August 1993.
16. M. Rich. “SSL's Credibility as Phishing Defense Is Tested.” http://news.netcraft.com/archives/2004/03/08/ssls_credibility_as_phishing_defense_is_tested.html. March 8, 2004.
17. “Phishing Aims for Epidemic Status.” http://www.pcmag.com/article2/0,1759,1573372,00.asp. April 2004.
18. McMillan, Robert. “Mozilla Gains on IE.” http://www.pcworld.com/news/article/0,aid,116848,00.asp. July 2004.
19. Tumbleweed White Paper. “Using Digital Signatures to Secure Email and Stop Phishing Attacks.”

© SANS Institute 2000 - 2005 Author retains full rights.

http://cnscenter.future.co.kr/resource/security/application/0304_tmwd_wp_digital_signatures.pdf. 2004.
20. Tuliani, Dr. Johnathan. "The Future of Phishing." http://www.net-security.org/article.php?id=672. April 5, 2004.

© SANS Institute 2000 - 2005, Author retains full rights.