

Phishing and Pharming: Today's Weapon of Choice

For as long as there have been banks, there have been bank robbers the difference is today you don't need a six shooter. There are still plenty of Jesse and Frank James' out there but compared to the criminals in the 21st century, the James and Dalton Gangs look like a bunch of amateurs. The Wild West criminals of yesteryear could only attack one bank at a time, riding into town guns blazing; everyone knew they had been there. Modern day wild wild west (www) criminals on the other hand are much more sophisticated and the attacks are performed on multiple targets in stealth mode, often times going undetected until it is to late.

Phishing, pharming, and malware are today's weapons of choice, and the payload is information. Information that can be turned into money: credit card, bank account, social security numbers, user IDs, passwords, and PINs. Armed with this information, they breach the institution's security, try to extort money from the institution, or commit identity theft. Customer information isn't the only data at risk; however, your corporate financial and intellectual data is at risk as well.

According to a report issued by the Internet Crime Compliant Center (IC3), the center logged more than 228,400 Internet crime complaints in 2005 and reported total losses of \$17.8 million.

What is Phishing?

A form of identity theft where deception is used to entice a user into revealing personal and confidential information such as:

- An account number
- Password or PIN
- Social security number
- Credit card number

What is Pharming?

Pharming is an attack in which a user can be fooled into entering sensitive data such as a password or credit card number into a malicious web site that impersonates a legitimate web site.

Who are the attackers?

Too often we think of the attackers as only the lone professional hacker, someone we don't know who has made a career out of hacking and cracking into computer systems. However, that isn't necessarily the case. There are organized crime rings from all over the world getting in on the action. You also may need to look no further than your own organization, a disgruntled

employee, a contractor, a vendor's employee, a former employee, a disgruntled customer. It also could be someone from the institution down the street, one of your competitors, or just a curious high school student.

What is the motivation?

Once upon a time the primary motivation was recognition, but just as the method for perpetrating the crime has evolved so has the motivation. Today it is all about financial gain, identity theft, and competition.

What are they doing?

Phishing and pharming attacks directly target valuable information. Believe it or not but phishing (pronounced fishing), a scheme using email typically with links to websites, has been around for about 10 years. A phishing email appears to come from a legitimate source like your financial institution and tries to lure users into divulging personal data. Initially hackers used phishing to steal America Online (AOL) accounts by scamming passwords. Today, according to the Anti-phishing Working Group, the United States hosts the largest number of phishing sites. Fig 1.



Fig. 1. APWG Activity Trend Report – January 2006

In addition, the attacks have morphed into much more sophisticated scams targeting the financial industry and online retailers. Fig. 2. Also, while once targeting the larger institutions, phishers are now setting their sites on the smaller, regional and community institutions as the larger institutions are perceived to have more resources for securing their sites and safeguarding information.

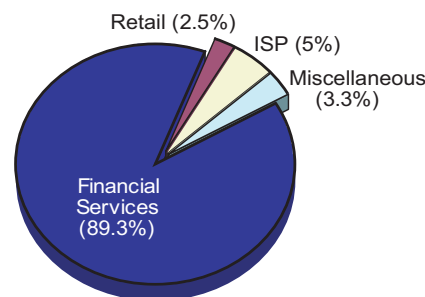
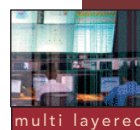


Fig. 2. APWG Phishing Activity Trend Report January 2006



Unlike phishing where the recipient actually has to respond to an email or click a link, pharming (pronounced farming) is more sinister. Pharming simply redirects users from a legitimate website to a fraudulent one without their knowledge. The pharmed site will look the same as the real site so the user will confidently enter their user ID, account number, and password. Once entered, the evil doer now has sufficient information to commit identity theft by impersonating the user, steal money from their account, apply for loans and credit cards, set up bill pay, or hold the information for ransom. Like phishing, pharming isn't new; however, its use to commit cyber crime is and its use is becoming more proliferated.

How are they doing it?

Phishing. Phishing attacks can be executed in a number of ways, but typically involves accumulating information from the institution's website, like the logo and header information, to give the email a legitimate look and feel. Then they cut and paste pages from the true website to create an authentic looking fake website. In many cases, these fake sites are virtually undistinguishable from the real site, right down to the Verisign seal, in fact the Verisign seal can be legitimate, it just happens to verify a completely different site. An email is created using the authentic looking logo and stating that the user's information needs to be updated, or validated, or that due to a security breach needs to be reset. A link is provided for convenience so all they have to do is click. When they do the victim is routed to the fraudulent site where they are prompted to input their account number, user ID, and password. Many even attempt to

collect secret information like mother's maiden name, or even their social security number. Some sites will then, after they have collected the information, actually redirect the user back to the legitimate bank site.

A newer scam involves sending the customer an email offering a chance to receive \$20.00 by filling out a survey; of course the link provided directs the user to a fake website where they post a survey complete with a request for the account number, user ID and password so that the funds can be deposited directly into their account.

And since many are becoming wise to the "click on the link" tactic, as of April 2006, phishers were sending out emails directing customers to verify their banking information by dialing a phone number that was conveniently provided.

Committing a phishing attack doesn't really require a great deal of skill or sophistication, in fact, "do it yourself" kits are readily available from the Internet. The kits include all the necessary tools to develop bogus messages and graphics, HTML code, and sample text.

Pharming. Pharming attacks are somewhat more sophisticated and difficult to perform, and if successful contain very damaging outcomes. There are several ways to commit pharming attacks most generally it involves exploiting a vulnerability in the Domain Name Server software (DNS) that allows the redirection of the legitimate website traffic to another fraudulent site. There are approximately 9 million DNS servers on the Internet, which are run by companies and Internet service providers. The DNS servers act as the white pages for the Internet, when you type in an address www.myfinancialinstitution.com

the DNS server translates it into an IP address like 192.1.2.123 for example and then forwards the traffic to the website. The vulnerability within DNS allows an attacker to "spoof" or "hijack" the traffic intended for www.myfinancialinstitution.com, also known as DNS poisoning, and routes it to the fake site.

As with phishing attacks, the evil doer will copy the institutions web pages so you don't realize you are not where you intended to be. Security experts say DNS poisoning like phishing isn't new, but due to the increased use of the Internet to conduct financial transactions, criminals are now using the exploit for profit.

In addition to DNS poisoning, attackers can use static domain name spoofing, where they slightly change the actual name from www.myfinancialinstitution.com to www.myfinancialinstitution2.com or they will change the .com to .net. Pharmers also will submit requests for domain transfers to a domain registrar asking that the domain be switched from one registrar to another. When accepted, traffic is redirected to the illegitimate server. Failure to properly manage your domain name can lead to yet another method of "hijacking" a website. Domain names are leased for a fixed period of time and need be re-registered. If the name expires, any one including an evil doer can transfer ownership of the name.

Another tactic is the use of crime ware in the form of key loggers and Trojans. In these instances malicious code is installed on an unsuspecting user's computer which will capture

keystrokes, specifically user ID and passwords then send them to the attacker. Trojans are also used which will plant a backdoor on the computer so the attacker can commandeer the computer and use it at will to perform nefarious acts or scan file on the hard drive. This crime ware can reside on "breached" legitimate websites and is downloaded unknowingly to the victim's computer. Password stealing malicious code reached an all time high in January of 2006 according to the Anti-Phishing Working Group. Fig 3.

Phishing-based Trojans – Keyloggers, Unique Variants

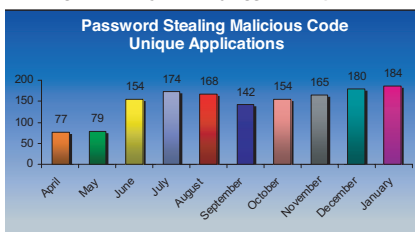


Fig. 3. APWG Phishing Activity Trend Report January 2006

Another pharming method which is becoming more prevalent involves an attacker sending out a worm that modifies the host file on a windows computer which will redirect legitimate requests from an online banking server to a fake one.

Regardless of whether the attack is phishing or pharming, they are becoming more sophisticated and the payload more damaging. The Internet provides a means for anonymous crime. Even if the perpetrator is caught, prosecution is difficult since many of the criminals are located in foreign countries.

Why should you care?

Everyone loses as a result of these attacks. When identity theft is the goal, it can take up to two years and several thousand dollars for a victim to recover. For a financial institution dollar losses can mount into the millions depending on the

nature of the attack and how wide spread the damage. Costs for financial institutions include:

- Reissuing credit and debit cards
- Notifying customers/members
- Reimbursement to customers/members
- Security implementation
- Anti-fraud program implementation
- Loss of customer/member confidence/trust
- Reputation damage
- Loss of actual customers/members

What is your reputation worth to you?

What do the regulators say?

As early as 2003, the FFIEC agencies were distributing guidance to financial institutions on email and fraudulent Internet related schemes.

- OCC Alert 2003-11 Customer Identity Theft: Email and Related Internet Fraud Threats
- FDIC FIL 27-04 Guidance on Safeguarding Customers Against Email and Internet Related Fraudulent Schemes, March 12, 2004
- NCUA Letter to Credit Unions 04-CU-05 Fraudulent Email Schemes
- OTS CEO Letter 193 Phishing and Email Scams March 8, 2004
- FFIEC Interagency Guidance FFIEC Phishing Brochure September 2004
- FDIC Putting an End to Account Hijacking Identity Theft December 14, 2004
- FDIC Identity Theft Study Supplement June 17, 2005
- FDIC FIL 64-2005 Guidance on How Financial Institutions Can Protect Against Pharming Attacks
- OCC Threats from Fraudulent Bank Web Sites July 1, 2005

The 2003 and 2004 email and Internet fraud guidance's were issued to raise financial institution awareness of phishing scams and warn against the risks associated with the scams. Management was instructed to consider prevention, detection, and response actions such as:

- Providing notification to customers and members about phishing
- Improve authentication methods
- Increase suspicious activity monitoring
- Enhance security for protecting confidential information
- Monitor for fraudulent web sites using variations of the institutions name
- Train customer, members, and staff regarding suspicious email requests
- Establish process for notifying Internet service providers, law enforcement, and regulators

The agencies also published a brochure with information to help consumers identify and combat phishing scams, the brochure is available on the FFIEC website (www.ffiec.gov) and advises consumers:

- Never click on a link provided in an email if there is reason to believe it is fraudulent.
- Do not be intimidated by email that warn of dire consequences for not following their instructions.
- If there is a question about whether the email is legitimate, go to the company's site by typing in a site address you know is legitimate.
- If you fall victim to a phishing scam, alert your financial institution, place fraud alerts on credit files, and monitor account statements.
- Report suspicious emails to the Federal Trade Commission.

In subsequent documents, the agencies address the risks with pharming attacks and provide general guidance on detection and prevention. The steps that are recommended include:

- The use of digital certificates
- Diligently managing domain names
- Monitoring for DNS poisoning, monitoring web server logs, and monitoring for email messages that have been returned to institution's email server
- Consumer education

What can you do?

If my recollection of history is correct, when the James Gang robbed the Northfield Minnesota Bank, the whole town knew they were coming. As a defensive strategy, the townspeople laid in wait for several days to ambush them as they rode into town. They were prepared, just as you should be by deploying layered security consisting of prevention, detection, and response strategies.

There is no one solution; no silver bullet when it comes to security, therefore, a defense in depth approach is required. Or in other words put as many obstacles in the way of the attacker as possible. While you may not be able to ensure 100% protection, you can significantly lessen the impact from these attacks. The responsibility for preventing and mitigating attacks is a responsibility that must be shared between the organization, the customer, and the service provider. Some of the steps you can take:

- Deploy strong authentication for users
- Authenticate your web site to the user
- Force users to log on to a HTTPS web page
- Use SSL
- Use digital certificates

- Monitor DNS registration
- Monitor for suspicious activity
- Keep logs
- Monitor online banking transactions
- Monitor website traffic
- Monitor website for vulnerabilities
- Use automated online solutions to monitor Internet activity and existence of phishing scams
- Use scanning tools to look at occurrences of the institution's name, logo or trademark
- Perform server log analysis to help detect suspicious activity that may indicate a phishing attack
- Monitor for DNS poisoning
- Monitor for intrusions
- Deploy anti-spyware tools
- Identify all machines connected to the Internet
- Perform port scans, ensure you know which ports are open and close all unused ports
- Utilize the most up-to-date patches
- Report suspicious activity and actual attacks

To achieve maximum effectiveness and efficiency you should consider automated monitoring and intrusion detection. Depending upon the expertise and resources you have in-house you may decide to implement and manage these solutions in-house. However, given the challenges with internally managing such solutions, you may look to outsource to a third party. Either way, you still have the ultimate responsibility for ensuring the security of your confidential information assets.

In addition to the security controls listed above, you also need to implement robust testing of the controls you have in place to ensure they are effective, and remain effective over time. You also need to implement customer and employee education programs. People need to be made aware of the threats and trained to not reply to emails,

phone calls, and pop-ups requesting personal information. FTC attorney Patricia Poss states that customers are less likely to respond to a phishing attack if they have heard of them. Inform your customers that you will never ask for personal information in an email and make sure they know not to click on a link provided in an email. Also, think through how you communicate with customers via email and what information you provide them and request from them.

You also need to be prepared by having an incident response plan for when an incident happens. You must have a road map of how to handle the situation efficiently, effectively, and timely. The first step would be to develop an incident response team, commonly referred to as a CIRT (Computer Incident Response Team). Next build a process for preparing for, addressing, and responding to the incident on a 24 X 7 basis. Identify what would constitute an attack, who has the authority to respond, what steps would be taken to contain the incident, mitigate the impact, and preserve the evidence. You also must have procedures for notifying customers/members, law enforcement, and the regulators.

Given the challenges such as language barriers, time zones, and forensic data documentation associated with responding to phishing and pharming attacks, outsourcing may prove to be the most effective and efficient method.

Next Steps

Make these threats a non-event for your institution by implementing mitigation strategies to lessen the impact when it does happen, and I say when as it is just a matter of time. Be proactive not reactive. The failure to do so could mean the difference between surviving an attack or succumbing to its devastating effects.

About the Author

Susan Orr is a leading financial services expert with vast regulatory, risk management, security best practice knowledge and expertise. During her 14 year tenure as a bank examiner, Susan held numerous lead positions including Regional IT Examination Specialist, Special Assistant to the Regional Director, Special Assistant to the Director of DSC, and Special Assistant to the Vice Chairman of the FDIC. Susan was also a lead instructor for the FDIC's technology school and was instrumental in key industry initiatives such as the FDIC E-Risk Strategic Initiatives Risk

Monitoring Committee, the Chicago Region Interagency Technology Group, and the Federal Financial Institutions Examination Council (FFIEC) IT Handbook rewrites. Prior to launching her consulting practice, Susan was Vice President of Regulatory Compliance at for an Internet security company where she advised staff, customers, and partners on regulation, security, and risk management. Susan retains close relationships within the FFIEC agencies as well as industry trade groups to stay abreast on new technologies, best practices, and regulatory issues.

Susan currently consults for several security providers and vendors as well as performs IT security and regulatory reviews for financial institutions. She also speaks regularly at risk management and security educational seminars and has authored numerous white papers on emerging information technology and security risk management topics. Susan is a Certified Information Systems Auditor (CISA), Certified Information Security Manager (CISM) and Certified Risk Professional (CRP).

