

Phishing and Pharming

*Providing multi-layered,
enterprise-wide protection from
phishing and pharming exploits*

Websense, Inc.
World Headquarters
10240 Sorrento Valley Road
San Diego, California 92121
USA
Tel: 800.723.1166 or 858.320.8000
Fax: 858.458.2950
www.websense.com

A b s t r a c t

Organizations face a complex challenge in securing their computing environment. Organizations and their employees are increasingly targeted in phishing attacks designed to steal proprietary company data and distribute malicious code. New pharming incidents also present increasing challenges that IT needs to address.

This paper describes phishing and pharming and explains how Websense® software can be used to combat them.

Websense filters at multiple points on the gateway, network, and endpoints to provide a comprehensive solution that provides organizations with complete protection against complex internet threats such as phishing and pharming.

Contents

Phishing	1
The objective is identity or data theft.....	1
Phishing targets businesses.....	2
Phishing targets government agencies.....	2
Phishes link to malicious websites.....	2
Phishing undermines consumer confidence.....	3
Pharming	3
Responding To These Security Challenges	4
The Answer – Websense Web Security Suite	4
Websense Security Labs™ Services	4
Phishing And Crimeware Map.....	5
Security Alerts.....	5
BrandWatcher™.....	5
Conclusion	6
About Websense, Inc.....	6

The objective is identity or data theft.

The term “phishing” first surfaced in 1996 when thieves stole America Online (AOL) accounts using email as a fishing “hook” to steal passwords from AOL users. Before 2003, phishers used email requests to solicit information from their targets. Many of these emails had spelling, punctuation, and grammar errors, which many discerning readers questioned. In late 2003, phishing ploys became more sophisticated. Hackers registered look-alike domain names and created valid-sounding—and looking—websites. Over the next couple of years, phishers started to incorporate stolen logos, language, and webpage designs to make their ploys appear even more legitimate.

Phishing ploys trick internet users into providing confidential details in response to an email. Although financial institutions have been raising public awareness of phishing by placing warnings on their websites, some customers are still deceived by spam emails inviting them to disclose account information.

*Javelin Strategy & Research estimates losses to phishing last year [2004] totaled \$367 million.**

Phishing is not restricted to email and user account credentials. Attackers also use instant messaging (IM), exploited websites, peer-to-peer (P2P) networks, and search engines to download and run keylogging malware or direct victims to websites which are fraudulent or may contain malware. The goal is no longer restricted to only username and password access to bank accounts. Social Security numbers, credit cards, passwords, logins and other confidential information are also being stolen.

Attacks also target businesses, sending phishes to employees who may click on links or respond to messages, assuming that their IT departments are protecting them from such unsafe activities.



Brief History of Phishing

- October 2003 Mmail email worm released, targeting the online payment service, PayPal
- December 2003 Anti-Phishing Working Group reports email fraud and phishing up 400% over the holidays
- January 2004 Department of Homeland Security, Internal Revenue Service, and Federal Deposit Insurance Corporation are targeted
- February 2004 Scams submit stolen account information to real site for authentication
- April 2004 Hackers learn to replace the URL of the phishing site with the URL of the company being impersonated in the victim's address bar
- June 2004 Phishers validate stolen credit card numbers with targeted bank or credit card company
- June 2004 Gartner Inc. reports that phishing cost businesses and consumers \$2.4 billion during the previous year.
- July 2004 Phishers use AIM (America Online's instant messaging program)
- October 2004 Scammers open legit-looking but fake online pharmacies, banks, and mortgage companies to steal credit card numbers
- January 2005 eBay users are sent an “Account Validation” message, which uses a ‘hijacked’ domain
- February 2005 Phishers target PayPal and several well-known banks
- April 2005 Convincing scam threatens loss of PayPal account privileges
- July 2005 The NCUA is used to try and phish anyone with an account at any Federal Credit Union

* As reported in BizReport, 11/18/04, and disclosed by the Anti-Phishing Working Group

* “Phishing: Consumer Awareness and Behavior”, June 2005

Phishing targets businesses.

A recent report focusing on employee web surfing habits disclosed that even with media attention on web-based threats, employees are still taking risks.* Of those who admitted to unsafe surfing, 63 percent acknowledged they took the risk because IT had installed security software on their computers. Meanwhile, 40 percent of risk-takers admitted they did so because IT was available to provide support if problems occurred. It is clear that employees are relying on their IT departments to protect them against web-based threats. It is also clear that organizations must educate employees about web-based threats while at the same time implement safeguards that can protect the organization and its employees.

A July study [of] 1,200 users, 400 each in the U.S., Germany, and Japan, [reported that] 39 percent of enterprise workers believe that their company's IT department would keep them safe from viruses, worms, spyware, spam, and phishing and pharming attacks. That confidence, whether on the mark or misplaced, leads workers to do risky, even stupid, things at work, such as opening questionable e-mail messages or clicking on unknown Web site links.

(TechWeb News, 14 September 2005)

"Your account information needs to be updated"

A typical phishing attack starts with a spoof email notifying the recipient that account information needs to be updated. If the phishing expedition is successful, the consumer clicks a link in the email as requested and connects with a spoofed website where sensitive information including account numbers, usernames, and passwords is hijacked.

Phishing targets government agencies.

As reported in *InformationWeek*, employees at federal agencies are finding themselves victims of phishing, pharming, and spyware scams. Phishers have targeted U.S. federal entities such as the Federal Bureau of Investigations (FBI), the Federal Deposit Insurance Corporation (FDIC), the Internal Revenue Service (IRS), and Regulations.com. Six of 24 agencies told the U.S. Government Accountability Office (GAO) that phishing attacks resulted in increased help-desk support and instances of compromised credit card accounts.

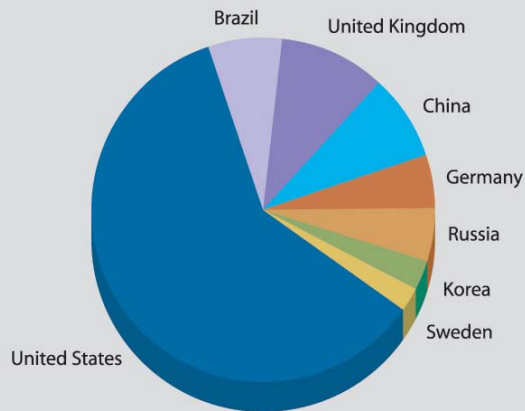
Phishes link to malicious websites.

In many phishing exploits, the linked-to websites look authentic and identical to the spoofed sites. These malicious websites often use international domain names to spoof the web addresses of legitimate sites. This exploit is a variation of a "homograph attack," taking advantage of loopholes in the way some popular web browsers display domain names that use non-English characters. Hackers use characters that resemble each other, for example, the letter "O" and the number "0" to fool users into thinking that a fraudulent website actually belongs to a legitimate company.

* TechWeb News, 14 September 2005

** Information Week, "Phishing and Pharming the Feds", 20 June 2005

Phishing Based Keylogger and Trojan Downloaders by Hosting Country



Anti-Phishing Working Group, "Phishing Activity Trends Report", June 2005

BrandWatcher™, included in the Websense® Web Security Suite™, notifies customers immediately if their brand, corporate identity, or website has been compromised.

Phishing undermines consumer confidence.

Corporate websites of valid, well-respected companies are being cloned to sell nonexistent products, or to get consumers to participate in money-laundering activities while believing that they are dealing with a legitimate organization. The public relations consequences for the company that has had its website cloned can be as severe as the financial losses.

Pharming

Because phishing is no longer as effective as it once was, fraudsters have developed "pharming," which is more difficult to detect. Pharming redirects users to fake sites when they try to access legitimate websites. A customer logs on, often using an address stored in his or her "favorites" folder, to what looks like a familiar internet banking site and is redirected to a fraudulent site.

Most pharming exploits use DNS wildcards and URL encoding to create email links that appear to be for legitimate sites. They actually send users to fake websites, where phishers try to steal confidential information, such as bank or credit account numbers.

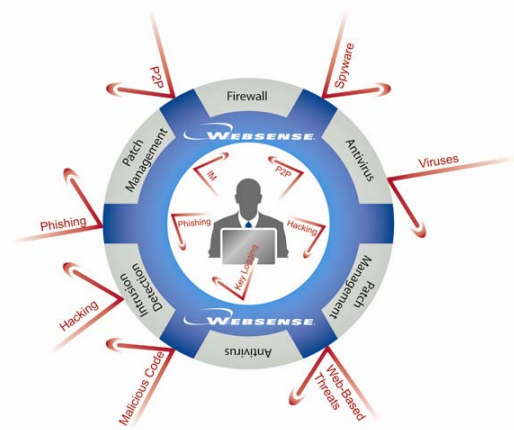
DNS wildcards, as in ".example.com," are typically used to guide mistyped emails to their intended destination.*

The spammed messages include a link that begins with a legitimate URL string but is followed by a long list of letters and symbols that encodes the bogus site's URL. These wildcard links are created at a third-party redirection service that then sends the user to the phisher's spoofed site instead of the desired URL. Once at the spoofed site, the victim can be deceived into entering account login info, which is then stolen by the hacker.

Responding To These Security Challenges

Most organizations rely on a combination of gateway firewalls and antivirus software to protect against web-borne threats. However, today's new computing threats like phishing and pharming are designed to bypass firewalls and antivirus solutions. While firewall technology has not changed much in the last few years, today's computing threats employ sophisticated techniques to bypass perimeter security. For example, many of these applications are able to communicate dynamically over different ports, thereby "hopping" right past static firewalls that block specific ports.

Firewalls can detect web traffic, but most have no means of monitoring the specific information being transferred. Spyware and other threats like P2P or instant messaging (IM) can penetrate firewalls. Since antivirus solutions are reactive, not preventive, they are effective only against known threats, and they provide even this limited protection only after an attack has already occurred. Organizations need content-level protection that complements firewalls and antivirus solutions.



WebSense complements traditional security solutions; it addresses the gaps in these traditional solutions, while creating a robust security solution spanning the gateway, network, and endpoints.

The Answer – WebSense Web Security Suite

WebSense Web Security Suite™ mitigates phishing threats by blocking access the phishers' malicious websites, thereby rendering the phishing attack harmless. WebSense Web Security Suite also blocks pharming URL redirect attempts. WebSense Web Security Suite provides an integrated web security solution that blocks spyware, malicious mobile code (MMC), and other web-based threats, as well as spyware and keylogger backchannel transmissions to their host sites. It also protects employees from phishing and pharming, and controls the sending and receiving of IM attachments. WebSense Web Security Suite provides real-time security updates for immediate protection from new security threats and includes award-winning web filtering technology, and robust reporting and analysis tools that provide organizations with complete information on user access to fraudulent sites or vulnerability to malicious code. WebSense Web Security Suite also includes the SiteWatcher™ and BrandWatcher services.

WebSense Security Labs™ Services

WebSense Security Labs researches malicious websites, phishing attacks, and other emerging threats associated with keylogging, spyware, IM attachments, and P2P applications. WebSense Security Labs mines and analyzes over 450 million sites a week for MMC.

The Security Labs team manages a honeynet of unprotected computers to discover new MMC, Trojan horses, keyloggers, and blended threats. Multiple honeypots on a network form a honeynet. A honeypot is a trap set to detect, deflect or in some manner counteract attempts at unauthorized use of information systems. It consists of computers, data or a network site that appears to be part of a network but which is actually isolated and protected, and which seems to contain information or a resource that would be of value to attackers.

The WebSense Security Labs findings are used to study techniques, actions, and behaviors on an enterprise network system. Information gained from the network of honeypots provides valuable information that enables WebSense Security Labs to discover attacks quickly and deliver a remedy to WebSense customers before antivirus signatures or other solutions are available, thus proactively protecting customers before an attack can affect them. With WebSense Security

Labs' early detection system, Websense provides a high degree of protection against rogue applications and new viruses to its customers, while delivering a valuable resource to the security community.

Phishing And Crimeware Map

The Phishing and Crimeware Map, located on the Websense Security Labs website (www.websensesecuritylabs.com), displays the most recent data collected by Websense Security Labs and provides a historical look into where phishing and crimeware related websites are hosted. Upon discovery, each site is investigated via its IP address to track the country of origin through the appropriate IP registrars and plotted on the map. The data is updated approximately 15 minutes after discovery.

Security Alerts

Websense Security Labs Alerts are email notifications sent to the security community and Websense customers, informing them of emerging threats and attacks as they are discovered. The alerts cover a variety of areas such as malicious websites, phishing attacks, keyloggers, and other web-based threats. These free email alerts provide links on the Websense Security Labs website with more comprehensive information about the threat, as well as remediation recommendations. The Websense Security Labs alerts are located at <http://www.websensesecuritylabs.com/alerts/>.

BrandWatcher™

A company's brand and reputation are one of its most valuable assets. Cyber criminals are capitalizing on consumer confidence in many well-known products and brands, using this trust to deceive users into divulging confidential account information. New brands are being targeted daily; Websense Security Labs has noted more than 1,500 reports of phishing attacks daily. As keylogging malicious code becomes more and more widespread, regional banks have become targets of these attacks, along with the larger, more well-known banks and ecommerce sites.

The BrandWatcher service, included in Websense Web Security Suite, lets customers know if their organization's website or brand has been targeted in a phishing or malicious keylogging code attack. This service provides the organization with security intelligence, including the attack details and other security-related information.

If the company's *website* has been spoofed, the BrandWatcher report will include information including where the site is hosted (IP address, URL, domain, etc.), the location of the site, the registered owner of the domain name and the address space, the status of the site (whether it is still up and running, for instance), and how widespread the reports are.

If the company's *brand* has been used in distribution of malcode, the attack information will include the source of the code, what the code does, and how widespread the distribution is.

Websense BrandWatcher™ Protects EDS Credit Union

Like many financial institutions, EDS Credit Union depends the internet as a self-service delivery channel for their customers' online banking needs. On June 21, 2005, EDS Credit Union's brand name was hijacked in a phishing attack.

In this attack, customers were asked to update their confidential account information once at the site, which had been damaged to closely resemble the authentic site, phishers attempted to steal confidential information such as passwords and social security numbers.

Less than 90 minutes after one of EDS Credit Union's customers received a phishing email, EDS Credit Union was alerted by Websense that their brand was being misused in a phishing scam. Websense then gave the company all of the security intelligence necessary to shut down the phishing website before any of EDS Credit Union's customers had "fallen for the phish."

Conclusion

Phishing and pharming attacks demonstrate how seemingly innocuous activities like opening emails and visiting trusted websites can be dangerous. When employees take risks—following links in emails, replying to IM requests, for instance—they expose the companies they work for to security and data theft risks.

It is critical to educate employees about these risks and also implement a reliable, robust content management solution. Websense Web Security Suite's three points of policy enforcement—at the internet gateway, the network, and at endpoints—offer multi-layered, content-level protection for the employee computing environment.

For more information and to download a free, fully functional 30-day evaluation, visit <http://www.websense.com/downloads>

About Websense, Inc.

Websense, Inc. (NASDAQ:WBSN), a global leader in web security and web filtering software, is trusted to protect 24 million employees worldwide. Websense proactively discovers and immediately protects customers against web-based threats such as spyware, phishing attacks, viruses and crimeware with maximum protection and minimal effort. With diverse partnerships and integrations, Websense enhances our customers' network and security environments. For more information, visit www.websense.com.

© 2006, Websense, Inc. All rights reserved. Websense and Websense Enterprise are registered trademarks of Websense, Inc. in the United States and certain international markets. Websense has numerous other unregistered trademarks in the United States and internationally. All other trademarks are the property of their respective owners.