Phishing - Threats and Countermeasures

Finjan White Paper

January 2007

For additional information, please visit www.finjan.com or contact one of our regional offices:

USA 2025 Gateway Place Suite 180 San Jose, CA 95110, USA Toll Free: 1 888 FINJAN 8 Tel: +1 408 452 9700 Fax: +1 408 452 9701 salesna@finjan.com	**Europe** 4th Floor, Westmead House, Westmead, Farnborough, GU14 7LP, UK Tel: +44 (0)1252 511118 Fax: +44 (0)1252 510888 salesuk@finjan.com
Chrysler Building 405 Lexington Avenue, 35th Floor New York, NY 10174, USA Tel: +1 212 681 4410 Fax: +1 212 681 4411 salesna@finjan.com	Alte Landstrasse 27, 85521 Ottobrun, Germany Tel: +49 (0)89 673 5970 Fax: +49 (0)89 673 597 50 salesce@finjan.com
Israel/APAC Hamachshev St. 1, New Industrial Area Netanya, Israel 42504 Tel: +972 (0)9 864 8200 Fax: +972 (0)9 865 9441 salesint@finjan.com	Printerweg 56 3821 AD Amersfoort Netherlands Tel: +31 318 693 272 Fax: +31 318 693 274

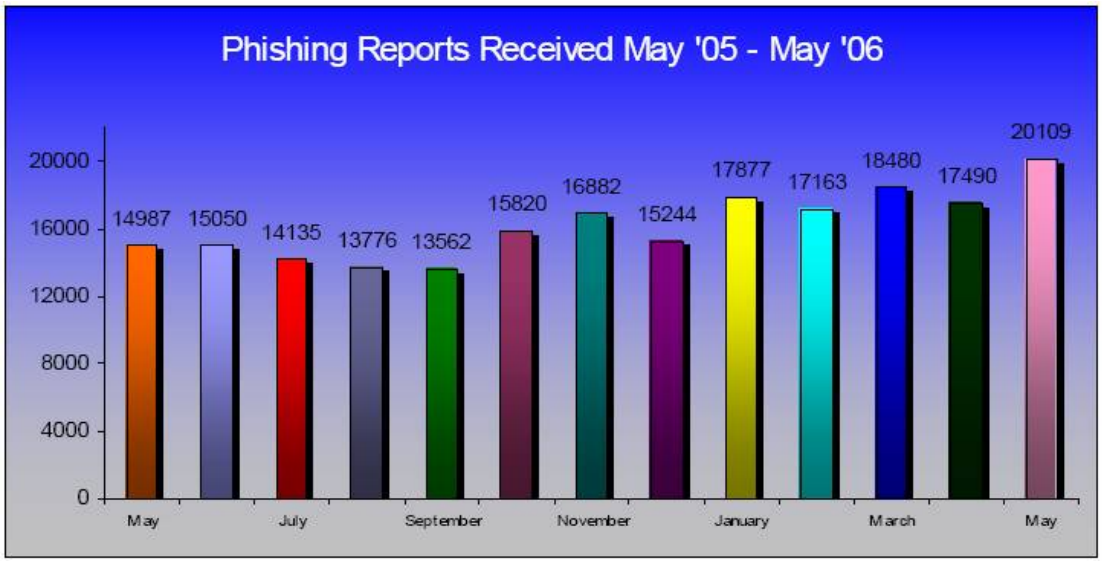
Email: info@finjan.com
Internet: www.finjan.com

Contents

Introduction

Phishing is one of the fastest growing scams on the Internet, compromising the personal details of millions of users worldwide. Typically instigated by professional hackers and criminal organizations, Phishing attacks use spoofed emails and fraudulent websites to deceive recipients into divulging personal financial data such as credit card numbers, account usernames and passwords, social security numbers, etc. As a result of these scams, an increasing number of consumers have suffered credit card fraud, identity theft, and financial loss. The exclusive motivation of phishers is financial gain.

According to Gartner, an estimated 2.4 million Americans were victims of Phishing attacks during the 12-month period ending in May 2005, resulting in financial losses estimated at $929 million. This threat continues to grow, as evidenced by the 34% increase in the number of unique Phishing attacks reported to the Anti-Phishing Working Group between May 2005 and May 2006.



Source: Anti-Phishing Working Group

The dramatic increase in reported incidents of Phishing is a major concern, given the growing dependence of businesses on the Internet. The main targets of Phishing scams to date have been large financial institutions, with the victims being individual users who were tricked into disclosing their personal details. However, it is only a matter of time before this threat reaches other types of businesses, such as telecommunications and utility companies, that deal with financially sensitive data on the Internet.

According to survey conducted by Entrust, 18% of the Americans who used to bank online, are planning to do it less frequently due to security concerns.

> *"Consumer confidence in online banking security has been damage. This is bad news for banks. If consumers start defecting from online banking to call centers or branches, this will put banks' costs up."*
> (Chris Voice, Vice President of Technology at Entrust)

> *"The continued rise in Phishing attacks shows increasing sophistication in strategy as well as more organized efforts among online criminals"*
> (Dave Jevans, Anti-Phishing Working Group chairman)

While Phishing targets individuals, it also presents a problem for corporations. If employees are not protected, enterprises could be held liable for not putting protections in place to prevent fraud. An attack could also result in employee login information being compromised, allowing a hacker to "log in" to an employee's network account and thus gaining access to confidential information.

Finjan delivers proactive web security solutions, featuring behavior-based technology that protects enterprises from known and unknown attacks arriving via the web. Finjan's **Anti-Phishing** solution provides superior protection against sophisticated Phishing attacks, without compromising an organization's productivity or performance. This solution uses multiple technologies to prevent Phishing attacks that can result in severe damages to both organizations and individuals.

What is Phishing?

Phishing is a combination of "social engineering" and "technical subterfuge" to steal consumers' personal identity data and financial account credentials. A spoofed email is sent to a large group of people, from an address that appears to be from their bank or some other legitimate institution. The email typically is worded to instill a sense of urgency, and to elicit an immediate response from the recipient, e.g., verify your account details or your account will be closed. The email usually contains a link to an online form that is branded to look exactly like the organization's website. The form will usually ask for sensitive details such as passwords, social security numbers, credit card details, etc. Until recently most phishers used the names of financial institutions (i.e., banks) to deceive people into giving away their account information. They also have started to use the names of other organizations such as eBay, Apple, etc.

In many cases, after giving up personal and financial information on a Phishing site, the victim is redirected to the real homepage of the company being targeted. Experts say this psychological trick helps erase doubts that victims may harbor about the veracity of the experience and allows more people to be swindled. From the user's perspective, the entire experience is transparent. In many cases, the user might never be aware that his/her details have been stolen.

There are a number of methods used by fraudsters in Phishing scams:

- Deception Methods (most prevalent method)
- Crimeware – Malicious Software (Trojan, Spyware)
- Keyloggers

Deception Methods

Spoofed Websites

Most often, consumers are directed to the fraudulent site by spam email designed to look like it came from well known organizations or institutions, such as Google or Citibank, or popular ecommerce companies. Each attack contains up to several million email messages designed to lure people to disclose personal information.

Phishing emails usually direct consumers to websites that are indistinguishable from legitimate ones. Some Phishing emails will deliberately replace characters or misspell words in the subject line in an attempt to bypass anti-spam filters.

Some examples of Phishing deception methods are provided below:

- Some Phishing emails use plain text email, or HTML emails, with fake/spoofed links often made to look like secure HTTPS websites. For example, the link title in the email could be:
  https://bankfinance/cgi/?verifyinformation
  But will actually point to the following URL:
  http://blabla.mydomain.com%69%6E%64%65%78%75%70%64%61%74%65%79%6F%75%72%69%6E%66%6F%72%6D%61%74%69%6F%6E%73%65%63%75%72%65@%36%31%2E%39%38%2E%37%30%2E%32%30%38:%34%32%31%31/%64%6C%6C/%69%6E%64%65%78%2E%68%74%6D
  The real address is not on the financial institution's server but rather on the phisher's spoofed site:
  http://blabla.mydomain.comindexupdateyourinformationsecure@61.98.70.208:4211/dll/index.htm

- Direct consumers to web sites that are indistinguishable from legitimate ones. The designers of these fraudulent sites select domain names that closely resemble those of the real sites.
  http://www.hotmail.hackerguy.nickelandimehosting.com
  http://www.evenlargerbank.money.nickelandimehosting.com
  http://www.bloatedcorp.lackey.nickelandimehosting.com

- Replaces web browser address bar with a working fake, using JavaScript.
  This technique allows the scammers to display a completely fraudulent web address URL, while taking the consumer to the phisher's spoofed site. This method was used in a well-known Phishing attack against Citibank (see example below).

- Use Internet Explorer (IE) vulnerabilities to hide real address

  - **Vulnerability 1:** There is a flaw in the way that Internet Explorer displays URLs in the address bar. By opening a specially crafted URL an attacker can open a page that appears to be from a different domain from the current location.
    By opening a window using the http://user@domain nomenclature an attacker can hide the real location of the page by including a non printing character (%01) before the "@". Internet Explorer doesn't display the rest of the URL making the page appear to be at a different domain.
    <button onclick="location.href=
    unescape('http://www.microsoft.com**%01**@zapthedingbat.com/security/ex01/vun2.htm');" >Test Exploit</button>

- **Vulnerability 2:** %@2F in URL is decoded when IE calculates the domain, but not decoded while downloading a page.
  So, for example, http://www.yahoo.com**%2F**@www.cnn.com/liudieyu
  leads to www.cnn.com/liudieyu instead of www.yahoo.com, and the domain of it www.yahoo.com for IE

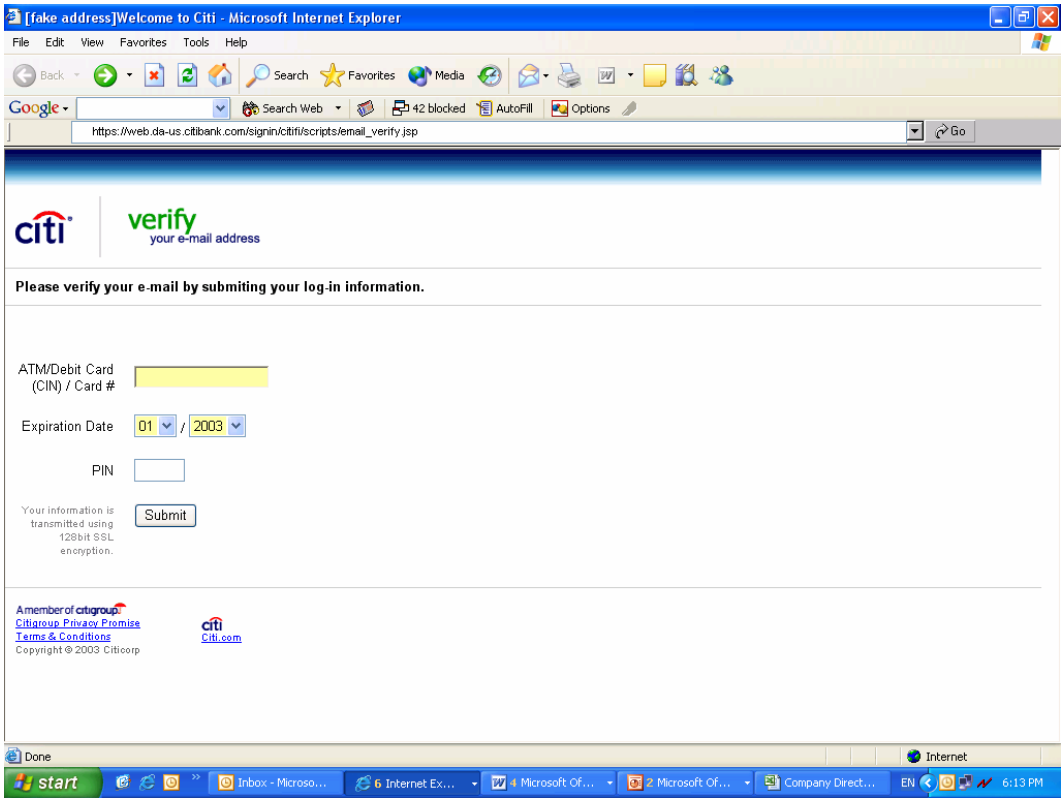
Examples of Phishing Attacks

The following examples illustrate some of the clever deception methods used in well known Phishing scams, with which many of us are probably familiar from our everyday email experiences.

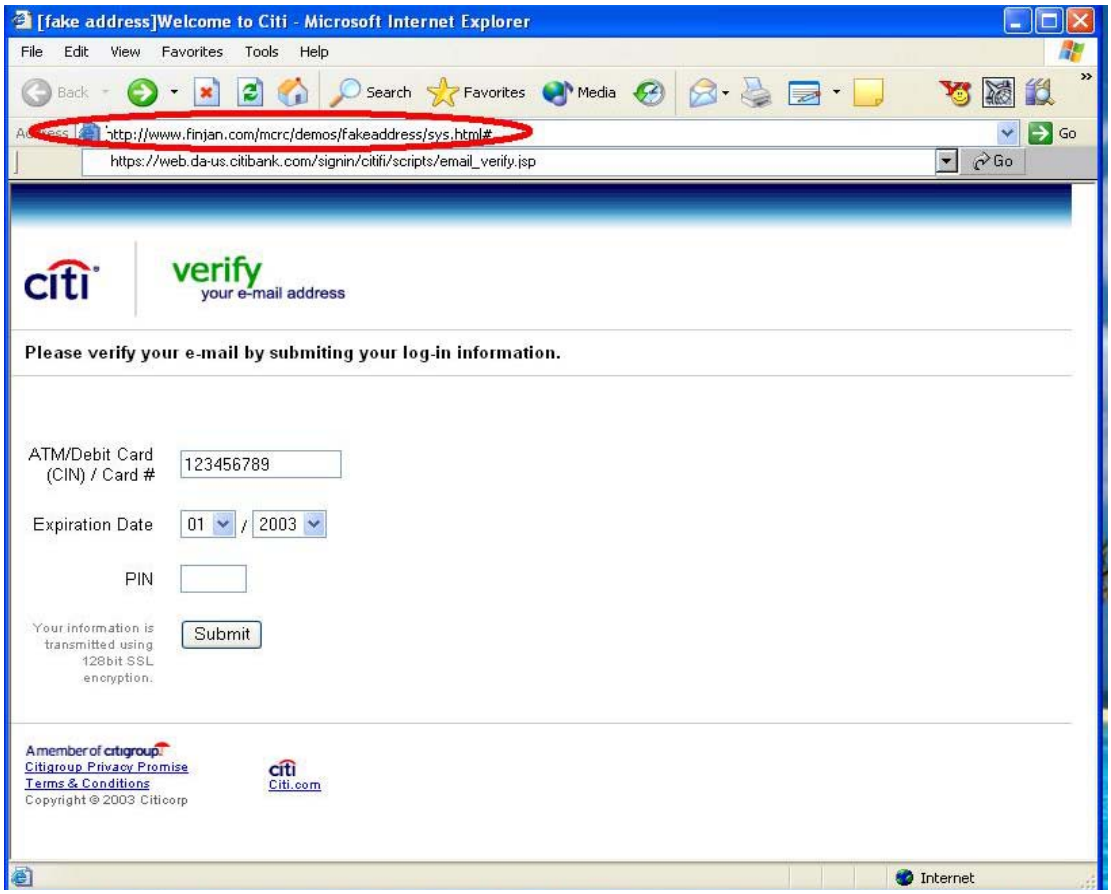
EXAMPLE 1 - CITIBANK

1. In this example, the recipient received an email with a spoofed address, containing a message designed to entice the recipient to click on a provided link. The links and branding within the email look completely genuine.

2. By clicking on the link provided, the user arrives at the page shown below, which appears to be a secure HTTPS website. The phisher hides the real address of the site by exploiting an Internet Explorer vulnerability related to non-printing characters.



3. By right-clicking on the toolbar and ticking “Address bar”, the true address bar is revealed. As illustrated in the screen below, this is really a non-secure HTTP site with a fake address.



4. Finjan technology recognizes the JavaScript that tries to get personal information and blocks it .

EXAMPLE 2 - Westpac Bank (Australia)

From: Westpac Bank Report [mailto:support@westpac.com.au]
Sent: 03 April 2004 22:58
To: Sales
Subject: Notification on transfer from your Westpac bank account

Dear user!
We are informing you that today, the amount of $973.00 AUD has been drawn out of your account.
Technical assistance of Westpac Bank.
<http://www.westpac.com.au>

The above email was sent with the bank's logo, and uses social engineering to get the user to click on the link. Apparently, spamming techniques were used to get the email out to as many people as possible.

They do not tell the user to do anything, just that $973 was transferred from their account.

When the user clicks on the link, it sends them to a web site which automatically redirected them to the real Westpac bank site. At this point they would have entered their user name and passwords, etc. and seen all of their normal bank account details such as utility bills, cheques and cash point withdrawals.

What they did not see was the "staging" web site had some embedded JavaScript, the same type of code as used by banking applications, that downloaded a keylogger which then recorded their user name and password details, and sent this on to another website, evidently in Russia.

It is interesting to note that the Phishing website was taken down within about an hour of the attack being launched, since the phishers knew that the majority of victims were going to get caught in the first hour or so, and that each subsequent hour would increase their chances of getting caught and/or located.

EXAMPLE 3 – SunTrust Internet Banking

The following is an excellent example of the use of social engineering in Phishing scams. The email from SunTrust Internet Banking informs customers that it is waiving monthly fees. All the customer needs to do in order to enjoy this saving is to click on a link and then verify an email address. It is interesting to note than within a few days after its appearance the fraudulent Phishing site used in this scam no longer existed.

From: SunTrust [mailto:support@suntrust.com]
Sent: 28 November 2004 01:19
To: Saleseu
Subject: Internet Banking with Bill Pay Fees Waived

Dear SunTrust Bank Customer,
SunTrust Internet Banking with Bill Pay has become even better. We are waiving monthly fees for SunTrust Internet Banking with Bill Pay and SunTrust PC Banking with Bill Pay for all our clients.
As an additional security measure, you need to activate this new feature by signing on <http://82.90.165.65/s> to Internet Banking. Please verify your preferred email address and the information that SunTrust uses to confirm your identity.
In the Update Internet Banking service area you can also view the accounts you currently have tied to your Internet Banking service, to view whether Bill Pay is enabled on a particular account, and to request other accounts to be added to your Internet Banking service.
To do so, simply sign on <http://82.90.165.65/s> to Internet Banking.

SunTrust Internet Banking

Malicious Software (Crimeware)

Using Trojans to Redirect Users to Fraudulent Site

This method uses Trojans to modify a user's DNS or host files in order to redirect a specific site to a fraudulent server. A spoofed email is sent to a large group of people; the email includes a link to download an executable (e.g., Trojan horse which modifies the DNS server of the specific workstation). From that point on, all requests to access this specific site will be redirected to a spoofed site (e.g., redirecting paypal.com to a spoofed site in Romania that looks identical to the original paypal.com site). The user will not be able to notice the difference because the web address (URL) will be the correct one. Most likely the spoofed site will ask the user to update his/her account details and financial data.

TINI is an example of an infamous Trojan, whose footprint is only 3KB in size and therefore is often associated with small files. When executed, this Windows Trojan silently listens on its preconfigured TCP port for incoming connections. When the Trojan receives an inbound connection from an attacker to its port, it opens a command prompt and allows the attacker to execute any command on the infected machine.

Finjan's web security solutions identify any attempt to download Trojans such as TINI, and block the download session. Instead of being infected with the Trojan, the end-user receives a blocked page with an explanation of why the page was blocked.

Phishing Using Keyloggers (Spyware)

Phishers have programmed commercial websites to deliver keyloggers to any innocent user who visits these websites. Taking advantage of known vulnerabilities, the attacker installs software which downloads and runs malicious programs on the PCs of website visitors.

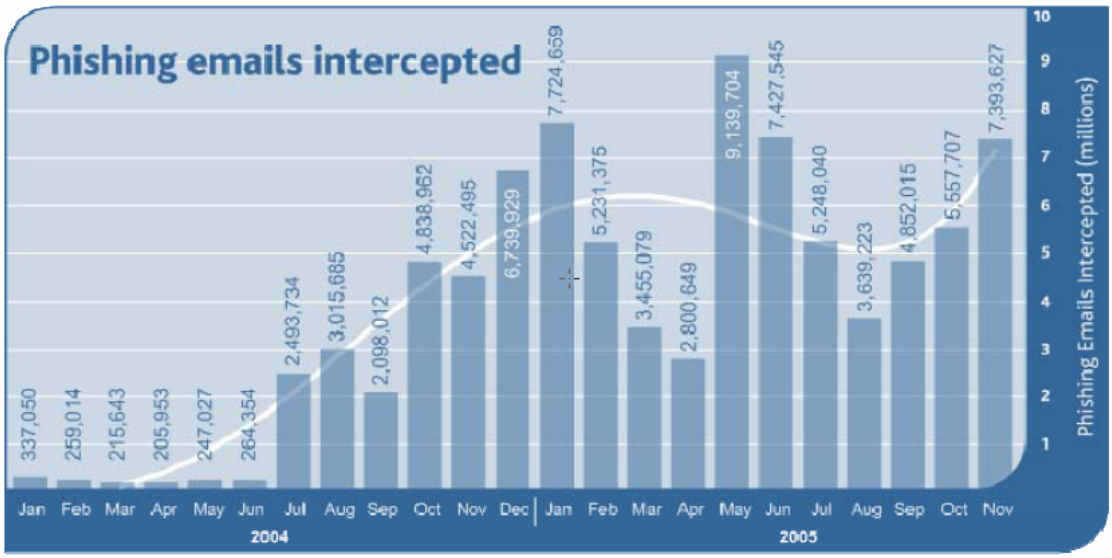
According to the Anti-Phishing Working Group, the ShangHai Huizhong Automotive Manufacturing (SHAC) website was a victim of such an attack. An IFRAME was added to the bottom of the site's home page. It tried to use a Microsoft® Internet Explorer CHM (compiled Windows HTML Help file) exploit that allows malicious code to be downloaded and run without user intervention. The website, which was hosted in Australia, downloaded a file called "help.txt", which is not a text file but a CHM Windows® Help file. This malicious Windows Help file dropped another file called fu**snow.exe, which was packed with a packing system called UPX (Ultimate Packer for Executables). That file in turn uses several built-in Windows APIs to connect to the Internet, open a back door, and install the keylogger.

Another type of Spyware used in Phishing scams is Internet Dialers. These dialers are applications that terminate the current connection to the Internet and instantly establish a new connection by typically dialing to highly charged international phone numbers. Usually associated with pay porn sites, these dialers are also referred as "sex dialers".

Finjan can analyze the behavior of applications arriving from the web and determine whether they violate the security policy as defined by the network administrator. Since Internet Dialers are installed as files on the victim machine and communicate over the network, their behavior can be easily identified and blocked.

What Is the Scope of This Threat?

Clearly, Phishing continued to be one of the major threats in 2005. According to online security services firm MessageLabs, the quantity of Phishing email as a proportion of all emails received increased from 1 out of 943 emails in 2004 to 1 out of 304 emails in 2005 (the peak was January 2005 when 1 out of every 126.5 emails was a Phishing email). (MessageLabs 2005 Annual Report).

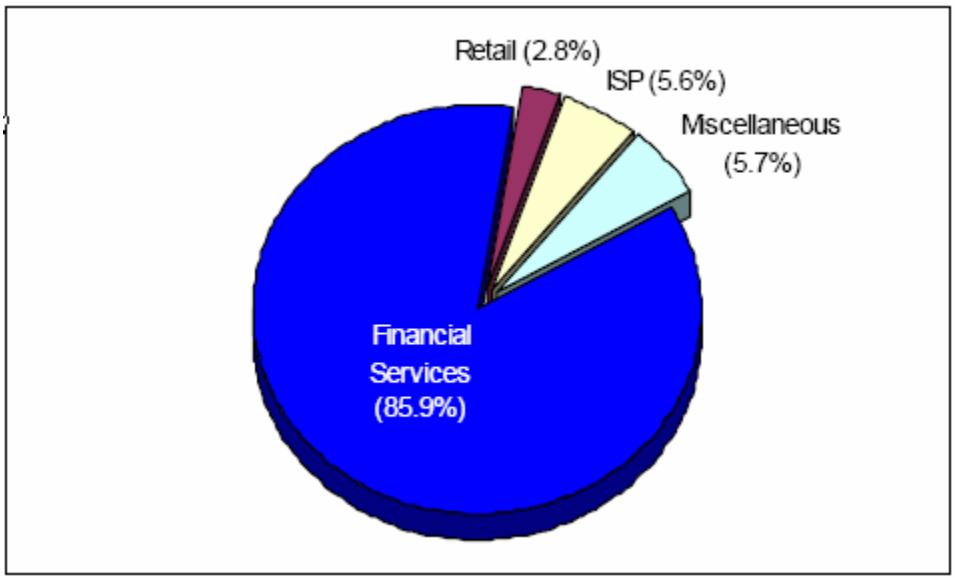


Source: MessageLabs 2005 Annual Report

By hijacking the trusted brands of well-known institutions, Phishing scams generally succeed to elicit a response from 5% of the recipients. Accordingly, a mailing to 30 million people where only 20% of the mail is successfully delivered and only 1% of those people have accounts with the organization will result in the fraudulent acquisition of personal details for 600 people.

Exact statistics on the number of Phishing attacks are difficult to ascertain, however the growth trend is clear. As noted above, the Anti-Phishing Working Group (APWG) reported an almost 100% increase of Phishing attacks on November 2005 as compared to November 2004.

Financial sector companies (e.g., banks, credit card companies and other financial institutions) were the leading targets of phishers in 2005, accounting for over 85% of all Phishing attacks, according to Anti-Phishing Working Group – H1/2005.



Source: Anti-Phishing Working Group

Why Traditional Security Solutions Alone Are Not Effective

Traditional security solutions were built in the 1990's to safeguard against email attachments and less sophisticated threats than those delivered via Active Content (e.g., JavaScript). Today's attacks take advantage of vulnerabilities in web browsers, which offer more opportunities for malicious/inappropriate behavior.

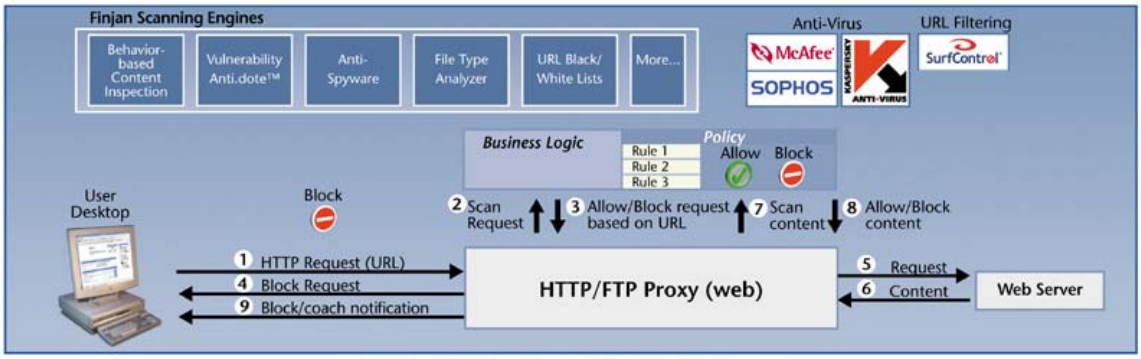
The traditional solutions are reactive in nature and thus are not sufficient for combating threats driven by Active Content, such as JavaScripts. Configuring the settings of Internet browsers and other products in light of past exploits, deployment of firewalls and using traditional anti-virus software do not address today's need for analyzing and restraining the behavior of Active Content, according to an organizational security policy.

Moreover, since the common deception methods utilize scripts, the only way traditional tools can prevent this form of deception is by disabling JavaScript in the browser settings. However, as most web pages today utilize these standard tools, this is highly impractical. It is precisely this challenge that underlies the need for behavior-based security solutions.

Finjan's Unique Behavior Based Solution

Finjan's **Vital Security™** solutions close the Window-of-Vulnerability™ using patented behavior-based technology that protects companies from new, unknown attacks driven by Active Content. Finjan's unique solutions leverage this technology to analyze content, determine the type of behavior and proactively block malicious or inappropriate content, while allowing appropriate content to flow in a transparent manner.

Finjan's behavior-based technology determines the full set of behaviors that a given piece of content will exhibit when loaded into the target application, e.g. a web browser. Then, in accordance with each organization's specific security policy, Finjan's system decides whether to pass, block or neutralize the content, ensuring no inappropriate or malicious content can enter the network.



Finjan's Proactive Behavior-Based Content Inspection Workflow

Finjan's scanning technologies inspect the application level traffic that might carry the malicious content which can infect the computers, and analyzes the behavior of the code itself - **before** it even begins to run on the target computer. Finjan's behavior-based content inspection identifies the combinations of operations, parameters, script manipulations and other exploiting techniques, and can determine that a piece of mobile code is trying to exploit one or more types of vulnerabilities.

With a field-proven track record, Finjan's unique **behavior-based technology is the only available solution capable of effectively combating new and unknown threats driven by Active Content, such as Phishing, Spyware, Trojans and other types of malicious code.**

How Finjan Protects Users Against Phishing

Finjan offers the world's best and most comprehensive web security appliances for businesses and organizations, ensuring zero-hour protection against unknown and known threats (e.g., Spyware, Phishing, viruses, worms, and Trojans). Our proactive appliance-based solutions deliver the most effective shield against web-borne threats, freeing enterprises to harness the web for maximum commercial results.

Finjan's **Anti-Phishing** solution, which is an integral part of the Vital Security™ Web Appliances, combines Finjan's patented behavior-based technology with industry-leading URL Filtering engines to provide superior protection against Phishing attacks. Finjan's **Anti-Phishing** solution identifies malicious Active Content in the message, as well as the associated URL from which it came, and blocks it at the gateway, thus ensuring full protection against Phishing attacks using the following methods.

Organizations with email security may also be able to prevent a portion of Phishing emails from reaching the end user. In cases where the email gets through, Finjan's web security solutions can identify the Active Content that tries to copy the user's personal information and block it at the gateway.

The following specific features in Finjan's products are used to combat Phishing:

- Scanning for known hacking techniques, such as replacing the web browser address bar with a fake one, and proactively blocking such attempts
- 3rd party URL Filtering engine categorizes known Phishing sites and blocks users from accessing them (limited effectiveness as Phishing sites are typically brought down soon after an attack to avoid detection)
- If the fraudulent site also contains malicious code or crimeware (e.g., Trojan, Spyware) inside the web pages, such code is detected and blocked by Finjan's behavior-based code analysis
- Many users are not familiar with browser warnings about problematic certificates or certificate violations and can be fooled into a Phishing attack. When deployed with Finjan's optional SSL Inspection module, this solution protects against Phishing attacks that use invalid, revoked or otherwise problematic certificates by enforcing your organization's certificate policies at the gateway.
- Phishing attacks that use SSL-encrypted content are invisible to most standard gateway scanning applications. Finjan's optional SSL Inspection module decrypts the SSL-encrypted content so that it can be scanned for malicious behavior by our web scanning applications

Conclusion

The continuing growth in the number of Phishing scams is a serious concern for the entire Internet community. Any individual with access to email or performing on-line business transactions is a potential victim of a Phishing attack. As time goes by, these Phishing scams are becoming more sophisticated and use smarter deception methods. Some phishers have also begun to use Trojans and Spyware, such as keyloggers, to capture information entered at legitimate web sites, such as on-line banking sites.

Phishing attacks exploit Active Content to take advantage of vulnerabilities in web browsers, which offer a plethora of opportunities for malicious/inappropriate behavior. Traditional security solutions, originally designed to safeguard against email attachments and less sophisticated threats, are reactive in nature and thus are not sufficient for combating complex threats driven by Active Content, such as JavaScripts. The sophistication of today's attacks requires an intelligent solution that can analyze the actual behavior of that content and determine whether it is malicious/inappropriate or appropriate.

Utilizing its patented behavior-based technology, Finjan offers the ONLY proactive web security solution that effectively repels all types of threats driven by Active Content, such as Phishing, Spyware, Trojans and other malicious code. By detecting and stopping known and unknown malicious attacks before they enter the corporate network, sensitive data remains secure, business operations are continuous and the costs associated with security incidents are minimized. Finjan's solutions allow organizations to harness the web for maximum commercial results, without security worries.

About Finjan

Finjan is a global provider of best-of-breed web security solutions for businesses and organizations, protecting millions of users from known and unknown threats. Finjan uses its patented behavior-based security technologies to determine actual code behavior and block any action that violates an organization's predefined security policy, therefore surpassing the levels of defense offered by reactive and signature-based anti-virus and intrusion detection solutions. This superior technology enables Finjan to proactively repel all types of web-borne attacks, securing businesses against known, unknown and emerging threats. Finjan's security solutions have received industry awards and recognition from leading analysts and publications including IDC, Butler Group, SC Magazine, PCPro, ITWeek, and Information Security. For more information about Finjan and its proactive protection solutions against threats driven by mobile malicious code, please visit: www.finjan.com.

