



WHITE PAPER

---

## Fraud Alert: Phishing — The Latest Tactics and Potential Business Impact





**CONTENTS**

+ Introduction	3
+ Phishing Knows No Limits	3
+ Be Aware of the Latest Phishing Schemes	4
Speare Phishing	4
Business Services Phishing	4
Phishing that Plays on Economic Fears	4
Blended Phishing/Malware Threats	4
Man-in-the-Middle SSL Stripping	5
Texting and Mobile Phone Phishing Scams	5
+ How Phishing Could Impact Your Business	5
+ Protecting Your Business	5
Consumer and Employee Education	7
+ Conclusion	7
+ Glossary	7
+ Learn More	7
+ About VeriSign	7



# Fraud Alert: Phishing — The Latest Tactics and Potential Business Impact

## + Introduction

As one of the top cyber crime ploys impacting both consumers and businesses, phishing has grown in volume and sophistication over the past several years. The down economy is providing a breeding ground for new, socially-engineered attempts to defraud unsuspecting business people and consumers. With honest money-earning avenues less available, the cyber crime ecosystem is ready with off-the-shelf phishing kits. It no longer takes a hacker to enable and commit fraud on the Internet — anyone with a motive can join in.

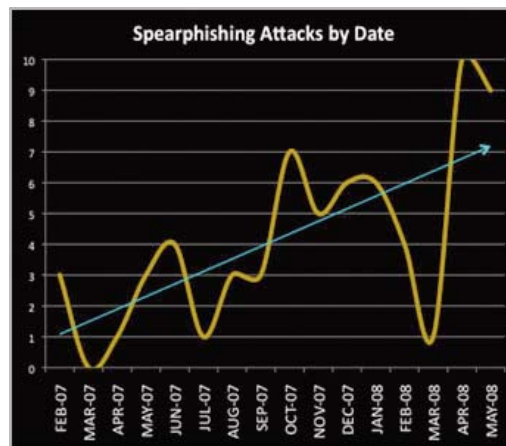
The potential impact on a business can be great — whether an employee or its customers have been phished, or the company Web site has been compromised. Organisations need to stay current on the latest methods employed by cyber criminals and proactively take steps to prevent this type of fraud.

This fraud alert highlights the current growth and trends in today’s phishing schemes, the potential impact on companies, and insight into how businesses can apply technology to protect themselves and their customers.

## + Phishing Knows No Limits

Phishing — luring unsuspecting users to provide sensitive information for identity or business theft — is a serious threat for both consumers and businesses. In the last decade since phishing arrived on the scene, this fraud method has been growing rapidly, with one estimate citing approximately 8 million daily phishing attempts worldwide.<sup>1</sup>

Figure 1. Spear-Phishing Attacks on the Increase



1. “Counterfeiting & Spear Phishing — Growth Scams of 2009,” Trade Me, *Infonews.co.nz*, March 2, 2009

*VeriSign®iDefense®— security intelligence teams which identify, verify, and track global threats and vulnerabilities — reported that in May 2008 more than 2,000 victims were compromised with spear phishing e-mails claiming to come from the U.S. Internal Revenue Service, the United States Tax Court, and the Better Business Bureau.*

The Anti-Phishing Working Group (APWG) reported that unique phishing attacks submitted to APWG rose 13 percent during the second quarter of 2008 to more than 28,000.<sup>2</sup> It also reported that, during the same period, the number of malware-spreading URLs infecting PCs with password-stealing code rose to a new record of more than 9,500 sites — a 258% increase compared with the same quarter in 2007. Figure 1 shows one area of phishing — spear phishing — and its growth over a 16-month period.

## + Be Aware of the Latest Phishing Schemes

### Spear Phishing

Targeted versions of phishing, called spear phishing, have emerged over the past several years. While common phishing is indiscriminate in its targets, spear phishing targets are known customers of a specific bank, mortgage provider, or other type of organisation.

Consumers aren't the only targets of spear phishing. Increasingly, corporate employees are being targeted by savvy criminals. In these attacks, the goal is to gain access to corporate banking information, customer databases, and other information to facilitate cyber crime. According to VeriSign iDefense, spear phishing against corporations reached new heights during April and May 2008. Many of these attacks target senior executives and other high-profile individuals. The victim counts from these attacks is staggering — over 15,000 corporate users in 15 months. Victims include Fortune 500 companies, government agencies, financial institutions and legal firms.

### Business Services Phishing

In addition to spear phishing targeted at employees, there have been recent schemes targeting businesses using services such as Yahoo! or Google AdWords. PhishTank reported that AdWords customers were sent e-mails alerting them that their accounts required updating. The account holder was encouraged to log into the spoofed AdWords interface and then provide credit card information.<sup>4</sup> With many small and mid-size companies relying on online advertising to drive traffic to their sites, their marketing managers could be easy prey for this type of phishing scam.

### Phishing that Plays on Economic Fears

Today's economic turmoil delivers unprecedented opportunities for criminals to exploit victims. For instance, popular scams include phishing e-mails that look like they are coming from a financial institution that recently acquired the target victim's bank, savings & loan, or mortgage holder.<sup>5</sup> The large amount of merger and acquisition activity taking place creates an atmosphere of confusion for consumers, exacerbated by the dearth of consistent communications with customers. Phishers thrive in this type of situation.

### Blended Phishing/Malware Threats

To increase success rates, some attacks combine phishing with malware for a blended attack model. For instance, a potential victim receives a phishing e-card via e-mail that appears to be legitimate. By clicking on the link inside the e-mail to receive the card, the person is taken to a spoofed Web site which downloads a Trojan to the victim's computer. Alternatively, the victim may see a message that indicates a download of updated software is needed before the victim can view the card. When the victim downloads the software, it's actually a keylogger.

2. "Phishing Activity Trends Report, Q2 2008," Anti-Phishing Working Group, November 2008

3. [www.antiphishing.org](http://www.antiphishing.org)

4. "PhishTank April '08 Stats. Learn to protect yourself, your company," PhishTank, May 5, 2008

5. "FTC Consumer Alert: Bank Failures, Mergers and Takeovers: A Phish-erman's Special," [www.ftc.gov](http://www.ftc.gov)

*“...End users are still falling for phishing attacks that are often combined with malware-based attacks. We also know that fraud losses are increasing, which is why there is so much demand for security and fraud detection products.”*

— Avivah Litan, Vice President and Information Security Analyst, Gartner<sup>7</sup>

*Damage caused by cyber crime is estimated at \$100 billion annually according to the Organisation for Security and Cooperation in Europe.<sup>8</sup>*

Phishing-based keyloggers have tracking components which attempt to monitor specific actions (and specific organisations such as financial institutions, online retailers, and e-commerce merchants) in order to obtain sensitive information such as account numbers, userids, and passwords.

Another type of Trojan that enables phishers to capture sensitive information is a redirector. Redirectors route end users' network traffic to a location where it was not intended to go. The APWG is seeing significant increases in both phishing-based keyloggers and redirectors.<sup>6</sup>

#### Man-in-the-Middle SSL Stripping

During 2008, a new type of malware was introduced that allows cyber criminals to spoof an encrypted session. This is a variance on the standard man-in-the-middle (MITM) attack that criminals use to access passwords or sensitive information passing unprotected over the network.

#### Texting and Mobile Phone Phishing Scams

Posing as a real financial institution, phishers are using SMS as an alternative to e-mail to attempt to gain access to confidential account information. Known as “smishing”, the typical scam informs the mobile phone user that the person's bank account has been compromised or credit card/ATM card has been deactivated. The potential victim is directed to call a number or go to a spoofed Web site to reactivate the card. Once on the site, or through an automated phone system, the potential victim is asked for card and account numbers and PIN numbers.

### + How Phishing Could Impact Your Business

While the financial industry continues to be a primary target for phishers, it's certainly not the only sector vulnerable to attack. Auction sites, payment services, retail, and social networking sites are also frequent targets. The APWG also reports a massive increase in attacks aimed at cell phone providers and manufacturers. In short, no business or brand is inherently safe.

Phishing attacks that pose as a company's official Web site diminish the company's online brand and deter customers from using the actual Web site out of fear of becoming a fraud victim. In addition to the direct costs of fraud losses, businesses whose customers fall victim to a phishing scam also risk:

- A drop in online revenues and/or usage due to decreased customer trust
- Potential non-compliance fines if customer data is compromised

Even phishing scams aimed at other brands can impact a business. The resulting fear caused by phishing can cause consumers to stop transacting with anyone they can't trust.

### + Protecting Your Business

While there is no silver bullet, there are technologies that can help protect you and your customers. Many of the current phishing techniques rely on driving customers to spoofed Web sites to capture personal information. Technology such as Secure Sockets

6. “Phishing Activity Trends Report Q2 2008.” Anti-Phishing Working Group, [www.antiphishing.org](http://www.antiphishing.org)

7. “Report: Phishing a Low-Paying, Low-Skills Job,” Kelly Jackson Higgins, *DarkReading*, January 7, 2009

8. “Experts: Cyber-crime as Destructive as Credit Crisis,” Reuters, [eWeek.com](http://eWeek.com), November 19, 2008

Layer (SSL) and Extended Validation (EV) SSL are critical in fighting phishing and other forms of cyber crime by encrypting sensitive information and helping customers authenticate your site.

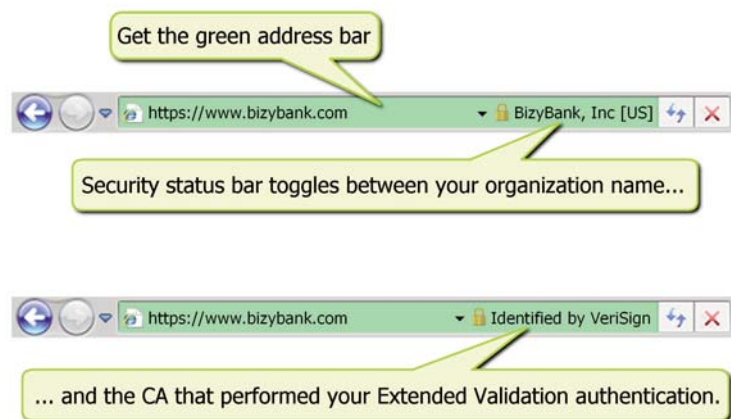
Security best practices call for implementing the highest levels of encryption and authentication possible to protect against cyber fraud and build customer trust in the brand. SSL, the world standard for Web security, is the technology used to encrypt and protect information transmitted over the Web with the ubiquitous HTTPS protocol. SSL protects data in motion which can be intercepted and tampered with if sent unencrypted. Support for SSL is built into all major operating systems, Web browsers, Internet applications, and server hardware.

To help prevent phishing attacks from being successful and to build customer trust, companies also need a way to show customers that they are a legitimate business. Extended Validation (EV) SSL Certificates are the answer, offering the highest level of authentication available with an SSL Certificate and providing tangible proof to online users that the site is indeed a legitimate business.

EV SSL gives Web site visitors an easy and reliable way to establish trust online by triggering high security Web browsers to display a green address bar with the name of the organization that owns the SSL Certificate and the name of the Certificate Authority that issued it. Figure 2 shows the green address bar in Internet Explorer.

The green bar shows site visitors that the transaction is encrypted and the organisation has been authenticated according to the most rigorous industry standard. Phishers can then no longer capitalise on visitors not noticing they are not on a true SSL session.

Figure 2. The Green Address Bar Triggered by an EV SSL Certificate



While cyber criminals are becoming adept at mimicking legitimate Web sites, without the company's EV SSL Certificate there is no way they can display its name on the address bar because the information shown there is outside of their control. And they cannot obtain the legitimate company's EV SSL Certificates because of the stringent authentication process.

### Consumer and Employee Education

In addition to implementing EV SSL technology, businesses should continue to educate their customers and employees on safe Internet practices and how to avoid cyber fraud. Teach them how to recognise the signs of a phishing attempt such as: misspellings (less common as phishers become more sophisticated), generic greetings instead of being personalised, urgent calls-to-action, account status threats, requests for personal information, and fake domain names/links.

Also educate your customers and employees on how to recognise a valid, secure Web site before they provide any personal or sensitive information by:

- Looking for the green bar
- Making sure the URL is HTTPS
- Clicking on the padlock to match the certificate information with the Web site they intended to go to

Education is a key component of building the trust necessary to overcome phishing fears. By helping your customers understand how to confirm they are safe on your Web site, you can grow revenues, differentiate your offering, and/or benefit from operational savings by moving more transactions online.

### + Conclusion

Phishing will continue to evolve into new forms, while attempting to take advantage of human behaviors such as compassion, trust, or curiosity. Protecting your brand and your business from phishing requires constant diligence, but pays rewards beyond reduced fraud losses.

By educating and protecting your customers with the highest levels of protection provided by EV SSL Certificates, your business can ensure customers have greater confidence in your online services. By demonstrating leadership in online security, you can broaden your market appeal and in doing so, generate new revenue streams.

### + Glossary

**Certificate Authority (CA)** — A Certificate Authority is a trusted third-party organisation that issues digital certificates such as Secure Sockets Layer (SSL) Certificates after verifying the information included in the Certificates.

**Encryption** — Encryption is the process of scrambling a message so that only the intended audience has access to the information. Secure Sockets Layer (SSL) technology establishes a private communication channel where data can be encrypted during online transmission, protecting sensitive information from electronic eavesdropping.

**Extended Validation (EV) SSL Certificate** — Requires a high standard for verification of Secure Sockets (SSL) Certificates dictated by a third party, the CA/Browser Forum. In Microsoft® Internet Explorer 7 and other popular high security browsers, Web sites secured with Extended Validation SSL Certificates cause the URL address bar to turn green.

**HTTPS** — Web pages beginning with "https" instead of "http" enable secure information transmission via the protocol for secure http. "Https" is one measure of security to look for when sending or sharing confidential information such as credit card numbers, private data records, or business partner data.



**Secure Sockets Layer (SSL) Technology** — SSL and its successor, transport layer security (TLS), use cryptography to provide security for online transactions. SSL uses two keys to encrypt and decrypt data – a public key known to everyone and a private or secret key known only to the recipient of the message.

**SSL Certificate** — A Secure Sockets Layer (SSL) Certificate incorporates a digital signature to bind together a public key with an identity. SSL Certificates enable encryption of sensitive information during online transactions, and in the case of organisationally validated Certificates, also serve as an attestation of the Certificate owner's identity.

**+ Learn More**

For more information about VeriSign® EV SSL solutions to protect against online fraud threats, please call 1-800-368-7173 or email: [sales@verisign.com](mailto:sales@verisign.com)

**+ About VeriSign**

VeriSign, Inc. (NASDAQ: VRSN) is the trusted provider of Internet infrastructure services for the networked world. Billions of times each day, VeriSign helps companies and consumers all over the world engage in communications and commerce with confidence. Additional news and information about the company is available at [www.verisign.com.au](http://www.verisign.com.au)

Visit us at [www.Verisign.com](http://www.Verisign.com)