CYBER SECURITY
INDUSTRY ALLIANCE

Phishing: Get the Facts

September 2006

Phishing: Get the Facts

What is phishing?

Phishing is a technique whereby criminals use spoofed e-mail or Web pages to trick recipients into providing personal information, such as social security numbers or credit card account information, which can be used for identity theft purposes. Because the criminals will hijack well known brand names to create their scams, these fraudulent e-mails appear to be legitimate at first glance, often asking consumers for updated account information for banks or other services that they actually use.

Phishing is different from other fraud types because it combines:

- Social Engineering: Phishing exploits individuals' vulnerabilities to dupe victims into acting against their own interests.
- Automation: Computers are used to carry out phishing attacks on a massive scale.
- Electronic Communication: Phishers use electronic communications networks (primarily the Internet).
- Impersonation: A phishing attack requires perpetrators to impersonate a legitimate firm or government agency.

How does a computer user become a victim of phishing?

> Phishing hit an all-time high in July 2006, with 14,191 new phishing sites reported, an 18 percent increase over the previous high. The number of brands hijacked by phishers was up 20 percent from the previous month, at a record high of 154 brands.
>
> -Anti-Phishing Working Group

Anyone can fall victim to phishing, as the Websites and emails used in phishing scams are often designed to look exactly like the real thing, even using identical logos. Common examples of phishing attacks include:

- An email asking you to validate your account details
- Cold phone calls from your bank asking for information

What can computer users do to prevent phishing?

Phishers have become very sophisticated and often there is no way to distinguish a fake online banking or e-commerce site from a real one. Often, the best defense against phishing attacks is to use caution when giving out your personal information. Do not email this information or give it out during transactions you did not initiate.

The Federal Trade Commission recommends that:

- You should only give away financial information online when *you* want something. For instance, you want to buy something in a transaction *you* initiated. Obviously, that's an appropriate time to give a credit card number. But unless it's an instance when *you* want something, it doesn't make sense for you to be giving away that info. If you initiate the transaction, chances are the request is legitimate. Difficulties arise much more frequently when you respond to a request for personal or financial information as opposed to supplying it because you want to open a new account, make a purchase, etc.

- If you get an email or pop-up message that asks for personal or financial information, do not reply or click on the link in the message. Legitimate companies don’t ask for this information via email. If you are concerned about your account, contact the organization in the email using a telephone number you know to be genuine, or open a new Internet browser session and type in the company’s correct Web address. In any case, don’t cut and paste the link in the message.
- Don’t email personal or financial information. Email is not a secure method of transmitting personal information. If you initiate a transaction and want to provide your personal or financial information through an organization’s Web site, look for indicators that the site is secure, like a lock icon on the browser’s status bar.
- Review credit card and bank account statements as soon as you receive them to determine whether there are any unauthorized charges. If your statement is late by more than a couple of days, call your credit card company or bank to confirm your billing address and account balances.
- Be cautious about opening any attachment or downloading any files from emails you receive, regardless of who sent them.
- Report suspicious activity to the FTC. If you get spam that is phishing for information, forward it to spam@uce.gov. If you believe you’ve been scammed, file your complaint at www.ftc.gov, and then visit the FTC’s Identity Theft Web site at www.consumer.gov/idtheft to learn how to minimize your risk of damage from ID theft.

What technology solutions are available to help prevent phishing?

- *Anti-virus software*: Some phishing emails contain software that can harm your computer or track your activities on the Internet without your knowledge. Anti-virus software and a firewall can protect you from inadvertently accepting such unwanted files. Anti-virus software scans incoming communications for troublesome files. In addition, anti-spam programs will also block a number of phishing emails. A firewall helps make you invisible on the Internet and blocks all communications from unauthorized sources. It's especially important to run a firewall if you have a broadband connection. Finally, your operating system (like Windows or Linux) may offer free software "patches" to close holes in the system that hackers or phishers could exploit. (copied from FTC)

- *Outgoing filters*: Consumers should utilize software that blocks certain strings from leaving your machine (companies look for such words as "Confidential"). Use such software in "alert" mode. However, don't enter the whole of your account numbers. For instance, enter only the first 3 digits of your social security number, or the first 4 digits of your credit card numbers and only partials of your bank accounts numbers. Never enter the full account number.

- *Anti-spam technologies*: Phishing is conducted very much like spam. So, any anti-spam technology would also be of help. Internet Service Providers (ISPs) such as Microsoft, AOL and others have efforts underway to weed out spam for their clients. These anti-spam technologies should be utilized to help prevent phishing attacks.

- *Anti-spyware technologies*: Many companies offer anti-spyware technologies which help prevent fraudsters from gaining unauthorized access to personal information through spyware and other key loggers.

- *Authentication techniques*: Change your passwords and PINs regularly. Banks advise that you use separate PINs and passwords for different accounts. That way, if one gets compromised, your entire financial life won't be revealed. Use advanced authentication solutions whenever they are available, such as tokens.

About the Cyber Security Industry Alliance

The Cyber Security Industry Alliance is the only advocacy group dedicated exclusively to ensuring the privacy, reliability and integrity of information systems through public policy, technology, education and awareness. Led by CEOs from the world's top security providers, CSIA believes a comprehensive approach to information system security is vital to the stability of the global economy. Visit our web site at www.csialliance.org.

Members of the CSIA include Application Security, Inc.; CA, Inc. (NYSE: CA); Citadel Security Software Inc. (CDSS:OTC); Citrix Systems, Inc. (NASDAQ: CTXS); Entrust, Inc. (NASDAQ: ENTU); F-Secure Corporation (HEX: FSC1V); Fortinet, Inc.; Internet Security Systems Inc. (NASDAQ: ISSX); iPass Inc. (NASDAQ: IPAS); McAfee, Inc. (NYSE: MFE); Mirage Networks; PGP Corporation; Qualys, Inc.; RSA Security Inc. (NASDAQ: RSAS); Secure Computing Corporation (NASDAQ: SCUR); Surety, Inc.; SurfControl Plc (LSE: SRF); Symantec Corporation (NASDAQ: SYMC); TechGuard Security, LLC; and Vontu, Inc.

Cyber Security Industry Alliance
2020 North 14th Street, Suite 750 • Arlington, VA 22201 • (703) 894-CSIA • www.csialliance.org