Lessons Learned by Consumers, Financial Sector Firms, and Government Agencies During the Recent Rise of Phishing Attacks

Prepared by the Financial and Banking Information Infrastructure Committee and the Financial Services Sector Coordinating Council

May 2005

Lessons Learned by Consumers, Financial Sector Firms, and Government Agencies During the Recent Rise of Phishing Attacks

Prepared by
The Financial and Banking Information Infrastructure Committee (FBIIC)
And the Financial Services Sector Coordinating Council (FSSCC)

May 2005

Introduction

Increasingly, Americans are receiving fraudulent e-mails that direct recipients to websites where they are asked to provide confidential personal and financial information. These e-mails may vary significantly in how they request information. Some claim that the individual's personal information is necessary to assist in the fight against terrorism or for some other alleged legal purpose. Other e-mails purport to be from government agencies or private sector entities, such as banks, Internet auction sites, or electronic payment services.

In these fraudulent schemes, commonly known as "phishing", the perpetrator sends an e-mail to consumers, falsely claiming to be from a legitimate company, in hopes of luring consumers to a "spoofed" website. The spoofed website mimics the legitimate website for the sole purpose of stealing the consumer's personal information. At the typical spoofed website, consumers are asked to update sensitive personal information, such as names, account and credit card numbers, passwords, Social Security numbers and other information. In addition to phishing, another electronic scam has emerged, known as "pharming", in which an Internet user is redirected to a criminal's spoofed site even though the user entered a valid URL in the browser's address bar. This redirection usually involves worms and Trojans that attack the browser address bar and exploit vulnerabilities in operating systems and the Domain Name Servers (DNS) of compromised computers.

Each month, these criminals are increasing their phishing activities dramatically. One organization devoted to fighting this type of fraud identified 13,141 unique phishing incidents in February 2005. The organization also reports that the financial services industry is the most commonly spoofed industry.[1] Each phishing attempt can result in thousands of consumers receiving fraudulent e-mail. Although the number of consumers that reveal their personal information is very small, even a low "success" rate is sufficient to encourage more phishing.

This document describes a few lessons learned by consumers, financial sector firms, and government agencies as they have responded to the recent wave of phishing activities. Please note that due to the evolving nature and growing sophistication of Internet and electronic scams, these lessons are not all inclusive and cannot guarantee security and protection from these frauds.

---

[1] Anti-Phishing Working Group, *Phishing Activity Trends Report*, February 2005.

The Phished: Lessons Learned by Consumers

Many consumers have successfully prevented, detected, and responded to phishing attacks by following these precautions and practices:

Measures to Prevent Falling Victim to Phishing:

1. Do not reply to or click on a web link in an e-mail that asks for any personal information unless you have initiated contact with the merchant. Be especially cautious about "urgent" emails warning you that your account will be closed unless you confirm your sensitive information. The government and many financial institutions have a policy of not soliciting a consumer's sensitive information through e-mail. Instead, telephone the company cited in the e-mail using an authenticated number or other form of communication that you are sure is genuine. One possible source of an authenticated number is your previous month's statement from that company.

2. Before submitting financial information through a website, look for the **locked padlock** or other security indicator on the browser's status bar or look for "http**s://**" at the beginning of the web address in the browser's address window. The presence of a **padlock** or similar indicator and the http**s://** does **not** guarantee that the website is legitimate or secure. However, the absence of either the padlock or the http**s**:// does indicate that the website is not secure and that it may not be legitimate.

3. Apply the latest patch for your web browser and operating system software, making sure the patch is legitimate. Review and turn on the appropriate security features in your browser software. If you use a Microsoft operating system, you may wish to turn on the automatic update setting to receive the latest patches as they are released.

4. Install and periodically update your firewall, as well as anti-virus, anti-Spyware, and anti-spam software. Ensure the software is current and operational. If you have children in the house, consider enabling the available parental controls.

Measures to Detect Phishing Attacks or Fraudulent Activity:

1. Review credit card and financial institution account statements for any unauthorized charges as soon as you receive them.

2. If your statement is more than a couple days late, call the institution to confirm your billing address, account balances, and whether they have mailed your statement.

Measures to Respond to Phishing:

1. If you have received a phishing e-mail purportedly from a financial institution, let the institution know that you have received a suspicious request for personal information. Contact the institution directly by calling a verified domestic telephone number or by typing the correct web address into your Internet browser. You may find legitimate contact information in your monthly statement.

2. Forward the phishing e-mail to the Federal Trade Commission (FTC) at uce@ftc.gov. If you believe you have been defrauded, visit the FTC at http://www.consumer.gov/idtheft/ to file a complaint and to learn how to minimize the financial damage from identity theft.

3. If your account has been compromised as a result of a phishing incident, change your password or ask your institution to close the online user ID and establish a new user ID and password.

4. If you are a victim of fraud or suspect that you are, please contact your financial institution(s) to report the crime and prevent further fraud. Also contact the three major credit bureaus and obtain a copy of your credit reports. Review these reports monthly for any changes. Below are the telephone numbers and addresses of the three major credit reporting bureaus:

	Equifax	Experian	TransUnion
Order Credit Report	1-800-685-1111	1-888-EXPERIAN (397-3742)	1- 800-888-4213
Report Fraud	1-800-525-6285	1-888-EXPERIAN	1-800-680-7289
Address	P.O. Box 740241 Atlanta, GA 30374-0241	P.O. Box 2002 Allen, TX 75013	P.O. Box 1000 Chester, PA 19022

The Spoofed: Lessons Learned by Financial Sector Firms and Government Agencies

Financial sector firms, government agencies, and other organizations have learned important lessons on how to defeat phishing attacks. Many financial regulators have issued guidance[2] to the institutions they regulate, including the following joint release:

> Joint Release of the Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, National Credit Union Administration, Office of the Comptroller of the Currency, and the Office of Thrift Supervision, Federal Bank, Thrift and Credit Union Regulatory Agencies Provide Brochure with Information on Internet "Phishing" (September 8, 2004), *available at* http://www.fdic.gov/news/news/press/2004/pr9304.html.

Commonly cited measures to prevent, detect, and respond to phishing attacks include:

Measures to Prevent Falling Victim to Phishing:

1. Personalize e-mails to consumers so that consumers have a greater assurance of the e-mail's legitimacy.

2. Remind consumers on your website that you will never send them an email asking them to come to your website to enter personal information.

3. Set up your loan application websites so that current customers do not have to enter Social Security numbers and other personal information that you already have on file.

4. Keep website certificates up to date so that consumers are assured of the site's legitimacy.

5. Remind consumers to obtain and use the latest patch for their web browser and operating system software.

6. Provide on company or agency websites a domestic telephone number for consumers to call to verify e-mail requests for information.

7. Register domain names that are similar to the name of the firm or agency so that consumers are less likely to confuse a false website with the legitimate website. Practice consistent branding.

---

[2] This summary of lessons learned is not legal or regulatory guidance. It does not supplement or replace regulatory guidance issued by any of the agencies that are members of FBIIC. For regulatory guidance on responding to phishing attacks, please contact your financial regulator.

8. Consider establishing a trademark for the domain name of the firm. Under the Anticybersquatting Consumer Protection Act, 15 U.S.C. 1125(d), a firm may be able to initiate immediate action in Federal district court against the suspicious website to protect the firm's trademark.

Measures to Detect Phishing Attacks:

1. Monitor the Internet for the suspicious use of trademarks and key content.

2. Monitor the Internet for fraudulent variations of the firm's or agency's name, trademark, seal, or website address.

3. Instruct call center employees to identify and notify management of reports of suspicious e-mails.

Measures to Respond to Phishing:

1. Promptly post a prominent alert describing the incident on the firm's or agency's website.

2. Contact consumers by e-mail or postal mail warning them not to respond to suspicious e-mails. Remind consumers of the firm's or agency's official policy of not soliciting sensitive information through an e-mail.

3. Alert staff and third-party vendors of the attack and ask that they watch out for unusual activity. Ensure employees know how to respond to victims' calls, specifically, how to: respond to questions; ask the right questions and collect appropriate information regarding the incident; inform the victim of next steps; and report the incident.

4. Advise those consumers who have fallen victim to the attack to change their passwords, report to the FTC, etc. (*see* Lessons Learned by Consumers section).

5. Contact the **Internet Service Provider (ISP)** hosting the illegitimate website and ask that the illegitimate site be shut down forthwith. Ask the ISP to disclose the identity of the owner of the illegitimate website.

6. Contact a **law enforcement agency**—local, state or federal—to pursue a subpoena or other appropriate remedy to identify the owner of the illegitimate website. Below are two law enforcement agencies with particular expertise in fighting cyber crime, including phishing:

    a. **U.S. Secret Service** Field Offices and Electronic Crimes Task Forces. http://www.secretservice.gov/field_offices.shtml

b. **Federal Bureau of Investigation** (FBI) Field Offices. http://www.fbi.gov/contact/fo/fo.htm

7. Forward phishing e-mails to the FTC at uce@ftc.gov. You may also file a complaint with the FTC at http://www.consumer.gov/idtheft/.

8. Report the phishing attack to the **Internet Fraud Complaint Center**, a partnership between the FBI and the National White Collar Crime Center, at http://www.ifccfbi.gov/index.asp

E PLURIBUS
UNUM