# 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 2004**

**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 2004**

## 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. 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 financial sector firms, Internet auction sites, or electronic payment services.

In these fraudulent schemes, commonly known as "phishing", the fraudster 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 name, account and credit card numbers, passwords, social security numbers and other information.

In recent months, fraudsters have increased their phishing activities dramatically. One organization devoted to this type of fraud identified 1,125 unique phishing incidents in April 2004 – a 180% increase over the number of attacks reported in March 2004. The organization also reports that the financial services industry is the most commonly spoofed industry.[1] Another recent study shows that 76% of all known phishing attempts occurred within the past six months. Each phishing attempt can result in thousands of consumers receiving fraudulent email. Yet another recent survey found that approximately 3% of adult internet users revealed personal information to the fraudsters. Because phishing scams are sent to thousands of customers, even a 3% success rate is sufficient to encourage more phishing.

This document describes a few of the key lessons learned by consumers, financial sector firms, and government agencies as they have responded to the unprecedented wave of recent phishing activities. Defeating phishing requires efforts by everyone to be successful.

[1] Anti-Phishing Working Group, *Phishing Attack Trends Report*, Apr. 2004.

# The Phished: Lessons Learned by Consumers

Many consumers have avoided falling victim to phishing attacks by applying the following precautions and practices:

Measures to Prevent Falling Victim to Phishing:

1. Do not reply to or click on a link in an e-mail that warns you, with little notice or prior legitimate expectation that an account of yours will be shut down unless you confirm your billing information. Instead, contact the company cited in the e-mail using an authenticated telephone number or other form of communication that you are sure is genuine.

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

3. Apply the latest patch for your web browser and/or operating system software (but be sure that the patch is legitimate).

Measures to Detect Phishing Attacks:

1. 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 and to determine whether they have mailed your statement.

2. Look for a domestic telephone number on a company or agency website, and call the number to verify the legitimacy of the web site. Many phishing attempts originate from outside the U.S. and thus are not likely to have a working domestic phone number. As a further precaution, particularly against U.S.-based phishing efforts, seek to verify the number, such as with directory assistance or company information that you know to be reliable.

Measures to Respond to Phishing:

1. Report suspicious activity to the FTC. Send the actual phishing e-mail to uce@ftc.gov. If you believe you have been defrauded, file your complaint at http://www.ftc.gov, and then visit the FTC's Identity Theft website at

http://www.ftc.gov/idtheft to learn how to minimize the financial damage from identity theft.

2. For additional guidance on how to avoid falling victim to phishing attempts, visit the Federal Trade Commission's (FTC) consumer help site at http://www.consumer.gov.

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

In recent months, 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] on avoiding phishing attacks to the institutions they regulate, including the following published documents:

- Alert from the Office of the Comptroller of Currency, to Chief Executive Officers and Chief Information Technology Officers of National Banks, Federal Branches, Service Providers, Department and Division Heads, and Examining Personnel (Sep. 12, 2003);

- Memorandum from the Office of Thrift Supervision, to the Chief Executive Officers of Thrift Institutions (Mar. 8, 2004);

- Letter from the Federal Deposit Insurance Corporation, to Financial sector firms (Mar. 15, 2004);

- Letter from the National Credit Union Administration, to Federally Insured Credit Unions (Apr. 2004).

The FBIIC and FSSCC have grouped the following lessons learned into effective measures to prevent, detect, and respond to phishing attacks. The most commonly cited measures include:

Measures to Prevent Falling Victim to Phishing:

1. Personalize e-mails to consumers so that consumers are assured of their legitimacy.

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

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

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

5. Register domain names that are similar to that of the firm's or agency's so that consumers do not confuse them with the legitimate website.

[2] This summary of lessons learned is not 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.

6. Establish 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 use of trademarks and key content by suspicious users on the Internet.

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.

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.

   Here are some examples of law enforcement agencies with particular expertise in fighting cyber crime, including phishing:

   a. **U.S. Secret Service** Field Offices and Electronic Crimes Task Forces. This website contains a contact list of the offices: http://www.secretservice.gov/field_offices.shtml

b. **Federal Bureau of Investigation** Field Offices. This website contains a contact list of the offices: http://www.fbi.gov/contact/fo/fo.htm

7. Forward any phishing e-mail to the **Federal Trade Commission** (FTC) at uce@ftc.gov. You may also file a complaint with the FTC at http://www.ftc.gov/idtheft.

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


E PLURIBUS
UNUM