Office of Thrift Supervision
Department of the Treasury *Managing Director, Examinations, Supervision, and Consumer Protection*

1700 G Street, N.W., Washington, DC 20552 • (202) 906-7984

March 8, 2004

MEMORANDUM FOR: **CHIEF EXECUTIVE OFFICERS**

FROM: Scott M. Albinson

SUBJECT: Phishing and E-Mail Scams

Purpose

A rapidly growing form of Internet fraud is a practice known as "phishing." This fraud can lead to financial loss, identity theft, and loss of customer confidence in your institution. The purpose of this memorandum is to familiarize you with the characteristics of phishing, and to encourage you to implement safeguards that will reduce the likelihood of your institution's customers becoming victims of this fraud.

Background

Phishing is the practice of sending fraudulent e-mail messages to addressees requesting them to supply confidential information. The message can be directed at a smaller number of targeted recipients, but is most often mass-mailed or "spammed" to thousands of potential victims. The e-mail is disguised to look like a request from a legitimate organization such as a thrift, a credit card company, or a retail merchant with which recipients may already have a business relationship. Often the message includes a warning regarding a problem related to the recipient's account and requests the recipient to respond by providing specific confidential information. The format of the e-mail typically includes proprietary logos and branding, a "From" line disguised to appear as if the message came from a legitimate sender, and a link to a website or a link to an e-mail address. All of these features are designed to assure the recipient that the e-mail is from a legitimate business source when in fact, the information submitted will be sent to the perpetrator.

Victims may be directed to provide personal account information by responding to the e-mail, or they may be directed to click on a link that takes them to a legitimate looking webpage containing a form on which they are instructed to provide the information. Typically, the information requested includes items such as account numbers, passwords, PINs, Social Security numbers or other personal identifying information that will allow the perpetrator to gain access to the victim's accounts, steal the victim's identity, sell the information to others seeking to do the same, or all of these.

Prevention and Mitigation

Customer education and staff training are important tools you can use to combat e-mail frauds such as phishing. Institutions should consider implementing the following measures as appropriate:

- Implement a policy that your institution will not solicit confidential or sensitive customer information via e-mail and inform customers of the policy on a periodic basis.

- Provide a notice to your customers describing your security policies and practices and the role the customer can play in protecting his or her own information. This notice should include information to make customers aware of frauds and scams that can be carried out using e-mail, the Internet, and other communication methods, and what to do if they suspect they are the targets of one of these schemes. The security policies and the notification to customers should include specifics regarding what information you will not request from customers via e-mails, telephone, or other communication methods. With this information your customers will be more alert to suspicious e-mails. This notice can appear on monthly statements, the institution's website, and other periodic communications.

- Include a security-related page on your website to educate customers about phishing and other frauds. The page might include information about known frauds and instructions on what customers should do if they identify or suspect one. An effective practice is to place a prominent link or button on each page of your website that will direct the reader to the security page.

- Adopt a policy to personalize e-mails to customers using their names in the message, and inform customers of this policy. Perpetrators often use mass-mailing programs to "spam" e-mails to many recipients using a non-personalized greeting such as "Valued Customer" or "To Whom It May Concern." Instruct customers not to respond to such e-mails and to notify you if they receive any e-mails purported to be from you that do not include this personalization.

- Keep abreast of advances in technology designed to protect customer information and reduce e-mail fraud, and take advantage of those that are effective and practical for your thrift.

- Apply system and software patches and upgrades on a timely basis.

- Maintain information security procedures in accordance with current industry best practices and regulatory guidance. (See resource list below)

- Keep website certificates current and educate customers how to verify that the pages they are viewing are actually those of your institution.

- Design educational popup messages to appear occasionally when a customer logs in or views certain pages. Possible message subjects include how to identify a phishing attack, how to avoid the consequences, how to report attacks to you, and how to get to the security section of the website.

- Train security and customer service staff regarding your policies and procedures for protecting customer information, including those concerning phishing and other forms of e-mail fraud, so they are sensitive to customer comments and informed of the appropriate actions to take.

Incident Response

If you become aware of actual phishing incidents using your institution's name, logo, graphics, etc. to solicit information from customers, you should consider taking the following actions as appropriate:

- Post a prominent alert notice on your website's homepage and login screen. The notice should relate the details of the phishing incident so the reader will be able to recognize it and know not to respond to it or other e-mail requests of this type. The notice should also reiterate your institution's security policies and practices and indicate how to identify legitimate communications from your institution. Finally, the notice should include a point of contact should the customer need more information or wish to report that they have been a victim of the scam.

- Contact customers directly by mail and/or e-mail providing them with the information noted above.

- Monitor customer accounts for unusual activity and trends.

- Flag and monitor closely the accounts of customers who report that they have fallen victim to a phishing or similar e-mail scam.

- Alert your staff to the incident so that they are sensitive to the situation and report activity such as unusual address change requests, account transactions, or new account activity.

- Encourage customers who believe that they have been a victim of the phishing scam to:

  - Change their passwords and login information if they bank electronically with you.

  - Contact credit reporting services and have a fraud alert attached to their credit report file. Customers who believe they have been a victim of a phishing or other e-mail scam should be reminded that the personal information they provided to the perpetrator may be used by the perpetrator to attempt to establish accounts or obtain credit at other businesses in their name.

  - Monitor the activity in their accounts at your institution closely for a period of time, and to notify you immediately of any suspicious activity.

  - Review the Federal Trade Commission (FTC) brochures listed in the next section that describe phishing and identity theft and what consumers can do to protect themselves and what they can do if they become a victim.

You should report incidents of phishing and other e-mail fraud attempts that target your institution to your OTS Regional Office immediately. Incidents should also be reported to appropriate law enforcement agencies.

Additional References

Following are further sources of information regarding phishing and other e-banking-related frauds that may assist you in developing policies, education programs, and customer assistance plans:

Office of Thrift Supervision

- 12 CFR 570, Appendix B, *Interagency Standards Establishing Guidelines for Safeguarding Customer Information*.

- CEO Letter 143, *Interagency Guidance on Authentication in an Electronic Banking Environment*, August 9, 2001

Federal Financial Institutions Examination Council IT Examination Handbook

- *Information Security Booklet*, December 2003
  www.ffiec.gov/ffiecinfobase/html_pages/it_01.html#infosec

- *E-Banking Booklet*, August 2003
  www.ffiec.gov/ffiecinfobase/html_pages/it_01.html#ebank

Federal Trade Commission

- *How Not to Get Hooked by the 'Phishing' Scam*, July 2003
  www.ftc.gov/bcp/conline/pubs/alerts/phishingalrt.htm

- *ID Theft: When Bad Things Happen to Your Good Name*
  www.ftc.gov/bcp/conline/pubs/credit/idtheft.htm

If you have any questions regarding this memorandum, please contact Robert E. Engebreth, Director, Information Technology Risk and Infrastructure Protection at (202) 906-5631 or Robert.Engebreth@ots.treas.gov