Security

White Paper

Protecting your Consumers, Members and Financial Institution Against Phishing Attempts

As you are no doubt aware, fraudulent e-mail scams are a growing problem. Increasingly, consumers are receiving e-mails and/or pop-ups requesting personal financial and confidential information. Many of these e-mails appear to come from legitimate sources such as banks, governmental agencies, ISPs and various online companies. Fraudulent e-mails may include links to bogus or spoofed websites that also request sensitive personal information.

E-mail scams that attempt to gather personal information are called "phishing" (or fishing). Cyber-criminals are throwing out bait in hopes of collecting sensitive personal data that can be sold or used for illegal purposes.

Recognizing Phishing Attempts

Phishing e-mails are becoming more difficult to recognize as the techniques used by the fraudsters are getting more sophisticated. However, we've listed a few tips to help you recognize phishing attempts.

- Phishing e-mails often ask the recipient to visit a linked site to verify or update personal information, including account numbers and/or passwords for 'security' purposes
- They may include misspellings and/or grammatical errors
- Greetings are often 'general' (Dear valued Bank Customer)
- They may have unfamiliar return addresses
- They usually include urgent or threatening appeals (e.g. your account will be closed if you fail to verify your information)

Also, some of the latest bogus e-mails purporting to be from financial institutions now include reassuring phrases claiming the bank will never ask for personal information or login information in an e-mail. The very same e-mail may also include a link to a bogus Web site requesting personal information. After the information is entered on the bogus site, an error message is often returned.

Lastly, it is also important to be aware of e-mails indicating a new patch for added functionality or security is available for computer systems. These e-mails may appear to be from a technology provider and they may offer a patch or update that you can download through an e-mail link. This creates the opportunity to install a rogue program (key stroke logger, backdoor, spy ware, or virus) on computers that can facilitate access to a hacker and the data stored there.

Responding to a Phishing Attempt

In the event the institution is targeted in a phishing attempt, the following actions should be taken:

I. Inform institution employees of the phishing attempt so they can accurately respond to client inquiries.

II. Consider sending target messages to clients and/or posting additional information on the institution's Web site to inform customers about the phishing attempt.

III. Attempt to get the original phishing e-mail so the header information can be analyzed. Forward the e-mail header information to the IT Manager and/or security officer. If assistance is needed contact the service provider and/or IT consultant.

IV. Notify the abuse contact at the ISP hosting the bogus site and request the site be shut down immediately. Service providers and/or Shut Down specialists may provide this type of assistance.

V. Bogus phishing e-mails can also be reported to the following:

a. Netcraft—http://toolbar.netcraft.com/
b. FTC: spam@uce.gov
c. http://www.ftc.gov/bcp/conline/edcams/spam/report.html
d. Anti-Phishing Working Group.
http://www.antiphishing.org/report_phishing.html

VI. Save a copy of the bogus site and any phishing e-mails.

VII. Notify i3c.gov and the regulators

Note for additional reference: http://www.occ.treas.gov/ftp/bulletin/2005-24.doc)

Are there any solutions?

Defeating phishing requires efforts by everyone to be successful. Currently, the best protection against these online 'schemes' is knowledge. With that in mind, we've provided suggestions to assist our clients in educating the end user.

FundsXpress Educational Tools to Protect Against Phishing:

We have created sample text that could be placed on your Web site and/or sent to end users through targeted messages.

SAMPLE MESSAGE:

Protect Yourself Against E-mail Fraud:

One of the latest types of e-mail fraud is called "Phishing" (fishing). Cyber-criminals attempt to collect personal and sensitive information through phony e-mails that appear to be from legitimate companies. Typically these e-mails direct the recipients to "verify or update" their accounts and usually include links to imitations of legitimate Web sites and/or forms to collect personal information. Financial Institution X will never ask for sensitive information from you via e-mail (ex. Social security number, access ID, pass code or account number.)

Here are a few tips to help protect your personal information while using the Internet.

- *Always avoid e-mailing personal and financial information.*
- *Be suspicious of any e-mail or pop-up messages with urgent requests for personal financial information.*
- *If an e-mail arrives unsolicited from any source indicating you must click on a link to visit a site and input personal data…. Be very wary of it.*
- *Be cautious about opening any attachment or downloading any files from e-mails you receive, regardless of who sent them.*
- *Instead of clicking on links in e-mails, type in the URL that you're familiar with and/or select the Web site from your favorites.*
- *If an offer sounds too good to be true, it probably is… and should be avoided.*
- *If you have any doubts about the validity of an e-mail, contact the sender using a telephone number you know to be genuine.*
- *Regularly log into your online accounts to check your bank, credit and debit card statements to ensure that all transactions are legitimate.*

- *If you initiate an online transaction and want to provide your personal information, look for indicators that the site is secure. The URL for secure sites typically begin with "https" instead of "http."*
- *Use anti-virus software and keep it up-to-date.*
- *Make sure you have applied the latest security patches for your computer. Most software providers, like Microsoft, offer free security patches.*
- *If you have broadband Internet access (e.g. cable modem or DSL), make sure that you have a firewall.*
- *Visit www.ftc.gov/spam to learn other ways to avoid e-mail scams and deal with deceptive spam.*

***Reporting**:*

Report phishing e-mails to the FTC at spam@uce.gov. You can also report spam e-mail to your ISP, such as AOL, MSN, or Yahoo.

If you believe your identity or personal information has been stolen, file a 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.

You can also report Internet crimes on the Internet Crime Complaint Center, www.ic3.gov

If you need any assistance, you can also contact us at (FI phone number)

SAMPLE:

Protect Yourself Against Online Fraud

Deceptive e-mail messages sent to you for the purpose of stealing personal and financial information are among the most common types of e-mail fraud. Disguised as legitimate e-mail and claiming to be from sources you trust, these messages attempt to entice you to provide various types of personal and confidential information, including online IDs and passcodes, Social Security numbers and account numbers. (Financial Institution X) will never ask for sensitive information from you via e-mail (ex. Social security number, access ID, passcode or account number.)

SAMPLE:

Protecting Yourself Against Phishing and Online Fraud

The number and sophistication of phishing scams sent out to consumers is continuing to increase dramatically. While online banking is safe, as a general rule you should be careful about giving out your personal financial information over the Internet.

- *Be suspicious of any e-mail with urgent requests for personal financial information*
- *Avoid filling out forms in e-mail messages that ask for personal financial information*
- *Always ensure that you're using a secure Web site when submitting sensitive information via your Web browser. To make sure you're on a secure Web server, check the beginning of the Web address in your browser's address bar - it should be "https://" rather than just "http://."*
- *Regularly log into your online accounts to check your bank, credit and debit card statements to ensure that all transactions are legitimate*
- *Ensure that your browser is up-to-date and security patches applied to your computer's operating system. Most software providers offer free security patches; e.g. see the Microsoft Security home page -- http://www.microsoft.com/security/.*

Other tools:

Regulators and various industry groups have published additional guidance. For example, a recent report prepared by a study published by the Financial and Banking Information Infrastructure Committee (FBIIC) and the Financial Services Sector Coordinating Council (FSSCC) in May 2004 titled, "Lessons Learned by Consumers, Financial Sector Firms, and

Government Agencies of Phishing Attempts" provides several good tips to help protect your institution and your customers. This report is available on the FundsXpress Support Site.

Some of the suggestions mentioned in the FBIIC and FSSCC report may be addressed by using the new FX sample alerts and Web site text. Here's an example of some of the suggestions in this report.

1. Personalize e-mails to consumers so they are assured of their legitimacy.
2. Contact consumers by e-mail or postal mail warning them not to respond to suspicious e-mails.
3. Remind consumers to obtain and use the latest patch for their Web browsers and/or operating systems.
4. Provide phone numbers on company Web sites for con sumers to call to verify e-mail requests for information.
5. Register domain names similar to the institution's so consumers do not confuse them with the legitimate Web site.
6. Monitor the Internet for use of trademarks, key content, variations on the institution's name, logo, or Web site address. (Note: Google searches can be used to monitor this type of information).
7. Instruct call center employees to identify and notify management of reports of suspicious emails.
8. In the event that the institution's Web site has been spoofed and/or phishing e-mails are purported to come from the institution, promptly post a prominent alert describing the incident on the institution's Web site.
9. Alert staff and third party vendors of an attack and ask that they watch for unusual activity.
10. Advise consumers who have fallen victim to attacks to change their passwords and report to the FTC and the appropriate authorities.
11. Contact ISPs hosting illegitimate Web sites and ask that the site be shut down. You may also ask the ISP to disclose the identity of the owner of illegitimate sites, although they may not be willing to provide this without a court order.
12. If customers have been victims of ID theft, instruct them to contact a major credit bureau to place a fraud alert on their credit report. The bureaus are now working together to share this type of alert.

Other good resources

Microsoft on Security

http://www.microsoft.com/security/default.mspx

Regulator Guidance:

FDIC FIL-26-2004 (March 2004)
http://www.fdic.gov/news/news/financial/2004/fil2704.html

FDIC Consumer News, Tips for Safe Banking On the Internet
http://www.fdic.gov/bank/individual/online/safe.html

OCC Alert 2003-11(Sept. 2003), Alert 2004- 12(July 2004) -
http://www.occ.treas.gov/Altlst04.htm

NCUA Letters #04-CU-05, #04-CU-06 (April 2004)
http://www.ncua.gov/letters/letters.html

OTS - CEO Letter 193 (March.2004) -
http://www.ots.treas.gov/resultSort.cfm?catNumber=47&catParent=44&doc_cat=25&showDocName=y&sel=8

Summary:

FundsXpress will continue to evaluate options to address this on going threat to end users. If you have any questions or additional suggestions, please contact me.

Angela Shoemaker
Financial Institution Compliance Manager
FundsXpress Financial Network, Inc.
Email: angela.shoemaker@fxfn.com
Web site: www.fundsxpress.com