



Financial Institution Letters

Guidance on Safeguarding Customers Against E-Mail and Internet-Related Fraudulent Schemes

E-mail and Internet-related fraudulent schemes, such as “phishing” (pronounced “fishing”), are being perpetrated with increasing frequency, creativity and intensity. Phishing involves the use of seemingly legitimate e-mail messages and Internet Web sites to deceive consumers into disclosing sensitive information, such as bank account information, Social Security numbers, credit card numbers, passwords, and personal identification numbers (PINs). The perpetrator of the fraudulent e-mail message may use various means to convince the recipient that the message is legitimate and from a trusted source with which the recipient has an established business relationship, such as a bank. Techniques such as a false “from” address or the use of seemingly legitimate bank logos, Web links and graphics may be used to mislead e-mail recipients.

In most phishing schemes, the fraudulent e-mail message will request that recipients “update” or “validate” their financial or personal information in order to maintain their accounts, and direct them to a fraudulent Web site that may look very similar to the Web site of the legitimate business. These Web sites may include copied or “spoofed” pages from legitimate Web sites to further trick consumers into thinking they are responding to a bona fide request. Some consumers will mistakenly submit financial and personal information to the perpetrator who will use it to gain access to financial records or accounts, commit identity theft or engage in other illegal acts.

The Federal Deposit Insurance Corporation (FDIC) and other government agencies have also been “spoofed” in the perpetration of e-mail and Internet-related fraudulent schemes. For example, in January 2004, a fictitious e-mail message that appeared to be from the FDIC was widely distributed, and it told recipients that their deposit insurance would be suspended until they verified their identity. The e-mail message included a hyperlink to a fraudulent Web site that looked similar to the FDIC’s legitimate Web site and asked for confidential information, including bank account information.

Risks Associated With E-Mail and Internet-Related Fraudulent Schemes

Internet-related fraudulent schemes present a substantial risk to the reputation of any financial institution that is impersonated or spoofed. Financial institution customers and potential customers may mistakenly perceive that weak information security resulted in security breaches that allowed someone to obtain confidential information from the financial institution. Potential negative publicity regarding an institution’s business practices may cause a decline in the institution’s customer base, a loss in confidence or costly litigation.

In addition, customers who fall prey to e-mail and Internet-related fraudulent schemes face real and immediate risk. Criminals will normally act quickly to gain unauthorized access to financial accounts, commit identity theft, or engage in other illegal acts before the victim realizes the fraud has occurred and takes action to stop it.

Educating Financial Institution Customers About E-Mail and Internet-Related Fraudulent Schemes

Financial institutions should consider the merits of educating customers about prevalent e-mail and

Internet-related fraudulent schemes, such as phishing, and how to avoid them. This may be accomplished by providing customers with clear and bold statement stuffers and posting notices on Web sites that convey the following messages:

- A financial institution's Web page should never be accessed from a link provided by a third party. It should only be accessed by typing the Web site name, or URL address, into the Web browser or by using a "book mark" that directs the Web browser to the financial institution's Web site.
- A financial institution should not be sending e-mail messages that request confidential information, such as account numbers, passwords, or PINs. Financial institution customers should be reminded to report any such requests to the institution.
- Financial institutions should maintain current Web site certificates and describe how the customer can authenticate the institution's Web pages by checking the properties on a secure Web page.

To explain the red flags and risks of phishing and identity theft, financial institutions can refer customers to or use resources distributed by the Federal Trade Commission (FTC), including the following FTC brochures:

- "How Not to Get Hooked by the 'Phishing' Scam," published in July 2003, which is available at: <http://www.ftc.gov/bcp/online/pubs/alerts/phishingalrt.htm>
- "ID Theft: When Bad Things Happen to Your Good Name," published in September 2002, which is available at: <http://www.ftc.gov/bcp/online/pubs/credit/idtheft.htm>

Responding to E-Mail and Internet-Related Fraudulent Schemes

Financial institutions should consider enhancing incident response programs to address possible e-mail and Internet-related fraudulent schemes. Enhancements may include:

- Incorporating notification procedures to alert customers of known e-mail and Internet-related fraudulent schemes and to caution them against responding;
- Establishing a process to notify Internet service providers, domain name-issuing companies, and law enforcement to shut down fraudulent Web sites and other Internet resources that may be used to facilitate phishing or other e-mail and Internet-related fraudulent schemes;
- Increasing suspicious activity monitoring and employing additional identity verification controls;
- Offering customers assistance when fraud is detected in connection with customer accounts;
- Notifying the proper authorities when e-mail and Internet-related fraudulent schemes are detected, including promptly notifying their FDIC Regional Office and the appropriate law enforcement agencies; and
- Filing a Suspicious Activity Report when incidents of e-mail and Internet-related fraudulent schemes are suspected.

Steps Financial Institutions Can Take to Mitigate Risks Associated With E-Mail and Internet-Related Fraudulent Schemes

To help mitigate the risks associated with e-mail and Internet-related fraudulent schemes, financial institutions should implement appropriate information security controls as described in the Federal Financial Institutions Examination Council's (FFIEC) "Information Security Booklet."¹ Specific actions that should be considered to prevent and deter e-mail and Internet-related fraudulent schemes include:

- Improving authentication methods and procedures to protect against the risk of user ID and password theft from customers through e-mail and other frauds;²
- Reviewing and, if necessary, enhancing practices for protecting confidential customer data;
- Maintaining current Web site certificates and describing how customers can authenticate the financial institution's Web pages by checking the properties on a secure Web page;
- Monitoring accounts individually or in aggregate for unusual account activity such as address or phone number changes, a large or high volume of transfers, and unusual customer service

- requests;
- Monitoring for fraudulent Web sites using variations of the financial institution's name;
 - Establishing a toll-free number for customers to verify requests for confidential information or to report suspicious e-mail messages; and
 - Training customer service staff to refer customer concerns regarding suspicious e-mail request activity to security staff.

Conclusion

E-mail and Internet-related fraudulent schemes present a substantial risk to financial institutions and their customers. Financial institutions should consider developing programs to educate customers about e-mail and Internet-related fraudulent schemes and how to avoid them, consider enhancing incident response programs to address possible e-mail and Internet-related fraudulent schemes, and implement appropriate information security controls to help mitigate the risks associated with e-mail and Internet-related fraudulent schemes.

¹ Refer to the FFIEC Information Technology Examination Handbook's "Information Security Booklet" located at www.ffiec.gov.

² Refer to FDIC Financial Institution Letter 69-2001, "Authentication in an Electronic Banking Environment," issued on August 24, 2001.