An IBA Preferred Service Provider

CISSPs, CISAs, CISMs, CPAs

Phishing Attack Response

my.infotex.com

www.emergingthreats.net

Fraudulent schemes, commonly known as “phishing, has increased through the years. These e-mails, sent to consumers, falsely claim 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.

Types of phishing e-mails have purported to be from government agencies or private sector entities, such as financial sector firms, Internet auction sites, or electronic payment services. Financial institutions are a favorite target of phishing scams.

If your financial institution has been spoofed, there are several actions that you should take. These steps include:

1. Alert staff and third-party vendors of the attack and ask that they watch out for unusual activity.

2. Promptly post a prominent alert describing the incident on the financial institution’s website.

3. Contact customers by e-mail or postal mail warning them not to respond to suspicious e-mails. Remind customers of the financial institution’s official policy of not soliciting sensitive information through an e-mail.

4. Advise those consumers who have fallen victim to the attack to change their passwords, report to the FTC, etc.

5. Contact the Internet Service Provider (ISP) hosting the illegitimate website and ask that the illegitimate site be shut down immediately. 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.