

Beware of financial fraud: “phishing”

The Financial Industry Regulatory Authority (FINRA), formerly the National Association of Security Dealers, continues to warn investors and consumers about “phishing,” a scam that uses spam e-mail to lure investors into revealing bank or brokerage account information, passwords or PINs, or other types of confidential information. Often the e-mails falsely claim to be from brokerage firms, banks or other services that investors are likely to use.

According to some estimates, scam artists are able to convince up to 5% of e-mail recipients to respond to them. And, alarmingly, the number and sophistication of phishing scams are continuing to increase dramatically, according to the “anti-phishing work group” (www.antiphishing.org).

Here’s what to look for

Scam e-mails may use the names of real people, or legitimate-looking addresses, authentic-looking logos or graphics, links to pages of a bona fide Web site and official-looking fine print or references to laws. This seeming authenticity lures the investor into providing sensitive information, usually by requesting that he or she send a reply e-mail or click on a link to a Web site that mimics a legitimate site.

To lower an investor’s guard, he or she may be told that: an account will be closed unless information is updated; the investor’s identity must be verified because the account is being used by a third party in violation of the law; because of a technical update, the account must be reactivated; or recent law changes require users to identify themselves.

How to protect yourself

FINRA offers several tips, developed by the Federal Trade Commission, to help prevent you from becoming a victim of phishing or other online identity theft:

- If you receive an e-mail that warns you, with little or no notice, that an account of yours will be shut down unless you reconfirm your billing information, do not reply or click on the link in the e-mail. Instead, contact the company cited in the e-mail using a telephone number or Web site address that you know to be genuine.

- Avoid e-mailing personal and financial information. Before submitting financial information through a Web site, look for the “lock” icon on the browser's status bar. It signals that your information is secure during transmission.

- Review credit card and bank account statements as soon as you receive them in order to determine whether there are any unauthorized charges. If your statement is late by more than a few days, call your credit card company or bank to confirm your billing address and account balances.

- Keep your personal and financial information secure online. Make certain that your computer system is up to date with the latest security patches and use antivirus and spyware detection software. Firewall software should thwart intruders from getting access to your PC over a network. Never download software or files from an unknown source.

- Report suspicious activity to the FTC. Send the actual spam to uce@ftc.gov. If you believe that you've been scammed, file your complaint at www.ftc.gov, and then visit the FTC's Identity Theft Web site (www.ftc.gov/idtheft) to learn how to minimize your risk of damage from identity theft.

You can find more information about phishing or other identity-theft scams by reviewing the investor alerts available at www.nasd.com.

© 2008 M.A. Co. All rights reserved.

Any developments occurring after January 1, 2008, are not reflected in this article.