



THE SAVVY CONSUMER COLUMN

FOR IMMEDIATE RELEASE
August 3, 2010

CONTACT: D. Christopher Garrett
or Shannon Ashford
(615) 741-6007

Send phishy e-mails seeking your information right to your spam folder

Nashville, TN – “We suspect an unauthorized transaction on your account. To ensure that your account is not compromised, please click the link below and confirm your identity.”

Have you received e-mail with a similar message? It’s a scam called “phishing” – and it involves Internet fraudsters who send spam or pop-up messages to lure personal information (credit card numbers, bank account information, Social Security numbers, passwords or other sensitive data) from unsuspecting victims.

“It’s impossible to keep up with the variations of these types of scams because they are forever changing,” said Mary Clement, director of the Tennessee Division of Consumer Affairs. “The best way to avoid being victimized is to practice safe computing and report fraudulent e-mails.”

According to the Federal Trade Commission, phishers send an e-mail or pop-up message that claims to be from a business or organization that you might deal with – for example, an Internet service provider (ISP), bank, online payment service or even a government agency. The message might ask you to “update,” “validate” or “confirm” your account information. Some phishing e-mails threaten a dire consequence if you don’t respond. The messages direct you to a website that looks just like a legitimate organization’s site. But it isn’t. It’s a bogus site whose sole purpose it to trick you into divulging your personal information so the operators can steal your identity and run up bills or commit crimes in your name.

Consumer Affairs offers these tips to help you avoid getting hooked by a phishing scam:

- Don’t reply to e-mail or pop-up messages that ask for personal or financial information, and don’t click on links in the message. Don’t cut and paste a link from the message into your web browser – phishers can make links look like they go one place when they actually send you to a different site (hovering over the link can help you find out the real address).
- If you need to reach an organization you do business with, call the number of your financial institution on the back of your card – not the number listed on an e-mail. And, you always have the option of visiting the business in person.
- Use anti-virus and anti-spyware software, as well as a firewall, and update them regularly.

-more-

- Don't e-mail personal or financial information.
- Be cautious about opening any attachment or downloading any files from e-mails that you receive, regardless of who sent them.
- Forward phishing e-mails to spam@uce.gov – and to the company, bank or organization impersonated in the e-mail.

The Federal Trade Commission has an e-card that you can forward to your friends to warn them about phishing scams. The link is www.ftc.gov/phishing.

Consumer Affairs (www.tn.gov/consumer/) is a division of the Department of Commerce and Insurance (www.tn.gov/commerce/), which works to protect consumers while ensuring fair competition for industries and professionals who do business in Tennessee.

#