

FRAUD ALERT

OIG Information Bulletin No. 3

BEWARE OF “PHISHING” EXPEDITIONS!

Internet scammers casting about for people’s financial information have a new way to lure unsuspecting victims: They go “phishing.” Phishing is an e-mail & Internet scam that uses spam or pop-up messages to deceive you into disclosing your credit card numbers, bank account information, Social Security number, passwords, or other sensitive information.

Phishers send an e-mail or pop-up message that claims to be from a business or organization that you deal with – for example, your Internet Service Provider (ISP), bank, online payment service, or even a government agency. The message usually says that you need to “update” or “validate” your account information. It might threaten some dire consequence if you don’t respond. The message directs you to a Web Site that looks just like a legitimate organization’s site, but it isn’t. The purpose of the bogus site is 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.

Don’t Get Hooked by a Phishing Scam!

- Do not reply or click on the link in the message. Legitimate companies don’t ask for this information via e-mail. If you are concerned about your account, contact the organization in the email using a telephone number you know to be genuine. Don’t cut and paste or click the link in the message.
- Don’t e-mail personal or financial information. E-mail is not a secure method of transmitting personal information. If you initiate a transaction and want to provide your personal or financial information through an organization’s Web Site, look for indicators that the site is secure, like a lock icon on the browser’s status bar or a URL address for a web site that begins “https:” (the “s” stands for “secure”). Unfortunately, no indicator is foolproof; some phishers have forged security icons.
- Review credit card and bank account statements often. If your statement is late by more than a couple of days, call your credit card company or bank to confirm your billing address and account balances.
- Use anti-virus software and popup blocking software and keep them up to date. Some phishing e-mails contain software that can harm your computer or track your activities on the Internet without your knowledge. Anti-virus software and a firewall can protect you from inadvertently accepting such unwanted files. Anti-virus software scans incoming communications for troublesome files. Look for anti-virus software that recognizes current viruses as well as older ones; that can effectively reverse the damage; and that updates automatically. A firewall helps make you invisible on the Internet and blocks all communications from unauthorized sources. Finally, your operating system (like Windows or Linux) may offer free software “patches” to close holes in the system that hackers or phishers could exploit.
- Be cautious about opening any attachment or downloading any files from e-mails you receive, regardless of who sent them.