Fraud Alert!

Don’t Get Phished

Protecting yourself against e-mail fraud

E-Mail and Internet Fraud take advantage of the Internet’s ability to send e-mail messages worldwide in seconds or post website information that is accessible from anywhere using a variety of personal devices. Making identity theft and account fraud from online scams one of the fastest growing crimes today.

You should be especially vigilant to these:

■ Phishing

Fraudulent e-mails, appearing to be from a trusted source such as your financial institution or a government agency, direct you to a website asking you to “verify” personal information. Once scammers have your log-in information and password, they have the tools to commit account *fraud using your name.*

What you can do:

- If you receive an e-mail that tells you to confirm certain information, **do not** click on the e-mail link. Instead, use a phone number or website address you know to be legitimate.
- Before submitting any financial information through a website, look for the “lock” icon on the browser status bar, or look for “https” in the web address.
- Report suspicious activity.

Remember: Your financial institution will never send you an e-mail asking you to verify personal information!

■ Texts, pop-ups & downloads

Fraudsters use smartphone texts with “urgent” requests that lure the unwary into providing personal information. Website pop-ups generated by these fraudsters will often ask users to download “important” information or “free” apps—resulting in spyware or other viruses.

What you can do:

- Stop and think before providing personal information via smartphone or computer.
- Only communicate with your financial institution using phone numbers or e-mail addresses you know to be correct.
- Don't install apps unless you know the vendor.

Malware

Short for malicious software, and also known as "spyware," it is often included in spam e-mails. It then can take control of your computer and forward personal data to fraudsters.

What you can do:

Install and update regularly your:

- Anti-virus software
- Anti-malware programs
- Operating system patches and updates

General tips against internet fraud

- **Don't judge by appearances.** The availability of software that allows anyone to set up a professional-looking website means that criminals can make their websites look as impressive as those of legitimate businesses.

- **Be careful giving personal data online.** If you receive e-mail or text requests for personal data, don't send the data without knowing who's asking.

- **Be wary of disguised e-mails and texts**. If someone sends you an e-mail or text using an mail header that has no useful identifying data it could mean that the person is hiding something.

Here are some basic safety tips you can implement immediately:

- **Password**—Experts advise a combination of letters (some capitalized), numbers and symbols at least ten characters in length.

- **Virus protection**—Your computer's anti-virus software needs to be up-to-date to guard against new strains.

- **Spyware protection**—Anti-spyware programs are readily available. Every computer connected to the Internet should have the software installed…and updated regularly.

Resources

- Internet Crime Complaint Center (IC3): **www.ic3.gov**
- Federal Trade Commission (FTC) Consumer Response Center: **www.ftc.gov**
- Identity Theft Resource Center: **www.idtheftcenter.org**
- OnGuardOnline.gov: **www.onguardonline.gov**