Fraud Alert!

Texts, Pop-Ups & Downloads

Be on guard against "urgent" requests and unsolicited "deals" on the Internet

Fraud and the new technology

Cyber-fraud criminals that are masquerading as legitimate businesses or government agencies are tricking consumers into divulging valuable personal information over the computer, phone or fax in order to drain your accounts. Here are some of the latest tips for protecting against schemes using electronic devices.

■ Think twice before responding to "urgent" text messages

A text message is sent to your cell phone or smartphone warning that your debit or credit card had been blocked for security reasons. The message urges you to call a hotline to unblock your card, but instead you reach an automated response system asking for your card number, personal identification number (PIN) and other information.

Smartphone users are being targeted by scammers because these users almost always have their phone handy and tend to respond to calls and e-mails quickly, so that many may not realize a message is fake until it's too late. Not only that, but fake Web sites are also harder to spot on a small screen.

Your best defense against high-tech scams

- **Be aware** that cyber criminals always look for new ways to use popular devices such as smartphones to try to commit fraud.
- **Stop and think** before giving personal information in response to an unsolicited request, especially one marked as urgent, no matter who the source supposedly is.
- **Only communicate** with your financial institution using phone numbers or e-mail addresses you are certain about—such as the customer service number on your account statement or the back of your card—and add these important numbers to your phone's contact list.
- **Only install programs** that you know are from legitimate Web sites, such as your Internet service provider, financial institution, wireless phone company or trusted app vendors.

■ Be on guard against unexpected pop-up windows on Web sites, including your financial institution's

If after you're logged onto your financial institution's Web site—or on any Web site, for that matter—and you get an unexpected pop-up window asking for your name, account numbers and other personal information, that is likely a sign that a hacker has infected your computer with spyware and is trolling for enough information to commit identity theft and gain access to your accounts.

It's normal for your financial institution to ask for your login ID and password when you first log in and to ask you to answer a 'challenge question' if you want to reset your password or start using a new computer. But your financial institution will not ask you—through a pop-up window—to type your name and information such as your date of birth, mother's maiden name or account numbers. Financial institutions already have that type of detailed personal information.

■ Be suspicious of unsolicited offers to download games, programs, and apps

Those "deals" could contain malicious software directing you to fake Web sites or install spyware used to steal information that can lead to theft. Consider using anti-virus software specifically designed for smartphones and other mobile devices.

For more information on Cyber-Fraud visit:

- Internet Crime Complaint Center: **www.ic3.gov**
- Federal Trade Commission: **www.ftc.gov**
- Identity Theft Resource Center: **www.idtheftcenter.org**
- On Guard Online: **www.onguardonline.gov**