

Learn about . . .

Fraud Alert: Texts, Pop-Ups, Downloads

FDIC reports that criminals 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 bank accounts. Here are the latest tips from the Federal Deposit Insurance Corp. (FDIC) for protecting against new schemes using electronic devices.

A new scam involves a text message sent to cell phones and smartphones (a hand-held device to access the Internet and make calls) warning bank customers that their debit or credit card had been blocked for security reasons. The message urges users to call a hotline to unblock their card, but instead they reach an automated response system asking for their card number, personal identification number (PIN) and other information.

**THINK TWICE BEFORE
RESPONDING TO "URGENT"
TEXT MESSAGES.**

Smartphone users now 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.

If after you're logged onto your bank'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 PC** with spyware and is trolling for enough information to commit identity theft and gain access to your bank account.

**BE ON GUARD AGAINST
UNEXPECTED POP-UP WINDOWS ON
WEB SITES, INCLUDING YOUR BANKS.**

It's normal for your bank 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 bank 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, bank account and cell phone numbers. Banks only need that type of detailed personal information when the account is initially opened.

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

**BE SUSPICIOUS OF UNSOLICITED
OFFERS TO DOWNLOAD GAMES,
PROGRAMS AND OTHER "APPS."**

For additional tips on avoiding Internet fraud, visit www.onguardonline.gov

Source: Federal Deposit Insurance Corp. (FDIC)