



**FRAUD ALERT!**

**TEXTS,  
POP-UPS &  
DOWNLOADS**

**Be on guard against  
“urgent” requests and  
unsolicited “deals” on  
the Internet**

# FRAUD & THE NEW TECHNOLOGY

**F**EDIC 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.

---

 **THINK TWICE** before responding to “urgent” text messages.

---

A new scam involves a text message sent to cell phones and smartphones 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.

“Unfortunately, this is enough information for thieves to create counterfeit cards and commit fraud,” says Michael Benardo, Chief of the FDIC’s Cyber-Fraud and Financial Crimes Section.

Smartphone users are 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.

---




 **BE ON GUARD** against unexpected pop-up windows on Web sites, including your bank’s.

---

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 computer with spyware and is trolling for enough information to commit identity theft and gain access to your bank account.

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

## YOUR BEST DEFENSES AGAINST HIGH-TECH SCAMS?

-  **Be aware** that cyber criminals always look for ways to use new technology 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 bank using phone numbers or e-mail addresses you are certain

about—such as the customer service number on your bank statement or the back of your card—and add these important numbers to your phone’s contact list; and

-  **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.

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.

---

 **BE SUSPICIOUS of unsolicited offers to download games, programs and other “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. “You should consider using anti-virus software specifically designed for smartphones and other mobile devices,” advises David M. Nelson, an FDIC fraud specialist.

For additional tips on avoiding Internet fraud, **visit [www.onguardonline.gov](http://www.onguardonline.gov)**.