FRAUD ALERT!

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

TEXTS, POP-UPS & DOWNLOADS

FRAUD & 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 credit union accounts. Here are some of the latest tips 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 (a hand-held device to access the Internet and make calls) warning credit union members 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.

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 credit union's.

If after you're logged onto your credit union'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 credit union account.

It's normal for your credit union 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 credit union will not ask you—through a pop-up window—to type your name and information such as 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 credit union using phone numbers or e-mail addresses you are certain about—such as the member service number on your account 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.

date of birth, mother's maiden name, credit union account and cell phone numbers. Credit unions 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. Consider using anti-virus software specifically designed for smartphones and other mobile devices.

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