

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

A new scam involves a fraudulent text message sent to cell phones warning bank customers that their debit or credit card has been blocked for security reasons. The message urges users to call a special hotline to release their card. When dialed, the number asks the caller to type their card number and PIN and other sensitive information. Once that has been done, the scammers have all the information they need to begin using that information illegally.



**Think twice before responding to an “urgent” text message from a number or person you do not know.**

With the advance of smartphones and the ability to access the internet or e-mail, scammers have seized an opportunity to send fake messages. Since these phones are commonly in handy reach of the user and those users tend to respond to calls and e-mails quickly, scams may easily fall through the cracks. A smartphone user may fall victim to a scam by not realizing that a message was fake until it may be too late, and fake websites and e-mails may be harder to spot on a small screen.

**Be on guard against unexpected pop-up windows** on website, including your bank’s. While it is normal for your bank to ask for your access ID and password or require that you answer a challenge questions when you first log-in. However, your bank will not ask you through a pop-up window for other secure information such as bank account number, cell phone number, or mother’s maiden name.

**Be suspicious of unsolicited offers** to download games, programs, and other apps. They could contain malicious software or spyware that may lead to fraud.

**Stop and think before giving personal information** in response to an unsolicited request – especially one that is marked urgent.

**Only communicate** with your financial institution through phone numbers and e-mail addresses you are certain to be valid.

**Only install programs** on your smartphone or computer that are from legitimate websites.