Scam Alert: Ignore Phony Banking Texts and Phone Calls

By Better Business Bureau. December 13, 2019.

"Attention. Fraudulent activity has been detected on your account. Act Now." Should you? Banks nationwide have reported a surge in scam calls and text messages to their customers nationwide. In many of these cases, these alleged messages claim to be from the individual's actual financial institution, creating an even more realistic panic for people who think their bank account is in jeopardy and they need to correct the problem immediately. Little do they know, the ploy to get personal information is just beginning.

Scammers urge consumers via text message or voicemail to call an unfamiliar phone number provided or send a fake link to login into their online account. If called, thieves request that consumers repeat back personal bank information, such as account number, PIN number or even social security number to verify their identity. In some cases, the scammers already know the account number, which lends a false sense of trust.

In both cases, people are falsely believing their accounts have already been compromised.

The Better Business Bureau has tips on how to avoid being scammed by these convincing, but bogus, calls and text messages.

How the Scam Works:

You receive a text message or phone call from a bank, alerting you to a hold or fraudulent activity on your account. You may or may not have an account at that bank. The scammer may even know your account number.

The scammers use a variety of messages and techniques, but the desired outcome is the same. Scammers will use the opportunity to obtain your banking information. For example, a website may prompt you enter your ATM card number and PIN under the guise of "reactivating your ATM card." Other times, the link may download malicious software that gives scammers access to anything on the phone. A scammer on the phone may demand your personal information such as your social security number.

What Can I Do?

- **Verify that there is an issue**. If you get a phone call or text message from your bank, claiming your account has been compromised, hang up and call back. Find your bank's phone number online or on a statement to insure you're calling the bank and not a scammer.

- **Never give personal information to unsolicited callers.** Regardless if your bank, cable provider or utility company calls your home, never give your personal information to "verify" your identity. If it doesn't seem right, hang up and call the company back at the number you know is right.

- **Be cautious of links sent via text.** Scammers could send a link to a look-a-like site, mimicking the consumer's online banking portal. After entering your login information, the scammers then have access to your accounts online. Check the URL or visit your banks website from another source–not by clicking through a link sent via text.
    - **Ignore instructions to text "STOP" or "NO"** to prevent future texts. This is a common ploy by scammers to confirm they have a real, active phone number.
    - **If you think your text message is real**, be sure it's directing to a web address like "yourbank.com" not "yourbank.otherwebsite.com."
    - **Call the bank or check out their website.** If they have been targeted by a scam, they may have further information about it. This often includes an email address where you can send a screen shot or details about your scam text to help identify and stop the scammers.

For More Information

For more about scams, go to BBB.org/ScamTips. Read more about phishing scams at BBB.org/PhishingScam.

If you've been the victim of a scam, help others avoid falling victim by reporting what happened on BBB Scam Tracker.