

New “Smishing” Scam

Fraudsters are now sending text messages to credit union and other financial institution members’ wireless devices to lure them into giving personal information. Because wireless devices use SMS, a communications protocol, to send text messages, this is called “Smishing”, the latest form of phishing.

In Smishing, an e-mail tries to lure a recipient into giving personal information. The members receive a text message via cell phone warning that their bank account has been closed due to suspicious activity. It then tells them they need to call a certain phone number to reactivate the account. Unsuspecting callers who dial the number provided in the text message will be taken to an automated voice mail box that prompts them to key in their credit card or debit card number, expiration date and PIN to verify their information.

Avoid becoming a victim by following these simple recommendations:

- Be wary of any messages received from an unknown sender.
- Do not open unsolicited e-mails or text messages.
- Do not click on any links provided in unsolicited e-mails.
- Don’t display your wireless phone number or e-mail address in public. This includes chat rooms, websites, or membership directories.
- Check the privacy policy when submitting your wireless phone number or e-mail address to any website. Find out if the policy allows the company to sell your information.
- Contact your wireless or internet service provider about unwanted messages
- If you have a question concerning your account or credit/debit card, contact your financial institution using a telephone number obtained independently, such as the phone number from your statement, a telephone book or other independent means.

If you have been a victim of Smishing report the instance immediately. Our office phone number is (310) 432-2344.