

SCAM #19 ALERT

“Smishing” scammers turn to text messaging

Recently, fraudsters have been sending text messages to credit union members in an attempt to get account information. Because wireless devices use Short Messaging Service (SMS) to send text messages, this form of scamming is called “Smishing.”

The scammers send out a text message to credit union members saying that their account has been closed due to suspicious activity. The message instructs them to call a number that has been provided to reactivate their account.

Unsuspecting callers who dial the number will reach an automated voicemail system that prompts them to enter personal information such as credit or debit card numbers, PINs, and account information.

Remember, SEFCU will never send you an unsolicited text message. If you receive a text message prompting you to enter account information, do not disclose any personal information!

To be safe, take the following precautions:

- Never display your wireless number on a public Website, chat room, or membership directory. If a con artist is unable to get your phone number in the first place, you can avoid a situation where they could gain access to your account information.
- All text message solicitations are required to provide you ample opportunity to opt-out of receiving messages in the future. Be sure to opt-out if you don't want to receive text messages from a company.
- Check a Website's privacy policy before providing your cell phone number, or any information for that matter!
- Report suspicious behavior. With identity theft on the rise, it's important to take every precaution necessary to keep your identity safe. Finding scammers after they have stolen your identity can be difficult, so prevention is the best defense. If you receive a suspicious text message, report it to your cell phone provider and SEFCU immediately!

For more information on how to protect your identity, visit sefcu.com.



SEFCU is committed to helping members protect themselves against fraud. This is the nineteenth in a series of SCAM ALERTS to educate members about deceptive activities that could harm members' financial security. While we cannot advise members of every scam, we hope the series will advance awareness of privacy and security issues.