

SCAM #21 ALERT

Phishing scam resurfaces

Some credit union members throughout our service areas have reported receiving calls from individuals telling them there has been suspicious activity on their account. The caller then prompts members to enter personal information, like account numbers, Personal Identification Numbers (PINs), and credit card numbers. The scammer is just trying to gain your confidential account information – remember never give out confidential information!

Don't hesitate to report fraud

SEFCU will never call you to ask for a PIN, card number, or any other personal or account related information. If you get an unsolicited call requesting sensitive information, report the call as fraud to the Federal Trade Commission at FTC.gov, or by calling 1-877-FTC-HELP.

Be proactive

There are certain measures that you can take to prevent these types of scams from coming to your doorstep. Sign up for the National Do Not Call Registry to minimize the number of ways that your phone number can get into the wrong hands. Add your number to the list today by visiting ftc.gov/phonefraud.

Were you a victim?

If you think that you may have been a victim of a phishing scheme, you should close your account and open a new one. If you believe your personal information – like your name, or date of birth – has been stolen, you can add a code word to your account and anyone trying to gain access to your account will need to provide this word. If your card number was stolen, we can block your current card and reissue another one.

Make sure you don't become a victim of a phishing scam. Add your name to the National Do Not Call Registry today!



SEFCU is committed to helping members protect themselves against fraud. This is the twenty first 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.