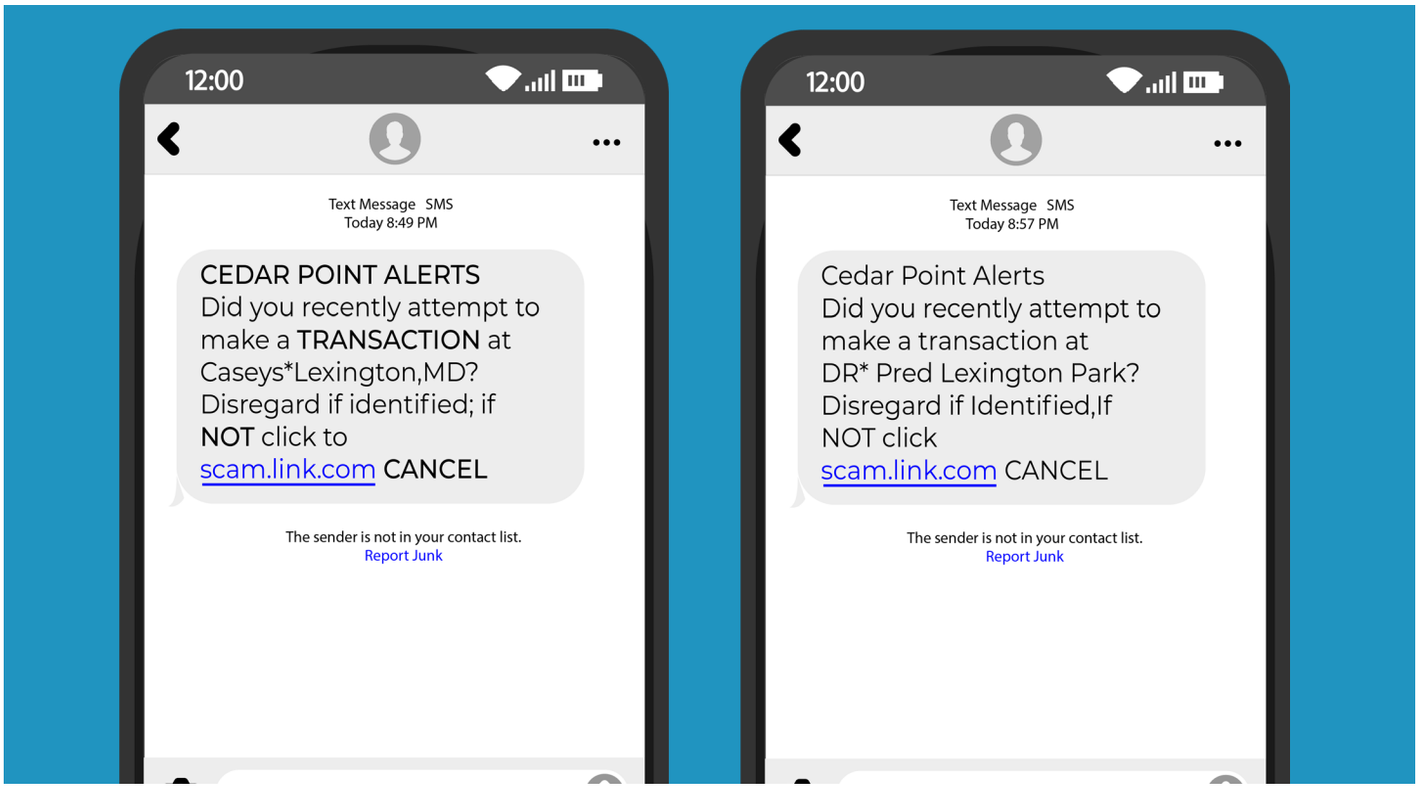
Fraud Prevention Bulletin

Fraudsters are getting creative these days. We aim to protect our members from fraud by educating them on the latest fraud schemes and how to combat them. We all think we know how to spot a scam, but are you up to date on your fraud knowledge? Learn how to spot smishing fraud schemes below.

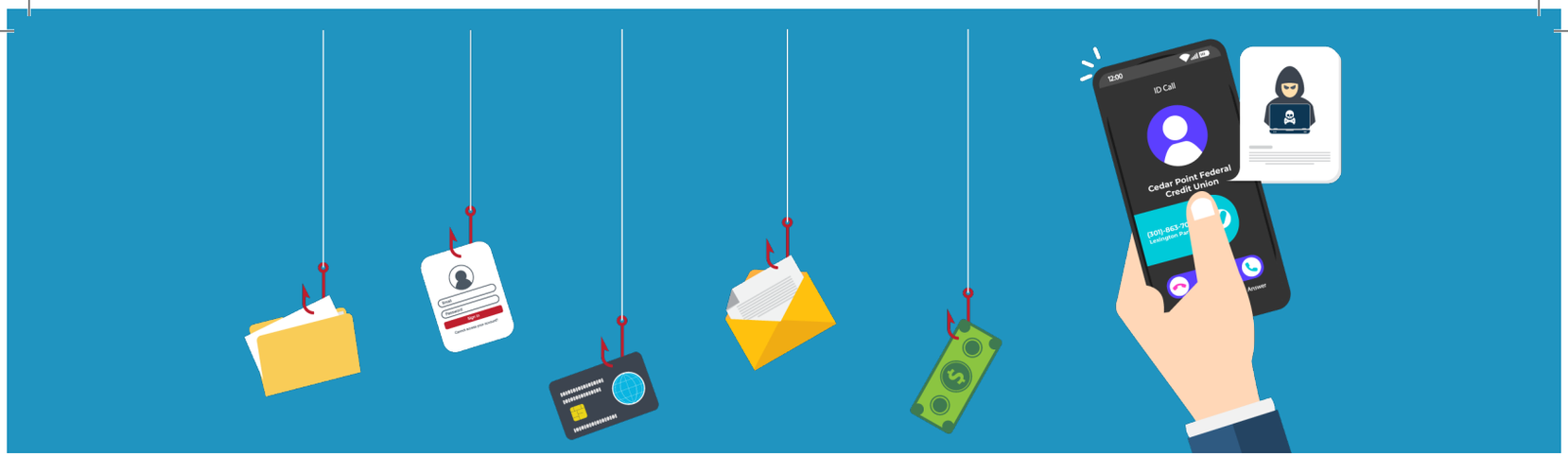
What is Smishing?

Smishing (SMS phishing) involves fraudulent text messages that appear to be from a bank or another legitimate company. These messages often include a link or phone number to trick you into clicking or calling. Clicking the link can install malware on your device, and calling the number can verify your phone number as active, making you a target for more scams.

SAMPLE FRAUDULENT MESSAGES:



If you receive a call, text, or email asking for personal information from a phone number or email address claiming to be Cedar Point or if you feel uncomfortable about the call, do not respond. Instead, call Cedar Point at 301-863-7071 to verify the legitimacy of the call, text, or email. Our Call Center representatives are available Monday through Friday from 9 a.m. to 5 p.m. and Saturdays from 8:30 a.m. to noon.



How To Protect Yourself

Now that you know what to look for, here are some tips to keep yourself safe if you encounter a scammer.

DON'T

Don't click on links in unexpected text messages. Fraudsters often send text messages pretending to be from banks, delivery services, or government agencies. These messages contain links that may install malware on your device or direct you to a fake website designed to steal your information.

Don't respond to suspicious texts. Even replying with "STOP" can confirm to scammers that your number is active, making you a target for more attacks. If you receive a suspicious message, report and delete it.

Don't give out personal information. Legitimate companies will never ask for sensitive details like your Social Security number, PINS, passwords, or account information via text message. If a message asks for these details, it's a scam.

USE CAUTION

Be wary of urgent or alarming messages. Smishing scams often create a sense of urgency, warning you about unauthorized transactions, locked accounts, or missed deliveries. Before taking any action, contact the company directly using their official phone number or website.

Check for spelling and grammar errors. Many scam messages contain typos or awkward phrasing, which can be a red flag. Enabling Spam blockers can help block spam calls and messages. Similar functions can be enabled on emails, which will send them to a separate folder, making it less likely for you to mistake them as legitimate.

BE VIGILANT

Verify the source. If you receive a text claiming to be from your bank, credit union, or a company you do business with, DO NOT CLICK THE LINK. Instead, contact the company directly using their official phone number or website.

Check your account balances and transactions regularly. If you see something unusual or notice a purchase you didn't make, report it to your financial institution immediately.

Remember, Cedar Point will NEVER TEXT you about unusual activity on your account. If you receive a text, call us at 301-863-7071 to verify the legitimacy of the text.