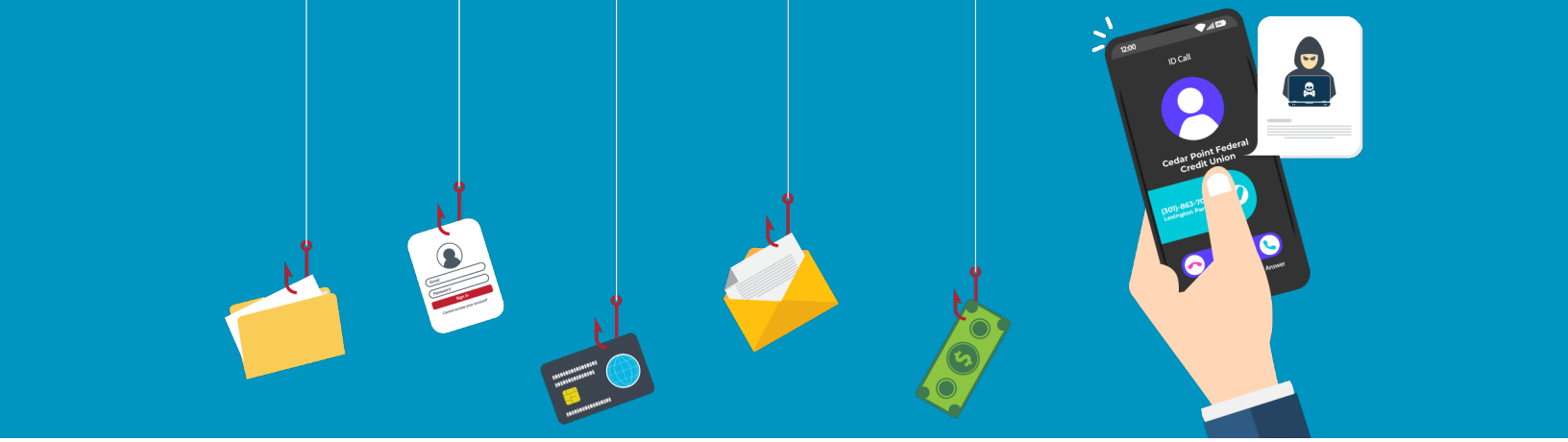


Fraud Prevention Bulletin

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 the common fraud schemes below.

SPOOFING

Spoofing is when fraudsters impersonate a trusted source. It can be through calls with false caller ID information, emails that look legitimate, texts with false links, and even false websites. The goal is to impersonate the source to access a user's account within the system, download malicious software, or send money to the fraudster. Fraudsters frequently impersonate Financial Institutions.

SKIMMING

Skimming is when fraudsters install devices on ATMs, Point-of-sale terminals, or fuel pumps to capture card data, like card numbers and pins. Fraudsters can then use this data to create fake cards or gain access to steal from victims' accounts. They may install skimmers and keypad overlays that fit over the original card reader or keypad. ATMs in well-lit, indoor locations and fuel pumps in view of the attendant are less vulnerable to tampering.

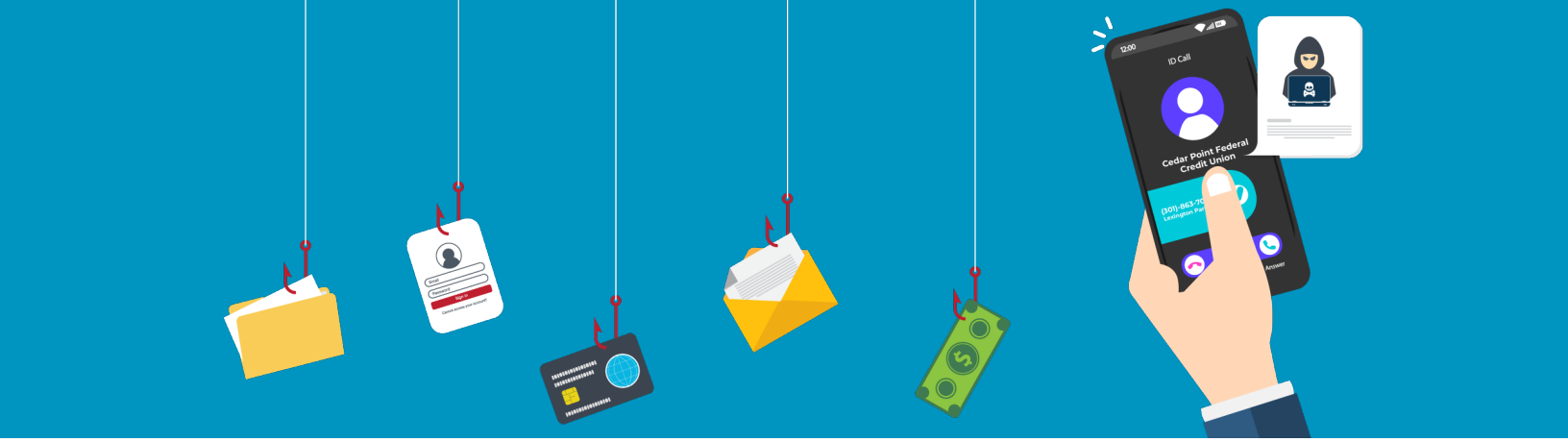
PHISHING

Phishing is when fraudsters try to get you to reveal personal or sensitive information to access accounts, often impersonating a legitimate source. Many phishing attempts use phone calls, texts, or emails. Phishers can install malicious code to your computer or phone through links that redirect you to fake websites, where they can gather information.

MOBILE PAYMENT

Mobile Payment Fraud is when fraudsters use payment apps to steal money. If fraudsters obtain information about an account, they can request money through payment apps to make the request seem legitimate. If you receive an unexpected payment from someone you know, verify the request with that person. Once money is authorized to be sent through these apps, getting it back can be difficult.

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

Answer calls from unknown numbers. It's safer not to answer calls from unknown numbers, as they can be scams. Remember that fraudsters can also manipulate caller IDs and appear to be from a trusted institution. If you answer, but it doesn't seem like who you're expecting, hang up.

Give out personal information. Scammers will ask for information like addresses, phone numbers, birthdates, Social Security Numbers, PINs, passwords, and multifactor-identification codes to gain access to your financial accounts.

Give out PINs or passwords. Make passwords unique to your account and free of sensitive information. Utilizing multi-factor identification is also a valuable tool as an extra safeguard. Do not share multi-factor identification codes with anyone.

USE CAUTION

With emails and texts with suspicious links. Scammers can set up access to your device through these links, making usernames, passwords, and multifactor identification codes easy to access. If you are sent something you aren't expecting or it contains spelling and grammatical errors, think twice about responding or clicking links.

If you are being pressured for payment or information. Fraudsters can be convincing. They use a sense of urgency to scare you into divulging information or procuring payment. Enable spam-blocking features. Enabling Spam blockers can help block spam calls or notify you when a call is likely spam. Similar functions can be enabled on emails and send them to a separate folder, making it less likely for you to mistake them as legitimate.

BE VIGILANT

Look for anything unusual on ATMs or point-of-sale terminals before using them. Inspect ATMs, POS terminals, and other card readers for anything loose, crooked, damaged, or scratched before using them. Don't use the card reader if you notice anything unusual.

Regularly check your account balances and transactions. 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 call you to ask for your PINs, login credentials, or verification codes. When you call us, we may ask for personally identifiable information as a means of identification.