Imposter Scam

Fraudsters continually find new ways to trick innocent people out of money or personal identifiable information. Whether it's an imposter scam –impersonating a credit union employee, a grandchild, debt collector, etc. –or stealing someone's identity, these fraudsters know how to pull it off.

Using common channels like emails, texts, phone calls, and social networks; fraudsters typically disguise their identify while retrieving your confidential information.

Fraudsters will use several different social engineering techniques to acquire sensitive information such as usernames, passwords, and account or payment card details –all while trying to trick you into believing they are from the credit union:

- **Phishing** (through email)
- **Vishing** (through phone calls)
- **Smishing** (though SMS/text messages)
- **Malware** (malicious software)

Fraudsters will also spoof the credit union's contact info (phone number; email, etc.) to appear to be from the actual credit union.
One common approach used is the fraudster (impersonating the credit union) claims that fraudulent transactions have been detected on your account and the credit union needs to verify your personal information. You may be asked to identify yourself with personal information, account info, login credentials, or a one-time passcode.
Recognizing scams can be difficult. But you can minimize the potential impact by knowing what to look for, taking the right action steps, and remaining vigilant.