Banking Scams

Fake Check Scam.
A scam artist creates counterfeit checks that look legitimate, with watermarks, routing numbers, and the names of real financial institutions. They then try to deposit them in banks, use them as part of other frauds against consumers, or use them to pay companies for products or services.

Unsolicited Check Fraud.
A scammer may send you a check that you didn't have a legitimate reason to receive. Unfortunately, if you cash it, you may be authorizing the purchase of items you didn't ask for, signing up for a loan, or something else you didn't ask for. The Federal Trade Commission offers tips to help you avoid being a victim of these scams, and recommends what to do if you have been a victim.

Automatic Withdrawals.
A company sets up automatic withdrawals from your account that you didn't approve. ***NOTE: The Credit Union offers this service for either making your monthly loan payments or deposits into your account. We do not set up this service without your permission and signature approval.***

Phishing.
Email messages that ask you to verify your credit union account number or debit card PIN. By clicking on the link or replying to the email with your account number, you are giving a scammer access to your financial accounts.

- **Be cautious about opening attachments or clicking on links in emails**. Even your friend or family members' accounts could be hacked. Files and links can contain malware that can weaken your computer's security.
- **Do your own typing**. If a company or organization you know send you a link or phone number, don't click on it. Use your favorite search engine to look up the website or phone number yourself. Even though the link or phone number in an email may look like the real deal, scammers can hide the true destination.
- **Make the call if you're not sure**. Do not respond to any emails that request personal or financial information. Phishers use pressure tactics and prey on fear. If you think a company, friend or family member really does need personal information from you, pick up the phone and call them yourself using the number on their website or in your address book, not the one in the email.
- **Turn on two-factor authentication**. For accounts that support it, two-factor authentication requires both your password and additional piece of information to log into your account. The second piece could be a code sent to your phone, or a random number generated by an app or a token. This protects your account even if your password is compromised.

As an extra precaution, you may want to choose more than one type of second authentication (e.g. a PIN) in case your primary method (such as a phone) is unavailable.

- **Back up your files to an external hard drive or cloud storage**. Back up your files regularly to protect yourself against viruses or ransomware attacks.

- **Keep your security up to date**. Use security software you trust, and make sure you set it to update automatically.