NEWS ALERT 9/2/21

Latest Scam Uses Mobile Apps to Steal Thousands: How to Protect Yourself

We remind our members that they should not provide confidential account information to unidentified individuals. PostCity Financial Credit Union and other legitimate companies would not ask for sensitive account information, such as passcodes or authentication codes. We have a number of measures in place to proactively warn our members about scams, and we periodically reach out to members with information about how to stay safe and avoid scams.

Experts agree it's always better to hang up and call your credit union or bank back directly to make sure you are talking to the real credit union or bank. Never use the same password. For example, if your email password is compromised and it's the same as your credit union or bank, scammers can then possibly gain access into your bank account.

Know the red flags

The most common types of scams will target you through fake emails, text messages, voice calls, letters or even someone who shows up at your front door unexpectedly. No matter which technique the scammer uses, you may be:

- Instructed to not trust your credit union or bank, or to respond to questions in untruthful ways
- Pressured to send money
- Threatened with law enforcement action
- Told to purchase gift cards and provide codes as a form of payment
- Asked to cash a check for a stranger or send money via wire transfer or Zelle
- Asked to deposit a check that overpays for something you're selling, then send the difference elsewhere

If you authorize a transfer or send money to a scammer, there's often little your financial institution can do to help get your money back.

Tips to Protect Yourself

- Try to create one password per each service and as different as possible to guess
- Whenever called by a bank or institution asking for validation, hang up and call yourself; most numbers can be spoofed.
- Never give out codes you receive on phone to strangers.

Continued on next page…

Know the best ways to avoid being scammed

Don't respond: If you're not 100% certain of the source of the call, email, or text, then hang up the phone, don't click on the link in the email, and don't reply to the text message.

Don't trust caller ID or answer phone calls from unknown numbers: If you recognize the caller ID but the call seems suspicious, hang up the phone. Phone numbers can be easily spoofed to appear to be from a legitimate caller.

Don't give out your information: Never provide any personally identifiable information unless you're absolutely certain the person and reason are legitimate. Remember: PostCity Financial Credit Union will never ask you to send us personal information such as an account number, Social Security number, or Tax ID over text, email, or online.

Research and validate: If the individual or organization seems suspicious, make sure the request being made is legitimate by calling the organization through an official number from their website or consulting with a trusted family member or friend.

If you feel you may have been a victim of a scam, contact us immediately.