Learn More. Live Better. Grow Together.
COMMUNITY ONE
Credit Union Inc.

We have recently experienced a rash of attempted fraud. Several members have reported attempts by fraudsters to hack their Credit Union accounts. Each member story is different, but the goal is the same: TO GAIN ACCESS TO YOUR ACCOUNT OR YOUR IDENTITY!

Scammers will tell you a story to tug at your heartstrings, threaten you with legal action, or make incredibly believable claims to make you their NEXT VICTIM and STEAL YOUR MONEY!

Here are just a few of the scenarios we have encountered recently:

"I'M FROM GOOGLE/PAYPAL/AMAZON, AND I NEED TO VERIFY YOUR ACCOUNT OR VERIFY A PURCHASE."
Members have received phone calls from someone pretending to represent one of these companies. They ask to verify your debit/credit card numbers to "test" the account, after which you find fraudulent transactions from everywhere draining your account balance.

CASH APP/ZELLE/VENMO FRAUD
Several members have reported that they have paid for a product or service using one of the many cash transfer apps out there, then never received what they purchased. Please be aware that these apps were developed to move money between friends and family…people you know and trust. These money transfer apps are not regulated and are very easy to use, making them another convenient tool in the fraudster's toolbox. The Credit Union is not responsible for losses when money is sent in error to a fraudster.

"I AM FROM COMMUNITY ONE CREDIT UNION, AND I NEED TO VERIFY YOUR ACCOUNT."
Fraudsters even pretend to call from C1CU! They will ask for your home banking logon and password, which gives them access to pay their bills with YOUR MONEY! They will spoof the Credit Union's phone number on Caller ID to make the call look like it is coming from C1CU.

GIFT CARD/LOTTERY/WORK-FROM-HOME SCAMS
Be very cautious of scenarios that sound too good to be true…because they usually are! If you didn't buy a lottery ticket, you probably didn't win! Scammers will try multiple ways to convince you to do what they ask. Here are just a few scam scenarios members have encountered:

- "I need to access your computer to help you resolve the problem. Please give me your username and password."
- "In order to prevent further legal action, you will need to send the total amount due immediately! You can send $1,000 to my Zelle/CashApp account and I will mark your account paid upon receipt."
- "You can pay me with a gift card. Buy $500 in gift cards from Best Buy and call me back with the card numbers and PINs."
- "You've won the lottery!! We just need your account number and your debit card number. You can pay the processing charge of $199 with your debit card, then we will send you your winnings to your account by wire transfer."

"GRANDMA/GRANDPA, I NEED BAIL MONEY!"
Members have received phone calls from someone pretending to be law enforcement or an attorney requesting cash to get the grandchild out of trouble. The fraudsters go as far as pretending to be a crying grandchild on the phone to convince their victim.

YOUR COMPUTER/PHONE IS HACKED
Opening links in emails, or inadvertently clicking on a link while surfing the internet can result in key logging software being downloaded on your computer. Then, the next time you log into Home Banking, the software records your username and password, giving the fraudsters access to your account.

Here at C1CU, the security of your account is our TOP PRIORITY. We are doing everything we can to keep your money safe, but fraudsters are very resourceful. It is very important, more now than ever, that you stay vigilant in keeping your personal information secure.

Should you receive an unexpected call with COMMUNITY ONE CREDIT UNION on the Caller ID, DO NOT ANSWER THE CALL! C1CU rarely has to call members regarding their accounts, so if it is truly your Credit Union calling, we will leave a voicemail message and you can call us back at 330-305-3050. We will NEVER need to verify your credit card or debit card numbers. We will never need to ask you tell us your Home Banking login and password. NEVER share this information with anyone!

Other steps you can take to ensure your money remains in your pocket include:

- Set up a password on your account that only you know. We will ask you for this password every time you call.
- Opt in for dual authentication on Home Banking. You will receive a one-time code via text or email whenever you access your account.
- Enable biometric ID on the C1CU Mobile App. Use your fingerprint to log in.
- NEVER SHARE YOUR PERSONAL INFORMATION WITH ANYONE.

PLEASE REPORT ANY ATTEMPTED FRAUD IMMEDIATELY TO OUR CALL CENTER AT 330-305-3050 OR 800-469-0497, SO WE CAN TAKE STEPS TO PREVENT FURTHER LOSSES TO YOUR ACCOUNT.