CUNA MUTUAL GROUP

Protecting Your Identity & Money

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.

Common Warning Signs

Scams are often hard to detect at a quick glance; however, these common red flags can help. Keep in mind…it is not uncommon for fraudsters to use intimidation tactics and urgent requests.

- Don't always trust the display name - criminals will spoof the email name to appear to be a legitimate sender
- Check for misspelled words, bad grammar, and/or typos within the content
- Be cautious of clicking links and opening attachments- DON'T CLICK unless you are confident of the sender or expecting the attachment
- Asking you to share a one-time passcode sent to your device (when they called you)
- Check the salutation - many legitimate businesses will use a personal salutation
- Do not provide personal information when asked
- Be suspicious of "urgent" or "immediate" response needed or "unauthorized login attempt" of your account
- Don't believe everything you see. Brand logos, names and addresses may appear legitimate
- The recipient group seems random or unusual (e.g. all last names begin with the same letter)
- The email appears to be a reply to a message that you didn't actually send
- Monitor the sender's email address for suspicious URLs & domains – often using similar letters and numbers
- If something seems suspicious; contact that source with a new email or phone call, rather than just hitting reply
- Always, be wary of tempting offers