CHEMCEL
Federal Credit Union
www.Chemcel.org

Member Scam Red Flags & Prevention Tips:

- Don't always trust the 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 are expecting the attachment
- Do not provide personal or account information when asked. Openly sharing information on social media can provide the necessary information to impersonate you or answer some challenge questions.
- Do not share a one-time passcode sent via text or email to your device(s)
- Check email salutations – Many legitimate businesses will use a personal salutation
- Be suspicious of "urgent" or "immediate" response needed or "unauthorized login attempt" of your account.
- Know the IRS or Social Security Administration will not contact you by phone, email, text or social media.
- Don't believe everything you see. Brand Logos, names and addresses may appear legitimate
- Be suspicious of random or unusual groups of people (e.g., all last names begin with same letter) on the to/recipient list.
- Watch for emails or texts that appear to be a reply to a message that you didn't actually send.
- Monitor the sender's email address for suspicious URLs & domains – using similar letters and numbers.
- If something seems suspicious; contact that source with a new email or phone call, rather than just responding or replying directly to the email, text, or call.
- Be wary of offers that appear too good to be true, require fast action, or instill a sense of fear.
- Keep social media accounts private and be cautious who you're connecting with
- Never share anything related to your credit union account, transactional history, or identifying information in an unprotected public forum.