Sound
FEDERAL CREDIT UNION

**Dear Valued Member,**

Your security is important to us. We want to keep you informed about common scams and how to recognize them.

Financial institutions nationwide are experiencing an increase in spoofing and phishing attempts. This is not isolated to Sound Federal Credit Union, but part of a broader trend affecting banks and credit unions across the country.

Scammers may spoof phone numbers so calls appear to come from a legitimate source, send urgent texts or emails about "fraud," claim you've won or found money, pose as government agencies or technical support, or request payment using gift cards or wire transfers.

**Please remember:**

- We will never ask for your full card number, full Social Security number, online banking username or password, one-time passcodes, PIN, or email login information.
- Never send money or buy gift cards because someone contacted you unexpectedly.
- Do not trust called ID alone. Spoofed calls can look legitimate.
- Be cautious of urgency, threats, or pressure to act immediately.
- If told money must be sent to "secure" your account, it is a scam.
- If someone says you have unclaimed funds and asks for direct deposit information, they are trying to obtain your account number. Legitimate companies typically mail a check if they do not already have your banking details.

Scammers rely on trust and fear to obtain personal or banking information. If something feels rushed or unusual, stop the conversation.

**If you receive a suspicious call, hang up. Do not click links in unexpected texts or emails. Contact us directly at (203) 977-4701 or info@mysoundcu.org.**

Thank you for helping protect your account and personal information.

Sincerely,

Sound Federal Credit Union

NCUA EQUAL HOUSING LENDER