

Scam Alert – Members Beware – Telephone and Text Scams

Please be aware of a phishing telephone scam that some credit unions across the country are reporting more frequently. Members are receiving phone calls from fraudsters posing as a credit union employee or credit union fraud department who tell them that their account has been compromised or that their credit/debit card will be or has been deactivated due to inactivity or for other various reasons.

Scammers are duplicating the phone numbers of financial institutions or fraud departments so the call appears to be coming from a legitimate source. The person making the call requests personal information or card data to verify ownership of the account before the account can be secured or the card can be reactivated. Should you happen to receive a call, text or email like this, please know that this is NOT a call, text or email from Corner Stone Credit Union, or any of our staff.

Keeping your personal information, log-ins, and passwords safe, secure, and private is vitally important.

Corner Stone Credit Union will **NEVER** contact you directly to request any of your account information, including:

- Social Security Number
- Credit or Debit Card numbers
- Security Code or CVV
- PIN – Personal Identification Number
- Address
- Date of Birth
- Online Banking Login Information
- Verification Codes
- Passwords

If someone contacts you and requests this information or your account details by phone do not share any information and hang up immediately. Likewise, if you receive an email, website pop-up, or text with a suspicious link – stop and think before you click.

Please contact us at 972-218-9266 or 214-887-8000, so we can stay at the forefront of any potential scams or fraud campaigns targeting our members.

Fighting Fraud Together

We use a variety of very strong security practices to keep your accounts safe, and we're actively taking a number of additional countermeasures to combat unauthorized activity. Still, member vigilance is our most effective form of fraud prevention.

The most important thing is to NEVER share your security credentials with anyone and, if something doesn't seem right, report it right away.

The FTC outlines simple ways you can avoid a phish and keep your information out of scammers' hands. [Read more...](#)

Finally, we ask that you please share this information with friends and family members who may be more susceptible and vulnerable to this type of fraud.