# Credit Union Impersonation Scams are on the Rise

Credit Union members must stay alert to the latest attempts by scammers to access personal financial data. Some of our members have recently received phone calls and texts from fraudsters posing as credit union fraud department checking last transactions on your account. Fraudsters spoof credit union phone numbers and email addresses and use pieces of personally identifiable information to gain members' trust before stealing account funds.

## Here's what you need to know about impersonation scams:

### What is a Credit Union Impersonation Scam?

Successful credit union impersonation scams occur when members are convinced they're communicating with an actual credit union representative via live voice call (Vishing), SMS text message (SMishing), or email (Phishing). But, in reality, they're sharing confidential information with a scammer.

Fraudsters use spoofing techniques to make it appear as though the communication is from the institution so they can:

- Steal your debit card information
- Bypass security protections and access your account online; and
- Solicit funds for fake payments

### Credit Union Impersonation Scam Scenarios

A scammer will do everything they can to appear as if they are a real credit union employee attempting to assist you with your account.

### Typical Vishing Scenario:

Posing as a credit union representative, the scammer contacts the member using a spoofed phone number. The caller claims they need to discuss an important matter, but they must first confirm the member's identity. The scammer is already on the credit union's online banking website and informs the member they need to provide the PIN sent to the member's phone or answer security questions. Since the caller says they're from the credit union and the number on the Caller ID appears to confirm it, the member doesn't hesitate to provide the requested information.

Vishing allows the scammer to use the information provided by the member to complete the login. They proceed to lock the member out of their account by changing the online banking password. The fraudster then transfers funds from the member's account to

their own temporary account before vanishing without a trace. The caller might even encourage the member to transfer funds to an external account claiming that the payment will be applied to a specific credit union loan.

**Typical Phishing and SMishing Scenario:**

Posing as a credit union fraud department employee, the scammer sends a spoofed email or text message to a member alerting them to suspicious debit card activity. Instructions urge the member to reply to the original message with account details, such as card numbers, CV2 codes, PINs, or other online account credentials. Phishing and SMishing give the scammer valuable data they can use to make unauthorized charges or access the member's account.

**How to Protect Yourself from Credit Union Impersonation Scams**

- Never share private information via SMS text message. Legitimate attempts to validate credit or debit activity only require a simple response (YES or NO) via text.
- Do not click on hyperlinked phone numbers sent via SMS text or on links inside emails.
- Pause before providing personal data via voice calls you did not initiate, even if the caller ID reads Chattahoochee FCU. Hang up and contact us using our phone number – 334.756.7027

**Chattahoochee FCU 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.

**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. If you do receive a fraudulent email, phone call or text impersonating Chattahoochee FCU, please call the credit union at 334-756-7027 so we can stay at the forefront of any potential scams or fraud campaigns targeting our members.

The FTC has valuable information on its website regarding unwanted calls, emails, and texts. https://consumer.ftc.gov/unwanted-calls-emails-texts

Please share this information with friends and family members who may be susceptible and vulnerable to this type of fraud.