FREQUENTLY ASKED QUESTIONS

Caller ID Spoofing & Vishing

What is Caller ID Spoofing?

Spoofing is when a caller deliberately falsifies the information transmitted to your caller ID display to disguise their identity. Scammers often spoof a number from a company or a government agency that you may already know and trust. If you answer, they use scam scripts to try to steal your money or valuable personal information, which can be used in fraudulent activity.

What is a Credit Union Impersonation Scam?

Successful credit union impersonation scams occur when members are convinced they are communicating with an actual credit union representative via a phone call. This is typically refered to as Vishing. But in reality, they're sharing confidential information with a scammer. Many times they will ask you questions to steal your debit/credit card information, account number, or ask you to verify your online banking credentials. 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.

How to identify a Vishing scenario?

While there are many ways a scammer can present themselves, they will pose as a credit union representative, and contact the member using the spoofed contact number. Upon calling the member, they will see that it is coming from the phone number they know and trust. The scammer may proceed with stated there is an issue with your account, or that your account has been compromised. They often request online banking credential or other sensitive member information to attempt to resolve the issue.

Characteristics to look out for are:

- The person is speaking with a sense of urgency;
- Leaving an urgent voicemail stating the member's account will be closed if the credentials or other information are not immediately provided; and using fearful tactics or causing the member to panic to them to comply.

How to protect yourself from Credit Union Impersonation Scams.

- Pause before providing sensitive information via voice calls you did not initiate, even if the caller ID reads "First Imperial Credit Union" or 760-352-1540. Hang up and contact us directly at 760-352-1540 or via online banking chat.
- If you do not recognize the number, don't answer the call. Instead, let the call go to voicemail and listen to the message later to decide whether to call back.
- If you suspect that the call is a vishing scam at any point, hang up, and don't try to carry on a conversation to be polite.
- Don't press any buttons or speak any responses to any prompts from an automated message. Scammers could potentially record your voice to navigate voice-automated phone menus tied to any of your accounts, or they might use a "press X" option to identify targets for future calls.
- Carefully listen to the caller and mentally flag if they're using social engineering language that leverages fear or urgency, or "once-in-a-lifetime opportunity" language.
- Register with the Do Not Call Registry. Most legitimate telemarketing companies avoid calling numbers on this list, so if you happen to receive a call from one, it's most likely a vishing attack.
- Do not click on hyperlinked phone numbers sent via SMS text or on links inside emails from senders you do not recognize.