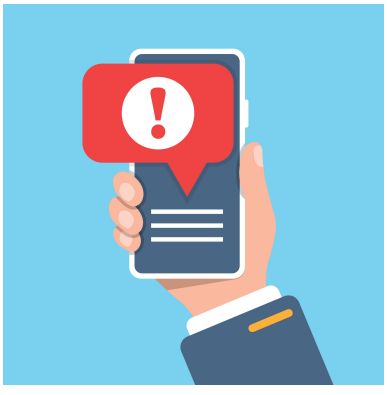
Your guide to staying ahead of the latest scams

It's part of Congressional Federal's mission to help protect our members from the ever-growing threats of financial fraud. Over the next few months we'll be sharing examples of prevalent scams that have targeted other members. Here is one scenario we're seeing in the marketplace; we hope this story can help prevent it happening to you.

Scenario One: Caller ID Spoofing



A scammer **impersonating an employee** of Congressional Federal Credit Union contacts you about suspicious activity on your account. The Caller ID says Congressional Federal Credit Union (the fraudster uses **"spoofing" technology**). They have relevant information on hand--taken from a data breach, social media, or public records. This makes the scammer seem legitimate and convincing as a real Congressional Federal representative.

The fraudster reassures you that they'll be taking care of the fraudulent charges for you. They just need you to **verbally confirm your password or provide them with other information** to confirm you are the owner of the account. They tell you "I'm going to process/take care of the suspicious activity. You might see the charges on your account at first but I'm going to reverse it." The call ends.

With the information acquired, **the scammer has access to your account** and can now change your phone number, email address, and account password on file to initiate and authorize transactions and transfers.

How to prevent this from happening to you

- **Call first, act second.** If you receive a suspicious phone call, thank them for the information and tell them you will handle it by contacting Congressional Federal yourself. Hang up immediately. Don't redial the number they called you from.
- **Do not respond to a suspicious or unexpected text.** Do not give out any information no matter what type of emergency they create or how trustworthy they sound.
- Remember that the name or number displayed can also be spoofed so the caller ID displays a name or number you recognize. **Call our verified main number (703-934-8300)** found on a statement, our app, or our website.
- **Remember we will never ask you to send money to anyone**, including yourself, to "reverse a transfer," "receive a refund," or anything similar.
- **Do not share any access code, password, or PIN** with anyone who contacts you requesting it.