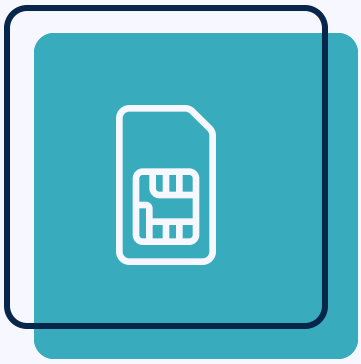
Stay One Step Ahead of Fraudsters

Protect Your 2FA!
"Fraudsters Are Getting Smarter—But So Can You!"

1 Don’t Share Your 2FA Codes

Fraudsters may try to trick you into giving them your verification code by pretending to be your credit union or a trusted service. **Remember**: Your credit union will never ask for your 2FA code via phone, email, or text.
You can always verify requests directly through your credit union's official customer service channels.



2 Watch for SIM Swapping

Fraudsters can hijack your phone number by transferring it to another SIM card, giving them access to your 2FA codes. Protect your mobile account with a PIN or password and report suspicious activity immediately.

3 Use Authentication Apps Instead of SMS

SMS-based 2FA can be vulnerable to SIM-swapping and phishing attacks. Consider using an authentication app like Google Authenticator or Microsoft Authenticator for stronger protection where possible.