# FRAUD PREVENTION TIPS

As digital banking continues to grow, so do the tactics used by fraudsters to deceive consumers. Credit union members are being targeted with increasingly sophisticated schemes designed to steal personal information, credentials, and even funds.
To help you stay informed and protected, we've outlined the top five scams currently affecting credit union members and the practical steps you can take to safeguard your accounts.

## 1. PHISHING & SMISHING SCAMS

Phishing (email) and smishing (text message) scams remain among the most common types of fraud. Members receive messages that appear to come from their credit union, often warning of "unusual account activity" or requesting verification of information. These messages are designed to trick recipients into clicking on malicious links or sharing personal details.

**PHISHING SCAMS (EMAIL)**

Phishing scams are fraudulent emails designed to steal your data.
Phishing scams may include:

- **Account compromise**: An email stating there is unusual activity on your account with a link to click to "verify your identity."
- **Account update**: An email claiming your account information could not be verified, so you must click a link to resolve the issue.
- **Fake invoice**: A fraudulent invoice or a payment request, typically with a link directing users to a fake website.

**SMISHING SCAMS (TEXT OR SMS)**

Smishing scams are fraudulent text messages designed to trick you into revealing personal information.
Smishing scams may include:

- **Suspended card**: A text message claiming your debt card has been suspended. The message then provides a link or phone number for you to reactivate it.
- **Prize winnings**: If you receive a text message notifying you of a prize win and requesting your information, be aware that this may be a scam.

**HOW TO PROTECT YOURSELF FROM PHISHING AND SMISHING**

If you are unsure of an email or contact us at 940.761.8600 or toll-free at 800.376.7825 Always keep the following in mind when receiving emails and text messages:

- Never click links or open attachments from unknown senders.
- PosTel Credit Union will never ask for your full account number, PIN, or password by email or text.
- **Be cautious of messages that create a sense of urgency**. Scammers use alarming language to pressure you into acting quickly before you have time to think or verify the information.

## 2. BANK IMPERSONATION CALLS (PHONE SPOOFING)

Scammers use technology to make their phone number look like it's coming from your bank or credit union. They sound professional and may already know some of your personal details. Then they ask for your account number, security code, or one-time passcode — information that allows them to access your accounts.
How to protect yourself from phone spoofing:

- If someone calls claiming to be from your credit union and asks for sensitive information, hang up immediately.
- Call the credit union at 940.761.8600 to confirm whether there's really an issue.
- Never share a one-time passcode with anyone, even if they say they're from your credit union.

## 3. ZELLE® AND P2P PAYMENT SCAMS

Scammers pretend to be from your credit union's fraud department. They call or text you, claiming there's a suspicious transaction on your account. To "reverse" the charge, they tell you to send money to yourself through a cash app or another P2P (peer-to-peer) payment app, but the money actually goes straight to them.
How to protect yourself from peer-to-peer payment scams:

- Remember: Zelle and other P2P payments are instant and usually can't be reversed.
- Never send money to anyone you don't personally know and trust.
- If you receive a suspicious message about a cash app transaction, hang up and call your credit union directly.

## 4. BANK IMPERSONATION CALLS (PHONE SPOOFING)

Scammers use technology to make their phone number look like it's coming from your bank or credit union. They sound professional and may already know some of your personal details. Then they ask for your account number, security code, or one-time passcode — information that allows them to access your accounts.
How to protect yourself from phone spoofing:

- If someone calls claiming to be from your credit union and asks for sensitive information, hang up immediately.
- Call the credit union at 940.761.8600 to confirm whether there's really an issue.
- Never share a one-time passcode with anyone, even if they say they're from your credit union.

## 5. ACCOUNT TAKEOVER VIA SOCIAL ENGINEERING

Scammers gather personal details, such as your birthday, email address, or physical address, from social media or data breaches. They use this information to reset your online banking credentials and take over your account.
How to protect yourself from social engineering attacks:

- Use strong, unique passwords for each account.
- Enable multi-factor authentication when available.
- Avoid sharing personal information on social media that could help someone guess your security questions.

## 6. FAKE CHECK & OVERPAYMENT SCAMS

This classic scam involves receiving a check that appears legitimate, often for a job offer, online sale, or prize, and being asked to send part of the money back. The check later bounces, leaving you responsible for the loss.
How to protect yourself from fake check scams:

- Be cautious of any unexpected check, especially if asked to return funds.
- Wait until checks fully clear before using any deposited money.
- Bring questionable checks to your credit union for verification.

## 7. MONITOR YOUR ACCOUNTS WITH POSTEL'S ONLINE APP

Regular account monitoring is one of the most effective ways to prevent fraud. With PosTel's App, you can:

- View recent transactions in real time
- Set up alerts for suspicious or unusual activity

## STAY INFORMED AND PROTECTED WITH POSTEL FAMILY CREDIT UNION

Fraud tactics continue to evolve, but awareness and vigilance are your best defenses. Be cautious of unsolicited calls, texts, or messages, and remember that we will never ask for sensitive information through unsecured channels.

If you ever notice something unexpected, contact us immediately.