NCE Credit Union wants you to be aware of the scams and frauds

Online Shopping & Marketplace Scams

Buying or selling on Facebook Marketplace, eBay, Craigslist, or other resale apps…..but something seems off.

Scammers use fake profiles, fake payment confirmations, and try to move communication off the platform.

- Someone insists on paying with gift cards, payment apps, or overpaying
- A seller who won't provide additional photos
- A buyer who is pushy or won't meet in person

- Only use built-in platform messaging
- Meet in public locations or police safe spots
- Avoid sending money before seeing the item

Toll Scams

You get a text saying you owe a toll, parking ticket, or driving violation – with a link to "pay now and avoid penalties."

The scammer wants your debit/credit card number or online banking login.

- Messages with vague details ("you missed a toll on 10/14")
- Fake or shortened website links
- Threats of late fees or license suspension

- Do no click the link.
- If you're unsure, contact the Texas Authority directly.

Phishing & Text Message Scams

You receive an email or text that looks like it's from your bank, a delivery company, a streaming service, or an online account.

The message often says there's a problem or something urgent (like a locked account or unpaid fees). It asks you to click a link and log in.

- Messages that create urgency ("Act now," "Your account is locked")
- Links that don't match the real website
- Requests for logins, account numbers, or personal details

- Do not click the link.
- Go directly to the company's website or app to check your account.
- Delete the message or report it as spam.

Card Skimming & ATM Fraud Scams

Scammers sometimes attach small, hidden devices to ATMs or card readers. These devices can steal your card number when you insert or swipe your card

The skimming device captures your card information, and sometimes a tiny camera records your PIN. The scammers then use your card number to make unauthorized withdrawal or

- An ATM or card reader that looks loose, damaged, or "chunky"
- A keypad that feels raised, spongy, or thicker than usual
- Outdoor ATMs, standalone ATMs, or gas pump card readers that are not frequently monitored.

- Use ATMs located inside your credit union whenever possible.
- Gently tug the card slot before inserting your card. If it feels loose or moves, don't use it.
- Cover the keypad with your hand when entering your PIN to block hidden cameras.


Elder & Caregiver Targeting Scams

Scammers call, text, email, or visit older adults directly – often sounding friendly, compassionate, or helpful.

They slowly gain trust, then request money, access to accounts, or personal information.

- Sudden new “friends” or helpers
- Requests to keep conversations secret
- Pressure to act quickly

- Encourage regular communication with family or caregivers
- Review financial statements together
- Call the credit union at the first sign of pressure or confusion

Imposter & “Authority” Scams

You get a call, text, email from someone claiming to be the IRS, Social Security, your credit union, law enforcement, or a family member in trouble.

The scammer tries to build trust or fear – and pushes you to act quickly before you can think.

- A caller who demands payment immediately
- Requests for gift cards, wire transfers, or “verification codes”
- Caller ID that looks legitimate – scammers can fake it

- Hang up
- Call the real organization using a phone number you trust

Reference Table

What it looks like

How it Works

Red Flags to Watch for

What To Do

NCE Credit Union wants you to be on guard!