COMMON TYPES OF SCAMS

Learn current scam tactics, so you know how to protect yourself from fraudsters.

CREDIT CARD & HELOC SCAMS

Fraudsters offer to pay off your credit card or home equity line of credit. They send you a check and tell you to deposit it. At first, your balance may look paid, and your available credit increases. Later, the check returns as fake. You still owe your original balance, and any money sent is gone.

How to Prevent Line-of-Credit Fraud:

- Don't let others make payments for you.
- Never deposit checks or move funds at someone else's request.
- Never use your available credit for someone else.

ELDER FINANCIAL EXPLOITATION (EFE)

EFE happens when someone takes advantage of elderly people or people with disabilities for financial gain. In Tennessee, it is a criminal offense to knowingly abuse, neglect, or exploit any adult.

Signs of EFE:

- Checks written as loans or gifts to unfamiliar people.
- Statements sent to alternate addresses.
- New credit cards opened in your loved one's name.
- New powers of attorney that the person does not understand.

If You Suspect Exploitation:

- Contact KTVAECU® or other institutions like the Social Security Administration.
- Report concerns to local Adult Protective Services.
- Add a trusted contact to the account. Trusted contacts are notified if EFE is suspected.

AI VOICE SCAMS

Scammers use artificial intelligence (AI) to clone voices of people you trust from audio clips posted on social media. If you receive a panicked phone call from a loved one asking for money, hang up and call them back on a trusted number. Don't send money until you know the call is real.

PHISHING AND IMPERSONATION

Fraudsters spoof phone numbers and email addresses to make you think they're from the Credit Union. They send fake texts asking you to send money, confirm a transaction, or verify your information.

Red Flags:

- Texts from a 10-digit phone number. Our text alerts ALWAYS come from short codes.
- Requests for login information, PINs, card numbers, or money.
- Suspicious links.
- Urgent language or threats.

We will never ask for your login username or password, account reset code, PIN, card numbers, SSN, or full account details. We do not send surprise links or pressure you to act quickly. We will never ask you to send us money.

ROMANCE SCAMS

Romance scams use fake online profiles to gain trust or emotional connection. Once trust is established, fraudsters ask for money or financial help.

Signs of a Romance Scam:

- Vague or limited profiles.
- Attempts to move the conversation off the dating platform.
- Quick declarations of love or commitment.
- Avoids meet-ups or video calls.
- Requests for money or help.

How to Protect Yourself:

- Limit what you share online.
- Do your research.
- Go slow and ask a lot of questions.
- Be cautious with anyone you haven't met in person. Stop contact immediately if money is brought up.

SKIMMER SCAMS

Skimmers are devices hidden on ATMs, point-of-sale terminals, or gas pumps to steal card data. Fraudsters use this stolen data to make unauthorized purchases from your accounts.

SCAN Before You Pay:

- S: Scan the area for anything out of place.
- C: Check for tampered equipment or damaged parts.
- A: Assess the card reader. Does it match the rest of the machine?
- N: Nudge the keypad and card reader. If something is loose, use a different machine.

tvacreditunion.com/security

Federally Insured by NCUA.

FACTS ABOUT FRAUD

Tennesseans lost more than $157,000,000 to fraud in 2024.

About **28%** of people say they don't use a strong password for their financial accounts.

LOGIN
***

Most people have saved their account information on at least one retail website.

One in three Americans reports being a victim of a cybercrime.

It costs less than $5.00 for fraudsters to purchase stolen card information. A victim's social and birthday can cost up to $100.00.

$ $ $ $ $ $ $ $ $

Federally Insured by NCUA.

KNOXVILLE TVA EMPLOYEES CREDIT UNION®

SIGNS OF A SCAM

IMPERSONATION OF SOMEONE YOU KNOW

Fraudsters pretend to be from organizations like the Social Security Administration, IRS, Medicare, utility providers, tech companies, or charities.

CLAIMS OF A PROBLEM OR PRIZE

Messages say you owe money, your account has an issue, a family member is in trouble, or your device has a virus. Fraudsters claim you've won a prize but must pay a fee to receive it.

PRESSURE TO ACT IMMEDIATELY

Fraudsters want you to act before you think it through. They may threaten legal action or account closure.

REQUESTS FOR SPECIFIC FORMS OF PAYMENT

Be suspicious of messages that insist you pay with cryptocurrency, gift cards, cashier's checks, or money wires. Fraudsters send false checks, then ask you to deposit them and send the money.

The KTVAECU Promise

KTVAECU will NEVER contact you to ask for your username or password, account reset codes, PIN, debit/credit card numbers, social security number, or account information. Never share this information with anyone.

We may contact you about your account at times. When we do, we may ask questions to validate your identity, but **we won't ask for your complete account numbers, card numbers, or online login information.**

tvacreditunion.com/security

Federally Insured by NCUA.

PROTECT YOURSELF FROM FRAUD

Build Strong Security Habits

To protect yourself from fraud, adopt these essential online habits:

- **Use Strong Passwords**
  Choose long passwords with uppercase and lowercase letters, numbers, and special characters.
- **Set Up Two-Factor Authentication**
  Two-factor authentication adds an extra step to confirm it's really you.
- **Customize Security Questions**
  Set up security questions with answers only YOU would know.
- **Protect Your Personal Information**
  Limit who you trust with your information. Never carry sensitive documents like your Social Security card. Shred personal documents before you throw them away.

Stay in the Know with Account Alerts[1]

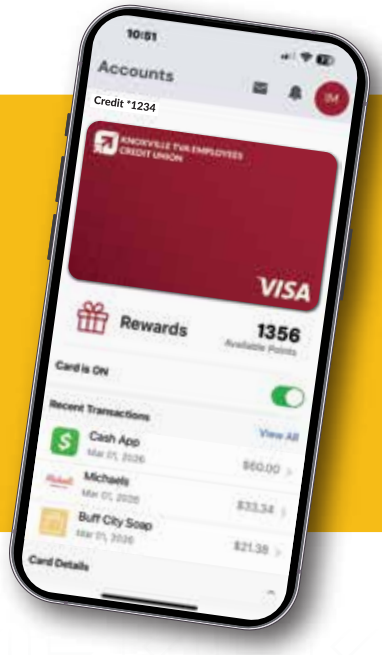
Account Alerts[1] help you spot unusual activity early. Set alerts through digital banking for:

- **Direct Deposits[2]**
  Get notified when a deposit posts to your account.
- **Large Purchases or Transactions**
  Receive alerts when a large transaction has been made on your account.
- **Login Attempts**
  Know about login attempts on your account.
- **Profile or Password Changes**
  Get alerted whenever your account information changes.
- **New Device Added**
  Get notified when a new device has been added to your account.

Upgrade Your Card Security with Card Controls[3]!

We make it even easier to protect yourself from fraud. With just a few taps, turn your card on or off, view recent transactions, customize alerts, and more.

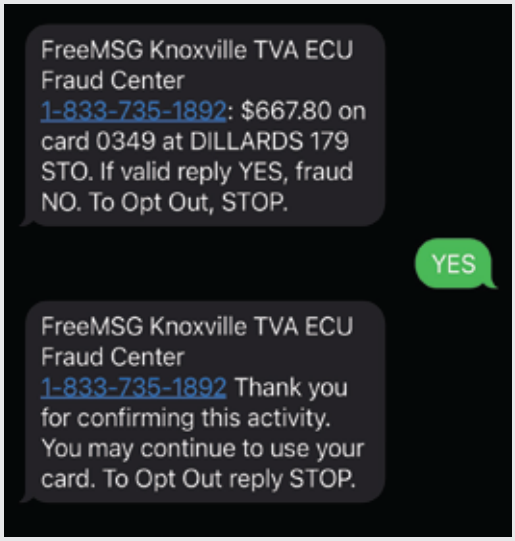
Learn More!
tvacreditunion.com



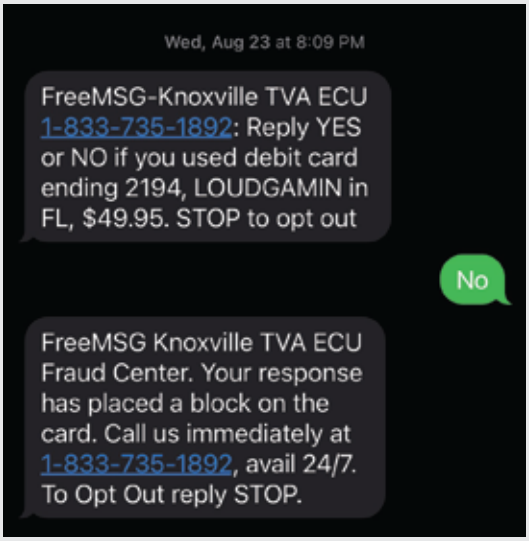
Federally Insured by NCUA. 1. Some restrictions may apply. Message and data rates may apply. Not all wireless carriers support FTEU (Free To End User) texting. If your carrier does not support these texts or your mobile number is not on file, you will continue to receive phone calls if unusual activity occurs on your card. Ask for details. 2. Some restrictions may apply. Ask for details. 3. Some restrictions may apply. Ask for details. Message and data rates may apply from your wireless carrier. Available to qualifying Members.

LOOK OUT FOR TEXT SCAMS

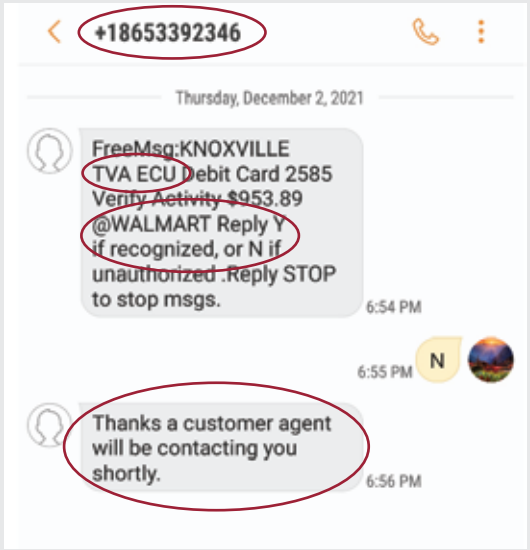
Fraudsters send fake text messages that look like real Credit Union Fraud Text Alerts. They claim there's a recent transaction or a problem with your card. **Here are some examples of what our authentic messages look like:**



If you receive a Card Fraud Text Alert and respond **YES**, this is the message you'll receive back.



If you receive a Card Fraud Text Alert and respond **NO**, this is the message you'll receive back.



Spot the Fake Card Fraud Text Alert

Red Flags:

- Text from a full-length phone number instead of a short code.
- Requests for login information.
- Contains grammar or spelling errors.
- Says an agent will contact you with no further information given.

IMPERSONATION FRAUD TIP

Never give out your card credentials! We already have this information and will not ask you for it.

After reaching out in a fake card fraud text, scammers may try to pressure you into giving out this information in an attempt to "tokenize" your cards into a digital wallet. Once your cards are tokenized by a scammer, it can be very difficult to reverse.

Never share your digital banking username, password, account reset codes, or PIN with anyone. KTVAECU will not ask you for complete account numbers, card numbers, or online credentials.

What Should I Do?

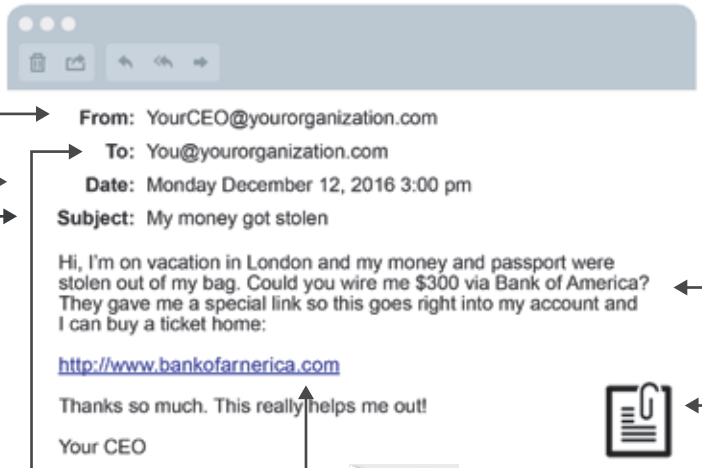
If you receive a text you suspect to be fraudulent, don't respond or call any numbers provided. If you suspect fraud on your account or are unsure about the identity of a caller, **contact us directly at (865)544-5400**, and we'll work with you to resolve any problems or concerns.

For more tips, visit our security webpage!

tvacreditunion.com/security

Federally Insured by NCUA.

EMAIL RED FLAGS



FROM

- The sender is someone you don't recognize or normally communicate with.
- The sender is someone you know, but the message is unusual or out of character.
- The sender's email address is from a suspicious domain.
- The email is unexpected or unusual and contains a hyperlink or attachment.

DATE

- The email is something you would expect during normal business hours, but it was sent at an unusual time, like 3 AM.

HYPERLINKS

- Hyperlinks included in the email show a different link-to address when you hover over them with your mouse.
- The email only contains long hyperlinks with no further information.
- The email contains a hyperlink that misspells a known website.
- For instance, www.bankofarnerica.com - the “m” is really two characters - “r” and “n”.

TO

- You're cc'd on an email sent to people you don't know.
- The email is sent to an unusual mix of people, such as a random group from your organization or a list of unrelated addresses.

SUBJECT

- The subject line is irrelevant or doesn't match the message content.
- The email message is a reply to something you never sent or requested.

ATTACHMENTS

- The sender includes an email attachment you aren't expecting or makes no sense with the message.
- The attachment is a possibly dangerous file type.

CONTENT

- The sender urges you to click a link or open an attachment quickly to avoid something bad or
- gain something valuable.
  The email is out of the ordinary. It has poor grammar or spelling errors.
  The sender asks you to click a link or open an attachment that seems illogical.
  You have an uncomfortable gut feeling about the sender's request to open an attachment or click a link.

Check out our security webpage for more tips!

tvacreditunion.com/security

Find us on Instagram™ for videos about looking out for fraud!

@tvacreditunion

Federally Insured by NCUA. Instagram is a registered trademark of Instagram, LLC.