COMMON TYPES OF SCAMS

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

ELDER FINANCIAL EXPLOITATION (EFE)

EFE is when fraudsters take advantage of elderly people or adults with disabilities for monetary or personal benefit, profit, or gain. In Tennessee, knowingly abusing, neglecting, or exploiting any adult is considered an offense.

Signs of EFE:

- Checks written as "loans" or "gifts" to someone the family doesn't know.
- Bank and credit card statements that go to alternate addresses.
- New credit cards opened in your loved one's name.
- New powers of attorney the older person doesn't understand.

If you see or know of an adult being exploited or abused:

- Alert KTVAECU® or another institution like the Social Security Administration.
- Report the abuse to your local Adult Protective Services.
- Add a trusted contact to their account. Trusted contacts will be notified if we suspect EFE.

FAMILY EMERGENCY SCAM

Artificial Intelligence (AI) can clone voices 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 number you trust. Don't send money until you know the call is legitimate.

FACETIME AND PHONE CALL SCAMS

If someone calls you asking for your online banking login, card numbers, or other sensitive information, hang up immediately! Recently, fraudsters have even placed calls through FaceTime. KTVAECU will never call you using FaceTime or other video chat applications!

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.

Here's how to spot a fake text or email:

- Texts from a 10-digit phone number.
  - Our text alerts ALWAYS come from a short code.
- Requests for login information or money.
  - We will never ask for your online banking username, password, account reset codes, PIN, debit/credit card numbers, social security number, or account information.
  - We will never ask you to send us money.
- Suspicious links.
  - We'll never ask you to click or forward a link.
- Urgent language or threats.
  - Fraudsters pressure you to act fast.

ROMANCE SCAMS

Some fraudsters use a fake online identity to gain a victim's affection and trust. They pretend to be interested in a romantic relationship or close friendship to manipulate and steal from their victims.

Signs of a romance scam:

- Vague or limited profiles.
- Attempts to move the conversation somewhere else.
- Early admissions of love.
- Avoids meeting or video calling.
- Requests for money or help with transactions.

How to protect yourself:

- Limit what you share online.
- Do your research.
- Go slowly and ask a lot of questions.
- Be suspicious if you have not met the person.
- Watch out for requests for money or personal account information.
- If you think you're being scammed, stop contact immediately!

SKIMMING SCAM

Skimming occurs when devices are illegally installed on ATMs, point-of-sale (POS) terminals, or gas pumps to capture card data. Fraudsters use this stolen data to steal from your accounts.

SCAN for skimming:

S: Scan your surroundings. Does anything look out of place?
C: Check for tampering. If panels are dented or broken, don't use the machine.
A: Assess the card reader. Does it look like the rest of the machine?
N: Nudge the keypad and card reader. Skimmers are meant to be temporary and might have some give.

tvacreditunion.com/security

Federally Insured by NCUA.

FACTS ABOUT FRAUD

Tennessee had over 8,000 complaints of online fraud in 2023. Victims lost more than $161 million.

About 28% of people acknowledge they do not use a strong password for financial account logins.

LOGIN
***

Most people have their account information saved on at least one retailer's website.

One in three Americans report 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.

tvacreditunion.com/security

Federally Insured by NCUA.

KNOXVILLE
TVA EMPLOYEES CREDIT UNION

SIGNS OF A SCAM

IMPERSONATION OF SOMEONE OR A COMPANY YOU KNOW

Fraudsters pretend to be from a government organization like the Social Security Administration, the IRS, Medicare, or businesses like your utility provider, a tech company, or a charity.

CLAIMS OF A PROBLEM OR PRIZE

Be cautious of messages that say you're in trouble with the government, you owe money, there's a family emergency, or your device has a virus. Scammers also ask you to verify information to fix a problem with your account. Others lie and say you won a prize, but you must pay a fee to get it.

PRESSURE TO ACT IMMEDIATELY

Fraudsters want you to act before you have time to think. They may threaten legal action or claim your device is corrupt.

REQUESTS TO PAY IN A CERTAIN WAY

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

The KTVAECU® Promise

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

We may need to contact you about your accounts at times. When we do, we may ask questions to validate your identity, but **we will not ask you for complete account numbers, card numbers, or online credentials.**

tvacreditunion.com/security

Federally Insured by NCUA.

WAYS TO FIGHT FRAUD!

Your security is our top priority! While we always work to keep your accounts safer, there are steps YOU can take to protect yourself.

Establish Good Security Habits

To protect yourself from fraud, consider adopting these essential online habits:

- **Strong Passwords**
  Longer passwords with uppercase, lowercase, numbers, and special characters are harder to crack!
- **Two-factor Authentication (2FA)**
  Two-factor authentication is like a security guard verifying your identity before letting you access your account. It requires you to respond on another device with a passcode to make sure it's really you!
- **Security Questions**
  Set up security questions with answers only YOU know.
- **Vigilance and Privacy**
  Be careful of who has your information. Never carry sensitive documents like your social security card with you. Shred personal documents before you throw them away.

Stay in the Know with Account Alerts[1]

Set up Account Alerts through online banking[2] or the KTVAECU® Mobile App[3] to stay updated about account activity. Choose push, text, or email notifications for:

- **Deposit**
  Get notified when a deposit posts to your account.
- **Large Purchase**
  Receive alerts when a large transaction has been made on your account.
- **Login**
  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.

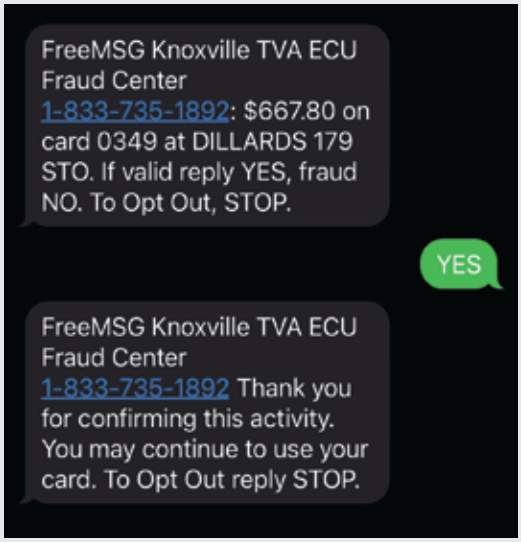
Upgrade Your Card Security with Control My Card[4]!

It's never been easier to protect yourself against fraud and keep your money more secure. With just a few taps, Control My Card by KTVAECU lets you turn your card on or off, customize alerts, change your PIN, and more!

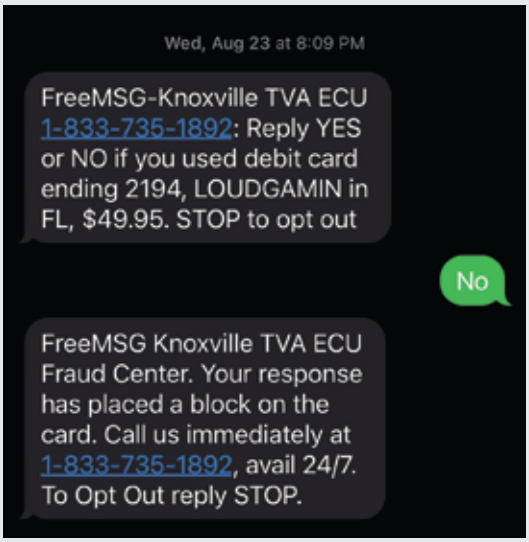
Federally Insured by NCUA. 1. Some restrictions may apply. Ask for details. Message and data rates may apply from your wireless carrier. Ask for details. 2. Some restrictions may apply. Ask for details. 3. Available to qualifying Members. Some restrictions may apply. Message and data rates may apply. Ask for details. 4. Some restrictions may apply. Ask for details. Message and data rates may apply from your wireless carrier. Ask for details. Control My Card by KTVAECU® is a registered trademark of Knoxville TVA Employees Credit Union. Available to qualifying Members.

LOOK OUT FOR TEXT SCAMS

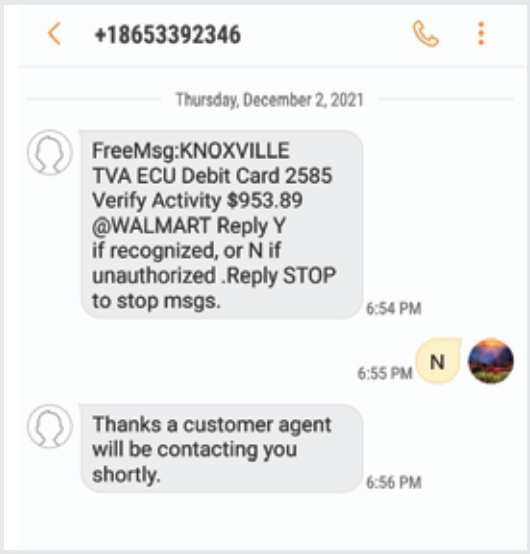
Fraudsters send fake text messages pretending to be the Credit Union. They claim there has been a recent transaction on your account. These messages can look like real Card Fraud Text Alerts[1] from KTVAECU®. **Here are some examples of authentic text messages from us:**



If you receive a Card Fraud Text Alert and answer **YES**, this is the message you should receive back.



If you receive a Card Fraud Text Alert and answer **NO**, this is the message you should receive back.



This is an example of a fake Card Fraud Text Alert message. One red flag is the phone number. Fraudsters often text from a full-length phone number instead of a short code.

Any response to this text will invite the fraudster to call you. Once you're on a call, they will try to trick you into giving your account information so they can access your accounts.

Never share your online 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?

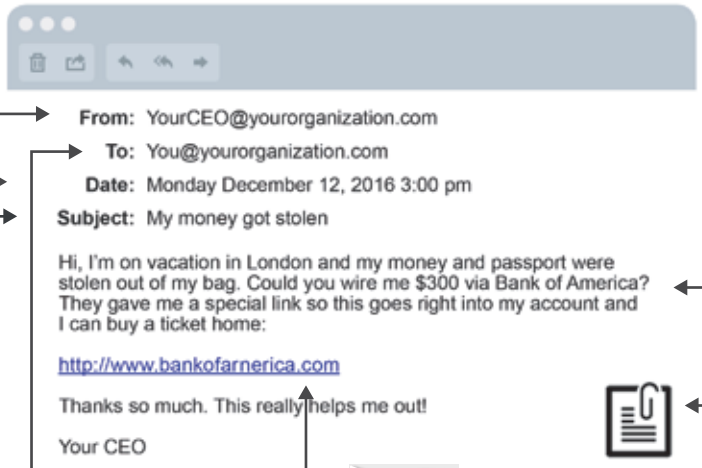
If you receive a text you suspect to be fraud, don't respond or call any numbers provided. If you suspect fraud on your account or are unsure about the identity of a caller, contact us directly at (865) 544-5400.

For more tips, visit our security webpage!

tvacreditunion.com/security

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.

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 also 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.