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