COMMON TYPES OF SCAMS

Knowledge is your best defense. Knowing what to look for is a great starting point. Below are recent scams we've seen in our community and how they work.

Text Alert Scam

Fraudsters are making their way to your bank accounts through text messages pretending there has been a recent transaction. You'll get a text alert asking if you recently completed a transaction. Regardless of how you answer, the fraudster will ask you to call a number, or you will receive a phone call from a fraudster who will attempt to trick you into giving your account information so they can access your accounts. If you question the identity of the call, ask for their company contact information and tell them you need to call them back later. Then, verify their information by calling the company at the phone number provided on their website.

Phishing Text Message

Phishing is the fraudulent practice of sending emails or texts claiming to be from a reputable company to induce individuals to reveal personal information, such as passwords and account numbers.

Look for email or text red flags:

- Be sure you recognize the company or financial institution.
- Look closely at the link by hovering over with your mouse. Make sure the link goes to a website you are familiar with.
- Spelling and grammar errors are a red flag.
- Slow down, and don't be pressured to act urgently. Scammers want you to act fast, so you miss the red flags.

Romance Scam

Romance scams occur when a criminal adopts a fake online identity to gain a victim's affection and trust. The scammer then uses the illusion of a romantic or close relationship to manipulate and/or steal from the victim.

Signs of a Romance Scammer:

- Vague, limited profiles
- Tries to take the conversation elsewhere
- Professes love early on
- Avoids meet-ups and video chat completely
- Requests for money
- Asks for your help with financial transactions

To protect yourself or someone else from romance scams!

- Limit what you share online.
- Do your research.
- Go slowly and ask a lot of questions.
- Listen to your gut.
- Be suspicious if you have not met the person.
- Be alert if you are asked to send money or share personal account information.
- If you suspect a romance scam, stop all contact immediately.

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

Elder Financial Exploitation (EFE)

EFE is the illegal or improper use of an elderly or adult with a disability's money, property, or other resources for monetary or personal benefit, profit or gain. In Tennessee, knowingly abusing, neglecting, or exploiting any adult is considered an offense.

Some red flags of EFE:

- Checks written as "loans" or "gifts" to someone the family doesn't know.
- Bank and credit card statements that no longer go to the customer's home.
- New credit cards show up in your loved one's name.
- New powers of attorney the older person does not understand.

If you see or know of an Elder being exploited or abused, you can do the following:

- Alert KTVAECU® or other institutions like Social Security Administration.
- Report the abuse to your local Adult Protective Services
- Add a trusted contact to their account. A trusted contact is someone we can put on an account to notify if EFE is suspected.

Family Emergency Scam

Artificial Intelligence (AI) can now clone voices by taking audio clips people post on social media. Scammers generate a panicked phone call about a "family member in trouble." If you receive a panicked phone call from a family member in urgent need of money, don't trust the voice because it might not actually be your family member. It could be AI. Instead, slow down the moment: Tell them you're going to hang up and call them right back. Then, reach out to your family member using a phone number you know to verify the first phone call. Don't send money until you verify the "story" is legitimate.

Skimming Scams

Skimming occurs when devices are illegally installed on ATMs, point-of-sale (POS) terminals, or gas pumps to capture data or record cardholders' PINs. Fraudsters use the data to steal from your accounts.

How to avoid skimming?
SCAN the area.
S: Scan your surroundings. Is it well-lit? Is there an attendant? Is there anything that looks out of place? Just like in school, safety first.
C: Check for any tampering. If panels are dented or broken, skip using the machine.
A: Assess the card reader. Does it look like the rest of the machine? The colors should match, and graphics should not be misaligned or cut off.
N: Nudge the keypad and card reader to see if they move. If they do, don't use it and report it immediately. Most skimmers are made to be temporary, so they usually have some "give" and can come loose.

Check out our security webpage for more tips!
tvacreditunion.com/security

KNOXVILLE TVA EMPLOYEES CREDIT UNION™