ACCESS
COMMUNITY CREDIT UNION

FRAUD PREVENTION GUIDE

PAUSE.
PREVENT.
PROTECT.

SPOT THE SIGNS

PROTECT YOUR INFO

PROTECT YOUR ACCOUNTS

REPORT FRAUD FAST

If you have given out personal information please call us immediately.

(806) 353-9999

CONTENTS

Common fraud schemes

Caller ID Spoofing

This technique is used to make an incoming call appear as though it is coming from a trusted or familiar source, such as a local number, a government agency, a bank, or even the recipient's own number.

- **DO NOT** trust caller ID alone to determine the caller's authenticity.
- **NEVER** provide sensitive information such as your Social Security number, passwords, or banking details over an unsolicited call.

Threatening emails

Fraudulent or malicious messages designed to frighten, intimidate, or pressure recipients—either customers or employees—into taking immediate action that results in financial loss, identity theft, or compromised security.

- **Do Not Engage:** Never reply, click links, or open attachments in threatening, unexpected, or suspicious emails.
- **Verify Independently:** If a message claims to be from a legitimate source (bank, company, government), contact them directly through official websites or phone numbers.

Phishing

When criminals use scam emails, text messages or phone calls to trick their victims. The aim is often to make you visit a website, which may download a virus onto your computer, or steal bank details or other personal information.

- **Never** click links or download attachments from unexpected emails or messages.
- **Be wary** of urgent, threatening language demanding immediate action.

Impersonation

When a scammer pretends to be a trusted person or organization to steal money or personal information. Scammers often pose as banks, government agencies, businesses, or family members and use phone calls, texts, emails, or fake websites to appear legitimate.

- **Never** act immediately under pressure or threats.
- **Do not** click suspicious links or attachments.

Common fraud schemes

Romance scam

A romance scam happens when a scammer creates a fake online relationship. These scams often begin through social media, dating apps, or messaging platforms. They tend to prey on widows to gain trust and eventually steal money or personal information.

- **Do not** trust excuses for why they cannot meet or video chat.
- **Do not** send money to someone you have never met in person.
- **Do not** send gift cards, wire transfers, or cryptocurrency.

Unexpected Mailed Check

Scammers randomly mail you a check out of nowhere and encourage you to deposit it. The check may look real, but it is usually fake or altered. Once deposited, they'll ask you to send part of the money back or use it for a "task," before the check ultimately bounces.

- **Do not** deposit checks you were not expecting or did not request.
- **Do not** use deposited funds until the check has fully cleared and is verified by your financial institution.
- **Do not** follow instructions to "keep a portion" and return the rest.

AI & Deepfakes

AI and deepfake scams use artificial intelligence to create fake but realistic audio, video, or images that impersonate real people. Scammers may clone a person's voice or face to appear as a trusted contact, coworker, or authority figure in order to trick victims into sending money or sharing sensitive information.

- **Do not** share account details if someone contacts you unexpectedly, even if they sound familiar.
- **Do not** rely on caller ID, profile photos, or video appearances as proof of identity.
- **Do not** trust voice or video alone. AI can fake both.

Authorized payment

Scammer tricks you into willingly sending money to them. Unlike unauthorized fraud, the payment is approved by the victim; often because they were manipulated into believing the request was legitimate.

- **Do not** follow instructions to move money to "safe accounts" or "protect your funds."
- **Do not** ignore warning signs like secrecy, urgency, or requests to bypass normal processes.

Common fraud schemes

Tech support

Scammers pretend to be from companies like Microsoft, Apple, or antivirus providers. They claim your device is infected, hacked, or has serious errors and pressure you to give them access or pay for fake repairs.

- **Do not** allow remote access to your computer or phone from unsolicited contacts.
- **Do not** pay for "repairs" or software from unexpected tech support calls or messages.

Investment scams

Investment scams trick people into putting money into fake or misleading opportunities that promise high or "guaranteed" returns with little or no risk. These scams often involve cryptocurrency, stocks, real estate, or exclusive "insider" opportunities.

- **Do not** trust unsolicited investment advice from social media, texts, or cold calls
- **Do not** share banking access or allow others to "manage" your investments without verification.
- **Do not** invest in opportunities that guarantee high returns with no risk.

Job Ad Scams

Job ad scams on Facebook often look like real employment opportunities but are posted by fraudsters trying to collect personal information or money. These fake listings may promise easy work, high pay, or remote jobs with little experience required.

- **Do not** apply to jobs that ask for payment to get hired or start working.
- **Do not** trust job offers that only communicate through social media messaging apps.
- **Do not** send money for "equipment," "training," or "onboarding fees."

Government imposter

Scammer pretend to be agencies like the IRS, Social Security Administration, or local law enforcement. They often claim you owe money, your benefits are at risk, or there is a legal issue that requires immediate action.

- **Do not** provide Social Security numbers, bank info, or verification codes.
- **Do not** trust caller ID. Government agencies do not demand payment this way.
- **Do not** believe threats of arrest, fines, or account suspension over the phone or email.

How you can protect yourself against fraud

- **Slow down-** Urgency is one of the biggest warning signs. Do not feel pressured or scared. Scammers prey off of fear and emotion.
- **Verify before you trust**- If something seems off, don't respond directly. Contact the organization using a number you already know is legitimate.
- **Never share your passwords or security codes-** We will NEVER ask for them. Use strong, unique passwords and enable multi-factor authentication.
- **Be cautious with links and QR codes-** This is important especially from unexpected messages.
- **Review your accounts regularly-** If something seems off, give us a call. You should NEVER have an unexpected deposit or withdraw.
- **Report anything suspicious right away-** The sooner you report it, the faster we can help protect your account.
- **Don't click links from unknown senders-** Even if the message looks legit. Scammers are good at making things look real.
- **Quick tip:** Be cautious of unusual payment requests **gift cards or urgent transfers** because those payments are hard to trace. If you're unsure, don't feel pressured, take a moment and reach out to us. **That pause can make all the difference.**

How Access protects you

At Access, protecting our members and their financial information is a top priority. While scammers continue to evolve their tactics, we work every day to help detect suspicious activity, secure your accounts, and provide support when fraud occurs.

Secure Online & Mobile Banking

Our online and mobile banking services use security measures designed to help protect your personal and financial information while you bank digitally.

Account Alerts & Notifications

Members can take advantage of account alerts to stay informed about transactions, balances, and account activity in real time.

Identity Verification Procedures

To help protect your accounts, we may ask questions to verify your identity before discussing account information or processing certain requests.

Debit & Credit Card Protection

We help monitor card activity for potentially fraudulent transactions and can assist with blocking or replacing compromised cards when needed.

FAQs

How do I know if something is a scam?
Scammers often create a sense of urgency, ask for personal information, request unusual forms of payment, or pressure you to act quickly. If something feels suspicious, pause and verify before responding.

What should I do if I clicked a suspicious link?
Change your passwords immediately, monitor your accounts for unusual activity, and contact us if you shared any personal or banking information.

Is it safe to use peer-to-peer payment apps?
Apps like Venmo, Cash App, and Zelle should only be used with people you know and trust. Scammers often use these apps because payments can be difficult to recover.

What are common signs of identity theft?

- Unfamiliar charges or withdrawals
- Bills or accounts you don't recognize
- Calls from debt collectors about unknown accounts
- Unexpected declines on legitimate transactions

What should I do if I mailed a check and it was altered or stolen?
Contact us immediately. Monitor your account closely and consider using secure payment methods or online bill pay when possible.

FAQs

Who can I contact if I have concerns about fraud?
If something feels suspicious, contact Access right away. We're here to help without judgment and support you through the next steps.

Are text messages from my financial institution always legitimate?
Not always. Fraudsters can spoof phone numbers and texts to appear legitimate. Never click suspicious links or provide information unless you verify the message directly with your financial institution.

Why would a scammer ask for gift cards or cryptocurrency?
Scammers prefer payment methods that are hard to trace and nearly impossible to reverse. Requests for gift cards, cryptocurrency, or wire transfers are major red flags.

ACCESS WILL NEVER:

- **Ask for your online banking login code**
- **Email you requesting a password change.**
- **Ask for your debit card pin**
- **Ask for screenshots of your account or verification messages**
- **Ask for full card numbers by text or email**

Additional resources

- **https://www.occ.treas.gov/topics/consumers-and-communities/consumer-protection/fraud-resources/types-of-consumer-fraud.html**
- **https://mycreditunion.gov/protect-your-money/prevention**
- **https://ncua.gov/regulation-supervision/regulatory-compliance-resources/fraud-prevention-resources**

Freeze your credit

1. Freeze with Equifax

- Online: Create an account at Equifax Freeze Page.
- Phone: Call (800) 349-9960 or (800) 685-1111.

2. Freeze with Experian

- Online: Submit a request at Experian Freeze Page.
- Phone: Call (888) 397-3742.

3. Freeze with TransUnion

- Online: Set up access at TransUnion Freeze Page.
- Phone: Call (888) 909-8872.

Contact us

806.353.9999

fraudsupport@accesscu.net

accesscreditunion.com

Are you a victim of fraud?

If you're unsure about something, please don't hesitate to reach out. Scams are designed to be confusing, and anyone can fall for them. There is no judgment here, only support, guidance, and care for our members.

Report fraud

- https://reportfraud.ftc.gov/
- https://www.identitytheft.gov/
- https://www.ic3.gov/
- Amarillo Police Department- (806) 378-3038