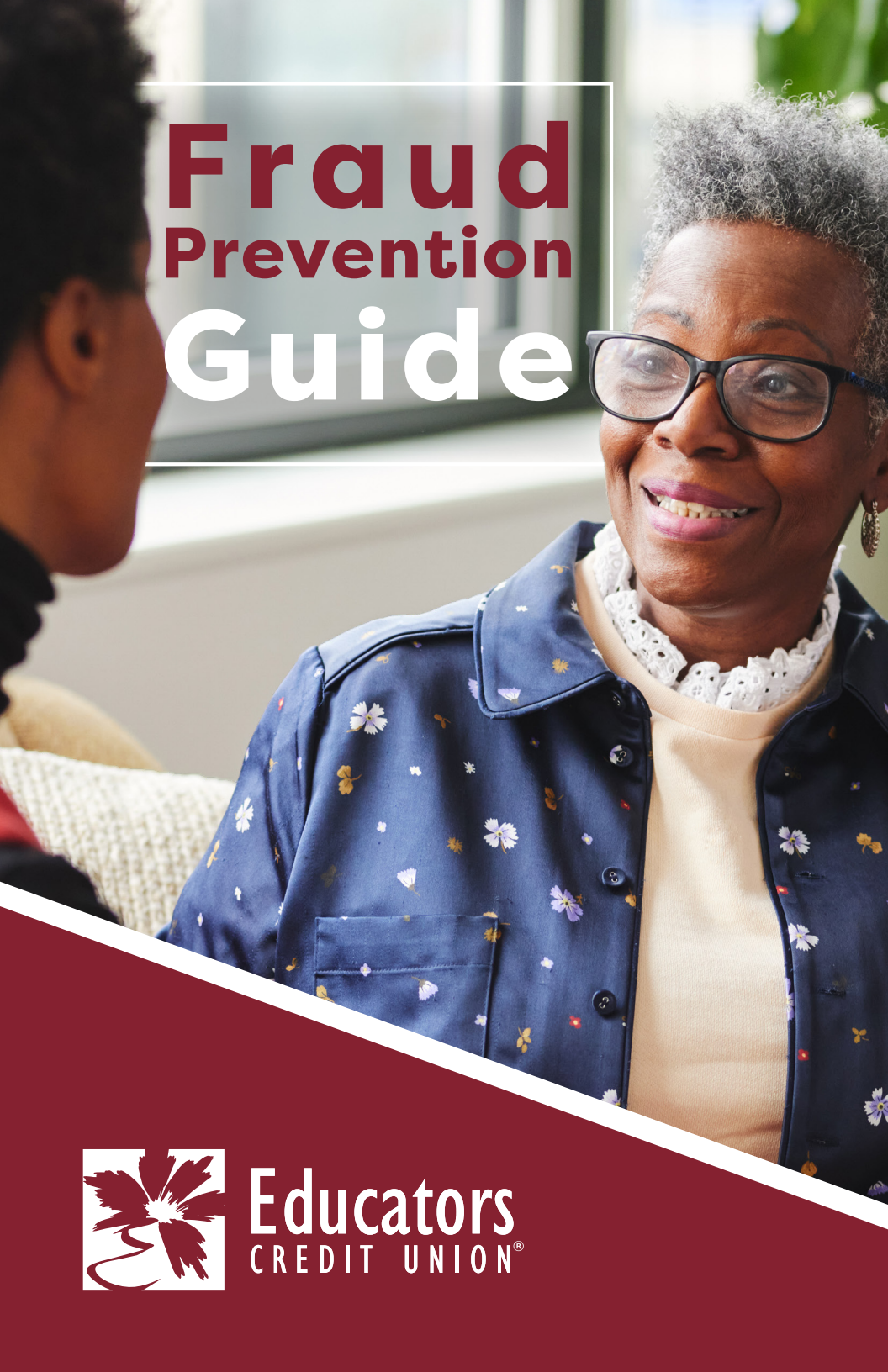


Fraud Prevention Guide

Educators CREDIT UNION®

Table of CONTENTS

At Educators Credit Union, we have an unwavering dedication to the financial well-being of our members.

As criminals introduce new and creative ways to commit fraud, our main priority is protecting you and your finances.

In this guide, you will read stories from unsuspecting victims, learn how to recognize the warning signs of a scam, and receive information on how to protect yourself from these scams. We hope this booklet gives you valuable information to help you and your loved ones from becoming victims of fraud.

Calls, Texts and Emails from Educators Credit Union

Did you receive a text, call or email from someone claiming to be from Educators Credit Union? We may text you to confirm a transaction, but we will never contact you first about your:

- Online Banking username or password.
- Card number or CVV (3 digits) on the back of your card.
- Full account (MICR) number.
- PIN.

You can always call us at 262.886.5900, so you can feel confident that you're talking to a member of the Educators Credit Union team.

Is it a scam?

Here are seven questions to help you.

If you answer ***yes*** to any of these questions, it's likely a scam.

- Were you asked to lie or hide information from your financial institution?
- Were you contacted unexpectedly about a payment, delivery or charge you didn't know about?
- Did someone call, email or text you asking for your username and password to Online Banking?
- Were you asked to wire money or buy gift cards?
- Did someone ask you to send back extra money because they overpaid you?
- Were you promised quick or easy money?
- Were any of the requests above presented as urgent or threatening?

SAFETY TIP

When in doubt, contact us at 262.886.5900! We're here to help you.

Seven tips to keep your accounts and personal information safe.

- **Never send or give anyone your Online Banking username and password.** There is no reason why anyone would ever need your login credentials to access your accounts.
- **Only log in from the Educators Credit Union Mobile Banking app or directly on our official website (ecu.com).**
- **Never act immediately.** Any legitimate business will never pressure you. Instead, they will allow you to decide when you're ready.
- **Keep your electronic devices up to date with the latest software updates.**
- **Don't send money back to someone who "accidentally" sent you money via digital payment.**
- **Use strong passwords.** A strong password is long and memorable, since longer passwords are harder for hackers to break. For instance, a password can be a long phrase with a mix of numbers and symbols. It's also essential to change your important passwords every three months and to not reuse passwords.
- **Verify, verify, verify.** If you receive an email, text message or phone call, verify it's from a trusted source.

Text message scam

It started with a text asking if Taylor spent $1,532 at Target.

Believing the text was from his credit union, he responded “NO.” Then, his phone rang.

"The woman on the phone told me the text was for fraud prevention," Taylor said. "She told me that she could help if I immediately gave her my username and password for Online Banking.”

Taylor followed these instructions. He believed she was reversing the fraudulent Target payment when in fact it was just the opposite.

“That’s where the scam was,” he said. “She took all the money out of my account. It was gone.”

Here’s how to identify this scam:

The person contacting Taylor about his account was pushy, and they insisted there was no other way to fix the problem besides following their instructions.

Here's how to protect yourself from this scam:

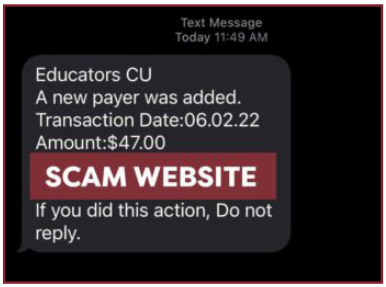
Never discuss account numbers, PINs, passwords, or other personal information with anyone who contacts you. Legitimate companies don't ask for information like your account numbers or passwords by email, phone or text.

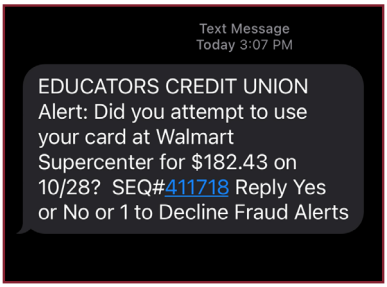
Don't call phone numbers sent in texts, emails or voicemails, as it will connect you with the scammers. **Instead, call Educators Credit Union directly at 262.886.5900 and check whether the email, text or voicemail is from us.**

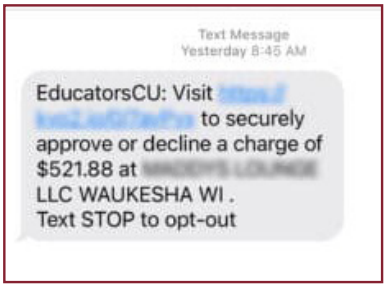
Don't trust caller ID. Just because your caller ID displays a phone number or name of a legitimate company you might recognize, it doesn't guarantee the call is really coming from that number or company. **Forward fraudulent texts to your wireless service provider at 7726 or "SPAM."**

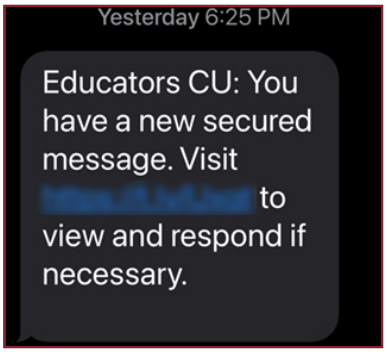
Don't click on links provided in text messages from numbers you don't recognize. Links can install malware and take you to fake websites that look real but whose purpose is to steal your information.

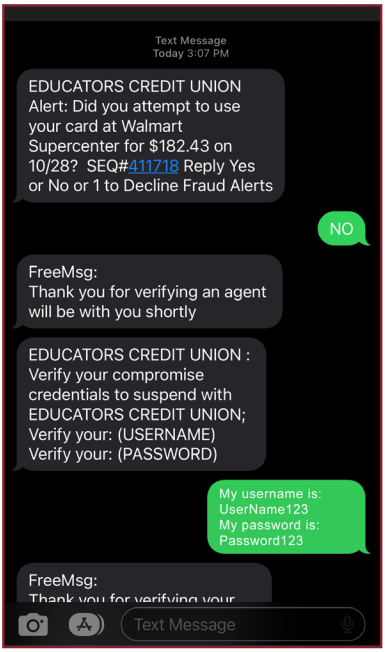
Examples of fake text messages:











SAFETY TIP

Report any suspected fraud to Educators Credit Union immediately.

Dating & Romance scam

One day, Isabella received a Facebook friend request from 'Ivan Miller.'

She decided to accept the request. He messaged her and said he was looking for friends to keep him company while he was on military duty overseas. A few weeks after befriending her, a romance started.

"He kept saying he couldn't wait for us to get married," Isabella said. "We became very close, and he emailed me every day because it was easier for him than using Facebook."

Ivan told her that he had some trouble with his credit card and couldn't get funds to pay for a plane ticket to visit her. Isabella sent him $5,000 in gift cards to cover the plane ticket and some extra expenses until his credit card situation was figured out.

Then, he said his mother was sick and needed money for surgery and as soon as he paid the surgery fee, he would be on his way to Isabella. She wired him another $20,000. It was a lot of money to send, but she figured he was a good and honest serviceman and if things worked out, they would spend the rest of their lives together.

Here's how to identify this scam:

Notice how the scammer:

- Professed he would **marry** Isabella quickly.
- Claimed he was **overseas** for work.
- Always had reasons why he needed to borrow money **urgently.**
- Requested Isabella buy him **gift cards.**
- Always made **excuses** to not visit Isabella.

Here's how to protect yourself from this scam:

Refuse to buy gift cards or send money to people you've never met in person.

Be careful how much personal information you share on social network sites. Scammers can use your information and pictures to create a fake identity or to target you with a scam.

Be wary of people you meet online. Sometimes these scams can last for extended periods of time.

Talk to friends or family about the people you meet on social media and notice if any concerns come up.

Report any suspected fraud to Educators Credit Union immediately.

Work-From-Home Job scam

As Layla scrolled through her social media timeline, she saw an ad for a remote medical billing job.

The posting boasted of flexible hours and an opportunity to make $2,800 each month without any prior experience.

She contacted the company, Star Medical, and scheduled an interview for the same day.

“During the interview, there were normal questions about job history, but then there were questions about my Social Security number and where I have my checking account,” Layla said.

Layla got the “job,” and Star Medical mailed her a $3,500 check to buy equipment from a company they recommended. After she bought equipment from the website, there was $1,000 leftover. The company told her to send the rest of the money back via wire transfer.

Shortly after Layla sent the money back, her credit union told her the original check was fraudulent, and she actually spent $3,500 of her own money.

Here's how to identify this scam:

- **The recruiter asked Layla for personal and financial information during the interview.** This information can be used to steal her identity.
- **The job advertised high pay with no qualifications.**
- **The company sent Layla a check to purchase office equipment from someone they recommended and then wire the remaining funds back.** This technique is often called an "overpayment scam." The fake check may look real and appears to clear at first, but soon it bounces, typically after the victim has sent money to the scammer.

SAFETY TIP

Report any suspected fraud to Educators Credit Union immediately.

Here's how to protect yourself from this scam:

Never provide financial or personal information to recruiters or employers without ensuring they are legitimate.

Do a background check of the prospective employer with the Better Business Bureau, Federal Trade Commission, and Internet Crime Complaint Center at **www.ic3.gov**.

If you have concerns that a check may be fraudulent, **take the check and the accompanying letter to the nearest Educators branch.**

Never agree to a wire transfer of any sort.

Do not trust a recruiter who asks for money from you upfront in return for finding you a job or providing job leads.

Tech support scam

Julien was browsing on the internet one day and noticed a pop-up window.

The pop-up window notified him of a security threat on his computer and urged him to call the number on the screen immediately.

“The person on the phone told me they worked for a computer security company and they needed remote access to my computer,” Julien said. “They told me I had to install a remote access software, so that they could take over my computer and fix the issue.”

Once Julien downloaded the software, they took control of his computer and told him he had to pay $100 to get access back. Julien paid the fee, but they still had access to his personal files containing financial accounts, passwords and personal data (health records, Social Security numbers, etc.).

Here's how to identify this scam:

Once the phony tech support representative made verbal contact with Julien, they convinced him to download a remote access software so they could take over his device. Once they took over his computer, they would not release control until Julien paid the ransom.

Here's how to protect yourself from this scam:

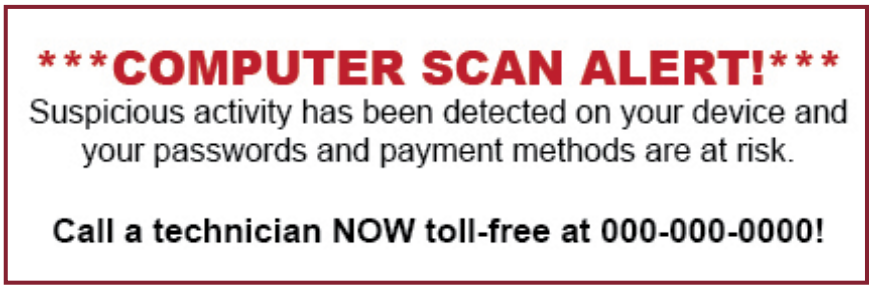
Never download remote access software. Instead, if you think there may be a problem with your computer, phone or tablet, consult with someone you trust or **take the device to a business that offers in person technical support.**

Do not call phone numbers on pop-ups. These phone numbers can connect you to fake security companies and even people pretending to be from the fraud department at Educators Credit Union.

Examine pop-ups and emails closely for signs that might indicate fraud, such as spelling and grammar mistakes.

Never provide your credit card or financial information to someone who calls and claims to be from tech support.

Examples of fake tech support pop-ups:



SAFETY TIP

Report any suspected fraud to Educators Credit Union immediately.

Debt Collector scam

Ari received an urgent call from someone claiming to be from the "IRS."

They said she owed a $4,000 tax debt. The caller had her name, address, and other personal information which made the call sound official.

"They were very demanding and hostile," she said. "They even threatened that the police were coming to arrest me."

The caller demanded that she either wire them $4,000 or purchase gift cards, so she purchased $3,000 in iTunes gift cards and $1,000 in Google Play gift cards. Then, she sent them pictures of the purchased gift cards.

Ari lost $4,000.

Here's how to identify this scam:

The Internal Revenue Service (IRS), government agencies, and any legitimate business will never threaten anyone with arrest or demand immediate payment of a tax debt or fine with unusual payment methods like gift cards, Bitcoin, or prepaid credit cards.

Here's how to protect yourself from this scam:

Hang up the phone immediately if someone contacts you claiming you will be arrested due to a tax debt.

Be suspicious of any contact with someone claiming to be from the IRS, even if it sounds legitimate. **When in doubt, call the IRS directly to check.**

Keep your Social Security number and bank account information private if you're contacted online or over the phone.

Beware of fake emails. The IRS will never initiate contact via an unsolicited email to request personal or financial data.

Report any suspected fraud to Educators Credit Union immediately.

Relative scam

Imagine getting a frantic phone call from your "grandchild" or "relative," who needs you to bail them out of jail in a foreign country or give them money because they were robbed.

You notice the person on the phone doesn't sound like your loved one, but they blame it on being distraught, sick or a bad connection.

You wire the money just in case they really do need help. But, when you call to check on your loved one, you realize they were at home, perfectly safe the entire time.

Here's how to protect yourself from this scam:

Never wire money to an unknown person. If you receive a call about a family member in distress, hang up and call the person directly or verify the information with family members.

Use a family code word. This family password should be unique and can be used during emergencies to verify identities.

Slow the process down. Never say yes to a money transfer based on a single call.

Ask lots of questions. Ask questions that would be hard for an impostor to answer correctly, such as the name of the person's pet, their mother's birth date, or a coworker's name.

Consider limiting the personal content you share online. Scammers can extract your voice from videos on social media. Ensure your profiles are private to restrict access to only friends and family.

SAFETY TIP

Even if it sounds like your relative, still be extremely cautious. Artificial intelligence can be used to make the caller's voice sound identical to your relative's voice.

Pet scam

Imagine you see a desirable pet listed for sale online.

You reach out to the prospective seller and express interest in purchasing the animal. After you send money to the alleged owner to pay for the pet, you are told that additional funds are needed to cover the cost of things like a ventilated shipping crate, insurance and other reasons.

Regardless of how much money is sent, the alleged seller will find new reasons to ask for additional payment. This continues until you realize you've been scammed at which point you could be out hundreds or thousands of dollars. The alleged sellers don't own any actual pets and are just out to scam victims of all the cash they can.

Here's how to protect yourself from this scam:

Always meet your future pet in person before paying.

Never wire money for a pet purchase.

Beware of any seller who says they're located out of town (or worse, overseas).

Don't pay for a pet you found online with money transfer apps and services.

Adopt from a local shelter.

Don't trust "free pet" offers or offers that seem too good to be true.

Report any suspected fraud to Educators Credit Union immediately.

Money Wiring scam

Be vigilant when it comes to using wire transfers as a payment method. Wire transfers allow fraudsters to receive money quickly and largely without a trace.

- If you receive a call from someone claiming to be from the government or a well-known business, such as Target, UPS or Amazon, advising that you owe them money, be extremely suspicious. Instead, hang up and call the company directly to check if the call is legitimate.
- If someone who you met on social media or online is asking you to wire them money, you may be the target of a romance scam. Refuse to wire money to people you've never met in person, regardless how "urgent" their request seems.

Always remember to verify, verify, verify.

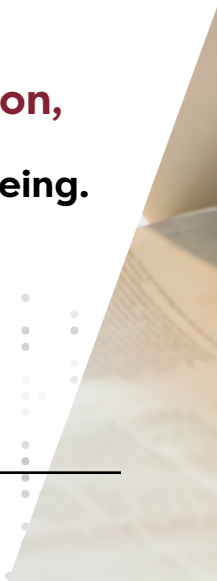
If you receive an email, **verify** it's from a trusted source.

If you receive a text message, **verify** it's from a trusted source.

If you receive a call, **verify** it's from a trusted source.

If you fear that you've been the victim of a scam, don't feel embarrassed or alone. We're here to support you and help you. Call us directly at 262.886.5900.

We're honored to be your credit union, and we will always remain steadfast in **our commitment to your financial well-being.**



Educators
CREDIT UNION®

Insured by NCUA
Equal Housing Opportunity
GDE-110

Follow us on social!
@myEducatorsCU