



Educators
CREDIT UNION®

FRAUD PREVENTION GUIDE



— Table of — **CONTENTS**

3.....We're Here For You

5.....Is it a Scam?

7.....Text Message Scam

9.....Dating and Romance Scam

11.....Work From Home Job Scam

13.....Tech Support Scam

15.....Compromised Bank Account Scam

17.....Debt Collector Scam

19.....Relative Scam

21....Pet Scam

23....Money Wiring Scam

25....Verify, Verify, Verify



**At Educators Credit Union,
we have an unwavering dedication
to the security of our members
and their money.**

As criminals introduce new and creative ways to commit fraud using emerging technology such as Artificial Intelligence (AI), 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 guide gives you valuable information to help you and your loved ones from becoming victims of fraud.

**We're here
for you.**

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.

We will also never ask you to:

- Move money.
- Take out cash and put it into an ATM or Bitcoin machine.
- Buy gift cards.

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



Is it a scam?

Here are eight 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?
- ▶ Are they insisting on staying on the phone while you go to the branch and coach you on what to say?
- ▶ 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.

Eight 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).**
- ▶ **Be cautious of images, videos and audio files sent by people you have never met in-person.** AI is making it easier than ever for scammers to fake identities online.
- ▶ **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.** Before doing anything, call Educators directly yourself at 262-886-5900 in order to dispute the transaction correctly. If you send the unknown deposit back and it is disputed, you could be responsible for the funds.
- ▶ **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 Educators Credit Union was in on the fraudulent activity, and I needed to immediately remove my money from the credit union. She said 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.”



SAFETY TIP

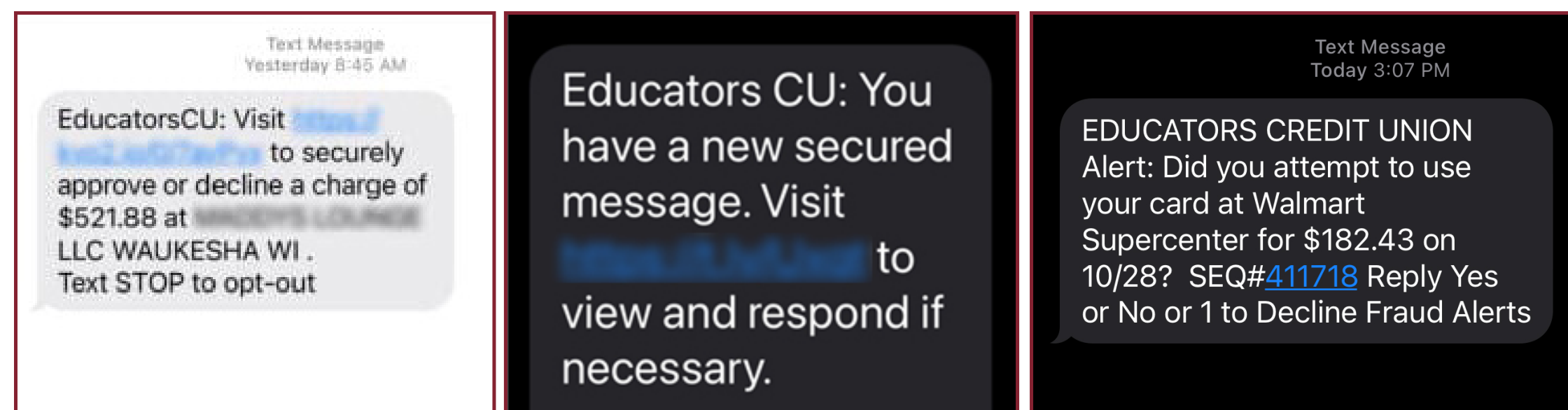
If you notice red flags, call us directly at 262.886.5900 to confirm if a text is legitimate.

Text Message Scam

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.

Examples of fake text messages:



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.



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.

Romance 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.



Always be suspicious if someone you've never met in-person asks for money.

How to protect yourself from this scam:

- Refuse to buy gift cards or send money to people you've never met in person.
- Be skeptical if you receive a message out of the blue from a celebrity trying to befriend you, even if they send videos or audio messages. AI can almost perfectly mimic anyone.
- 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.



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, claiming to be 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.



Remember: if something sounds too good to be true, it probably is.

Work-From-Home Job Scam

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.
- Some fake job listers will conduct their interviews fully over text, whether it's via email or an instant messaging app like WhatsApp. Almost all legitimate organizations conduct virtual interviews over a professional video conference platform like Zoom or Microsoft Teams.

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 detected that my computer was compromised, as well as my bank account,” Julien said. “They told me they would connect me to someone in my financial's fraud department who could help me move my money somewhere safe.”

Once Julien was connected to the next person, claiming to be from Julien's primary financial institution, they instructed him to not talk to anyone else about this situation. They then helped walk him through the steps of making a large transfer from his main savings account to a brand new one at a different financial.

"I trusted that this person really worked there and was trying to help," said Julien. He even received official-looking letters of confirmation of the transfers from "his financial" and the "Financial Trade Commission (FTC)" a day after making the transfers.

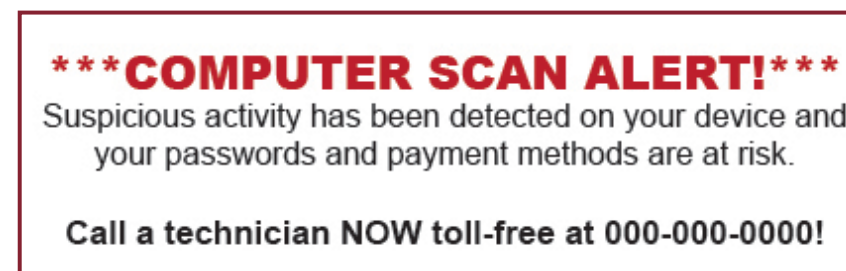
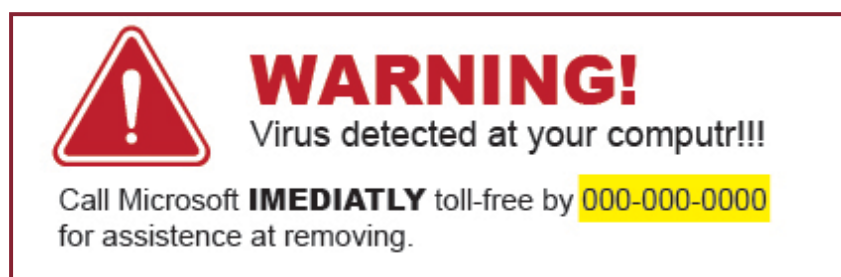
Ultimately, Julien lost a total of \$150,000 before realizing something was wrong.

Tech Support Scam

How to **identify** this scam:

- The pop-up may feature typos or low-quality logos and images. Some images may appear AI-generated.
- They tell you not to speak to anyone else, especially your financial. They may claim your financial is in on the fraud.
- They may ask you to download remote access software.
- They could ask you to create a crypto account and convert your money into crypto before transferring.

Examples of fake tech support pop-ups:



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.**



Never call a phone number provided by a pop-up on the internet.



Compromised Bank Account Scam

Peter received an urgent phone call one day claiming that his bank account was hacked.

“The scammer claimed to be from the FTC,” Peter said. “They insisted that they found evidence of money laundering in my bank account and that my credit union was working with them to resolve the situation.”

They added that the only way to protect their money was to move it to a brand new “safe” account at a different institution, and they needed to do it **now** before any other

funds were compromised. Peter was also instructed not to talk to anyone, including the credit union employees, because of the sensitive, legal nature of the ongoing investigation.

Frightened, Peter followed the instructions to move all of his account’s funds via wire transfer to a supposedly safe account. However, the account was actually the scammer’s.

Peter lost \$50,000.

Compromised Bank Account Scam

How to **identify** this scam:

- Caller will claim your money is in immediate danger.
- The scammer will instruct you not to talk to anyone including bank employees or family due to being a sensitive investigation.
- Caller instructs you to move your money to a “safe account.”
- Caller pressures you to act immediately.
- Caller requests unusual payment methods such as wire transfers, Bitcoin or gift cards.
- Caller assures you your money will be returned once the investigation is completed.

How to **protect yourself** from this scam:

- Shred sensitive documents to protect your identity and prevent scammers from learning where you bank.
- If you receive a phone call, text or email with red flags, cease communication and block them immediately.
- Call Educators Credit Union directly at **262.886.5900** to verify authenticity of a communication.
- Do not call phone numbers provided by the caller.



If you receive a phone call saying your bank account is compromised, hang up and call your financial to verify.



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.

Debt Collector Scam

How to **identify** this scam:

- The "IRS agent" threatens to send a police officer or FBI agent to arrest you.
- They ask for you to pay for the debt or fine with an abnormal currency like gift cards, cryptocurrency or pre-paid credit cards.
- They want immediate payment instead of offering to create a payment plan.
- If the caller is pretending to be from collections, you may not recognize the debt they claim you have to pay back.
- They may phish for your Social Security Number or financial information, which a real IRS agent or debt collector should already have.

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.



The IRS generally communicates via letters instead of phone calls. Unless you are expecting a phone call from them, be suspicious of anyone on the phone claiming to be from the IRS.



Relative Scam

One afternoon, Sarah received a phone call from her “son,” Jon.

She was immediately taken aback because he was already crying, and Jon wasn’t a crier. He sounded like he was severely injured.

“My heart just about jumped out of my chest, I was so worried,” Sarah said. “I wanted to help him any way I could.”

“Jon” didn’t quite sound like himself, but he claimed it was due to a car accident injury. He asked for her to send him money—immediately! He lost his wallet in the accident and needed money for a co-pay in order to receive medical treatment for his injuries.

After some frantic back and forth, “Jon” convinced Sarah to transfer \$500 for his “co-pay.” When she called Jon later to check in, she discovered the truth: her son had been safe at work all along.

Relative Scam

How to **identify** this scam:

- You may start out speaking to someone claiming to be a police officer or lawyer before being transferred to your “relative.”
- The caller is in obvious distress but may avoid telling you what happened, or not be able to tell the full story.
- They don’t sound like your relative, which they blame on a broken nose, other injury or a bad signal.
- They urgently need money. It can’t wait until morning.
- They become desperate or frantic if you offer to call someone like their parent or a friend. They will ask you to keep this a secret or come up with an excuse as to how only you can help.
- They ask for payment in an unusual currency like gift cards or cryptocurrency.

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 imposter 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 and feed it into an AI voice generator. 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. AI can be used to make the caller’s voice sound identical to your relative’s voice.



Pet Scam

Payton and his wife, Allie, agreed it was time to get a dog for their family.

Allie always wanted a Siberian husky, so Payton began searching online for responsible husky breeders. They found one with a well-maintained website that spoke of how they loved animals and treated their dogs with care and dignity.

"They sounded wonderful! They even had photos of themselves with their dogs," Allie said.

They looked at available puppies and fell in love with one that had different-colored eyes. Thinking this special puppy was going to sell fast, they immediately reached out to express interest.

It wasn't until then that they realized the breeder was located in Maine. The breeder assured them that safe transport of the puppy was possible with a small fee, but they only accepted wire transfers from businesses like Western Union.

A few weeks passed. Every few days, there would be an update about a new fee or charge they needed to process the adoption. **It wasn't long before Payton and Allie were charged a total of \$600 in adoption, transportation and other fees.**

Eventually, the phone calls ceased, and the breeder stopped answering when Payton called. Their puppy never arrived.

Pet Scam

How to **identify** this scam:

- The seller may be selling an incredibly rare animal at an impossibly low price—even free.
- They come up with excuses that you can't meet the animal in-person.
- The seller may also reside in a different state or even country.
- They may request atypical currency such as cryptocurrency, gift cards or wire transfers.
- Their website or listing may contain poor grammar.
- The photos may look digitally enhanced or made with AI.

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 peer-to-peer 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.



Never pay for a pet before meeting them in-person. If the seller begins making excuses why you can't meet in-person before exchanging money, be cautious and insist on meeting them.



Money Wiring Scam

Jordan received a phone call one evening from someone claiming to be from the FTC.

This person only identified themselves by their first name, Erin. Erin informed Jordan that they discovered fraud on their bank account and that they urgently needed to move their money to a new, safe account.

"When I mentioned wanting to call my credit union to sort this out, Erin told me that she had already worked with the credit union and there wasn't time for that," Jordan explained. "She said every moment longer we took to fix this, the more endangered my money was becoming."

Jordan was understandably frightened by the urgent language she used, and worried about his life savings. Believing that Erin was in fact who she said she was, he followed her instructions. He wired the money into what Erin claimed was going to be his new account, safe from the scammers.

Little did Jordan know, he had deposited his entire savings account right into the pocket of the real scammer, and it was unrecoverable.

He lost over \$40,000.

Money Wiring Scam

How to **identify** this scam:

- The scammer contacts you first, possibly offering a service, and asks for money upfront before providing the service.
- The service they provide may not be one typically paid for with a wire transfer.
- They will create urgency around the issue and **insist you must act now**.
- They may pretend to be your financial institution, or claim your financial institution is the cause of the issue and is not to be trusted.

How to **protect yourself** from this 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. If in doubt, hang up and call the company directly at the phone number on their official website to check if the call is legitimate.
- If someone who you met 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.



SAFETY TIP

If an organization calls you to make a payment you weren't expecting, tell them you will call back later. If they insist you stay on the line, it's probably a scam.

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 phone call, **verify** it's from a trusted source.

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

**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.****



© 2026 Educators Credit Union. All Rights Reserved. Any other trademarks mentioned within are property of their respective owners. (07/2026)

Insured by NCUA | Membership eligibility required. | Equal Housing Opportunity

