FOR YOUR PROTECTION

The financial community is seeing an aggressive increase in fraud. Be cautious of social engineering, phishing attacks and attempts to steal your identity or account information. AppleTree Credit Union is committed to educating our members on how to protect their accounts and to detect and prevent financial fraud.

Keep reading to learn more about red flags and actions to keep yourself, your money, and your identity safe.

Keeping Your ATCU Account Information Confidential

- NEVER share your logon ID or password.
- NEVER share your debit card or PIN.
- If in doubt, contact AppleTree Credit Union directly by calling 414.546.7800 or by using only the provided contact information on AppleTree.org.
- The primary account holder is the only person on the account that AppleTree authorizes to access the account online. If you give your logon information to anyone, including a joint account holder, you are giving that individual permission and the ability to view the balances and histories of all accounts to which you are affiliated.
- If you discover that someone is misusing your personal information, visit IdentityTheft.gov to report and recover from identity theft and call us at 414-546-7800 with any questions.

Common Scams:

Imposter Scams:

- These involve scammers posing as businesses or people you may know (banks, phone providers, friends and relatives).
- Scammers often spoof caller ID and real phone numbers to look more convincing.

Online Sales Scams:

- Promotions that sound too good to be true because they usually are.
- Scammers set up temporary fake online stores that disappear after you make your purchase.
- Know that scammers can make ads look like they're from a real company by using the same name and logo, even though they're not actually legit.
  Learn more about business impersonators at ftc.gov/impersonators. If you suspect a scam seller, tell the FTC at ReportFraud.ftc.gov.

Real Estate and Rental Scams:

- Scammers create fake listings for properties and vacation rentals.
- They may send an email that appears to be from your real estate agent or attorney telling you to wire them money.

Investment Scams:

- Unsolicited requests from "investment managers" that present a get rich opportunity that seems too good to be true. Once again, it is too good to be true.

Romance Scams:

- A scammer creates a fake identity, contacts a person through a dating app, and tries to quickly establish a relationship before telling an emotional story that ends with a financial request.

Technology Scams/Phishing:

- Phishing is considered the practice of fraudsters sending emails or texts from seemingly reputable sources (e.g., Microsoft, Best Buy, US Post Office, I.R.S.) to scam recipients into providing sensitive information, buying gift cards, or sending money. By clicking on links or images within the communication, scammers can possibly access your device.
- Spoofing is when a caller deliberately falsifies the information transmitted to your caller ID display to disguise their identity. In this case, you may see AppleTree's phone number on your caller ID but it is actually a scammer, claiming to be your credit union. If you answer, they use scam scripts to try to steal your money or valuable personal information, which can be used in fraudulent activity. If you receive a call from someone who says they represent AppleTree, please use caution.
- You could receive unsolicited requests to remotely access your electronic device.
- Scammers will pose as agents of trusted companies and claim they are trying to help you. They may tell you they are transferring you to your financial institution, while transferring you to an associate scammer.
- Technology scams may use emails, pop-ups, texts or phone calls.

Actions To Take to Protect Yourself:

- Always be skeptical of communication from someone you do not know.
- Never respond to unsolicited calls, texts, or emails, requesting one-time passcode authorizations.
- When in doubt, call back using a verified phone number.
- Never click on links or images from unsolicited emails or texts.
- Be cautious with emails that appear to come from someone you know. Check the email address carefully and compare it with the known address.
- Be on alert if you are pressured to act or respond immediately. Slow down and ask probing questions. Many fraudsters will attempt to relay a heightened sense of urgency. Remember, this is likely a ploy to push potential victims to act before thinking. Please do not fall for it!
- Exercise caution if asked to send money through cryptocurrency, wire, or money transfer. These are untraceable methods that make it difficult or impossible to return your money.
- Beware of rental or vacation properties where the rent is far below market value or where you are asked to make a payment before signing a lease or booking the rental.
- Let unknown callers go to voicemail and verify a callback number.
- If you see an ad for a company you know but you're not sure the ad is real, visit the company's website using a link you know is official — not the link in the ad.
- Pay by credit card. If you're charged for an order you never got, or for a product that's not as advertised, contact your credit card company and dispute the charge.

Identity Theft:

IMPORTANT: AppleTree Credit Union will never contact you and ask you to provide confidential information such as name, account numbers, social security numbers, or pin numbers.

Identity theft is when someone uses your personal or financial information without your permission. They might steal your name, address, or account numbers to open new accounts, steal your tax refund, or pretend to be you. There are several ways that scammers can steal your identity, including in person, online, through social media, and by phone.

Protecting your personal information helps you stay ahead of scammers, so we have put together some tips to keep you and your information safe. Scammers may:

- Steal your wallet or purse to get ID, credit, or bank cards.
- Go through your trash to retrieve bank statements or tax documents.
- Install skimmers at ATM machines, cash registers, and fuel pumps to digitally steal information from your bank card.
- Get personal information from your phone when you use public Wi-Fi.
- Use “phishing” to get information from you through fraudulent email, texts, or phone calls.
- Look through your social media accounts to find identifying information in posts or photos. Or they may ask you for personal information in online quizzes and surveys.

Here are some ways to protect your identity:

Sign up for AppleTree’s Credit Sense

- Credit Sense is a comprehensive credit score program that helps you stay on top of your credit.
- You will have instant access to your credit score and report, free credit monitoring, and financial education tips on improving or maintaining your score.
- You will be notified anytime your credit bureau is requested.

Pay Attention to Your Accounts

- Track what bills you owe and when they're due.
- Check your account statement, and sign up for e-statements if possible.
- Set up e-alerts for your ATCU online banking account.

Protect documents with personal information

- Shred documents that contain your personal information.
- Know what documents you should keep and what you should shred.
- Block out account numbers with a permanent marker.
- Invest in a fireproof lockbox for long-term documents.

Ask questions

- Why do they need your social security number?
- How will they keep your information safe?
- Can they use a different identifier?

Protect your online information

- Use strong passwords.
- Add multi-factor authentication for all accounts that offer it.
- Do not give your information out to a person that calls, emails, or texts you.

.