ePAPER

APCI FEDERAL CREDIT UNION

Fraud Awareness

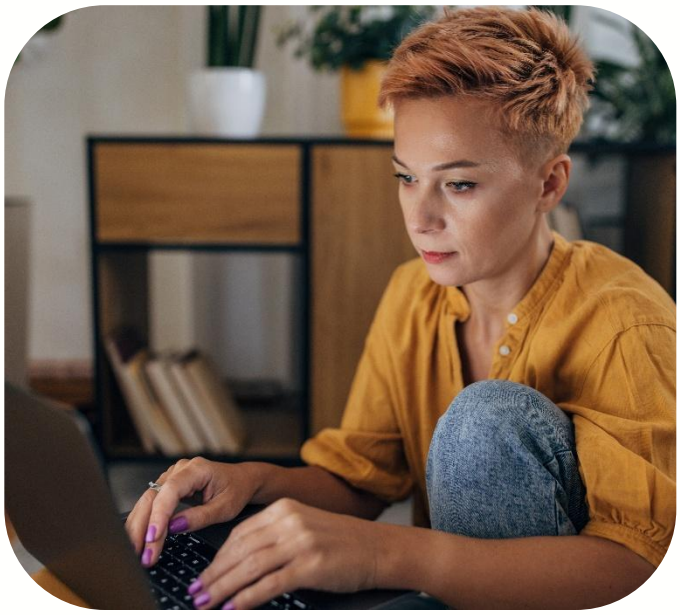
Stay Informed

The Impact of Fraud

Fraud can happen to anyone, regardless of experience, age, or income. Each year scams become more sophisticated, making it increasingly difficult to protect yourself and your finances.

According to the Federal Trade Commission (FTC), consumers reported losing more than $12.5 billion to fraud in 2024. This represents a 25% increase from the prior year. The increase was not driven by a higher number of fraud reports, but rather a greater percentage of people reporting financial losses from scams.

Staying informed about current and emerging scams is one of the best defenses. By understanding the ways to protect yourself, you can safeguard both your personal information and money, while gaining a peace of mind.



Scams to Look Out For

Get out of Debt

If you have debt and are looking for ways to manage it, be aware that you could be targeted by scammers. They promise to help manage your debt after you pay a fee. Never pay anyone before your debt is settled. To ensure you are not being scammed, research companies before agreeing to any services.

Amazon Refund

Ever get a text that there is an issue with an item you purchased from Amazon? Scammers will send texts stating that there is an issue with your order and will offer you a refund via link. This is a phishing scam to steal your personal information. If you have a recent purchase, check on Amazon's website to see if there are any issues.

Overdue Traffic Ticket

Scammers are pretending to be the Department of Motor Vehicles and are sending texts that state that you have an overdue traffic ticket. Similarly, scammers will pretend to be toll collectors and send texts stating that you have an unpaid toll charge. The links in the text messages will steal your personal information. Report and delete any unexpected or unwanted text messages.

FEMA Disaster

FEMA impersonators will show up, call, or text people after a natural disaster. They will offer services for a fee. FEMA does not charge people for disaster assistance. If you are being contacted by a FEMA representative and have never applied for FEMA disaster assistance, it is likely a scam.

New Boss Imposter

Your new "boss" will get in touch with you and request that you urgently purchase gift cards and share the card and PIN numbers. Do not buy gift cards if it is asked unexpectedly. You can also try to contact the colleague to verify the request.

Job Recruitment

If you get a job interview, research the company or recruiter to see if they are from a real organization. Scammers may email you fake enrollment paperwork before your interview that asks for your personal or financial information.

Cloud Storage

Scammers will send a text claiming that you are out of storage and provide a link to get more. Do not click on any links. Instead, check your account via the website of the company they are claiming to be from.

Law Enforcement Impersonation

A call comes through that claims they are from the police department. They may say you are going to be arrested if you do not immediately pay a fine. Hang up and call the department they claimed to be calling from.

Prize Winner

You receive a call or text that you have won a huge prize, but to get it you need to pay for taxes or fees. They may say it is a limited time offer so you must act fast. This is a tactic to try to get you to make a quick decision without thinking.

Work From Home Jobs

Scammers will send emails or texts about job opportunities. They will claim that you can work from home and make thousands of dollars a month. Instead of clicking on any links, look up the name of the company or the contact's name with words like "scam," "review," or "complaint."

Real ID

Messages are being sent by "DMV officials" saying you can skip the line at the DMV if you pay a fee or provide personal information. This is a phishing scam to steal your money or information.

Travel Website

You may see advertising for free or cheap travel deals. Be aware that these advertisements can be set up by scammers. Before clicking on the website, do research on the company marketing the deal.

Animal Welfare

Scammers will call or text and claim they are from the SPCA or animal shelter. They may try to say that your pet has been injured, and they need immediate payment so they can help your animal. If you have a pet, stop and check if they are at home. If you are not at home, you should hang up and call the shelter yourself.

APCI FCU Account Protection Tools

Digital Wallet

APCI FCU offers **Digital Wallet** compatibility. Digital Wallets are safer and more secure than carrying your physical wallet. Our **Visa® Debit Card** and **Mastercard® Plus Card** are accessible in the following Digital Wallets: Apple Pay, Google Pay, Samsung Pay, and Garmin Pay.

APCI eAlerts

APCI eAlerts are electronic notifications you can choose to receive when certain events you specify occur on your account. You can customize which alerts you wish to receive and how to receive them. To enroll, just log in to APCI eBanking, and set up your alerts.

Card Controls

Card control options are available within **APCI eBanking**, that allow you to block specific types of transactions from taking place.

Register for Advanced Card Controls and you can choose to:

- Block International In-store transactions
- Allow only certain types of transactions
- Set dollar amount limits by transaction or by month

If you are missing one of your cards or think it may have been compromised, and you are not ready to report it and request a new one, you can temporarily lock or unlock it with our Advanced Card Controls. This will prevent new account activity from happening while allowing previously scheduled or recurring payments to take place.

Our Methods

APCI FCU employs many methods to keep your account information safe including:

- Truncated account numbers
- Multifactor Authentication (MFA)
- Identity Verification Questions when you call us

In addition to the security factors that are obvious to members, we also practice diligent procedures when it comes to our systems that you may not be aware of. This includes regular security updates and patches, strong firewalls, and stringent policies & procedures governing the access of confidential data.