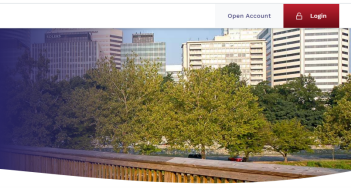
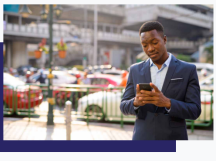
Protect your money and yourself against fraud.

FRAUD PREVENTION



At Arlington Community Federal Credit Union, your safety and well-being come first. We monitor for fraudulent and suspicious activity on all accounts, but we want to ensure you understand fraud prevention so you can protect yourself. That's why we recommend you never provide any personal, private information via phone or email and we keep you updated on current fraud schemes.



How ACFCU Fights Fraud

- We will NEVER solicit personal information from you for non verification purposes, including your full social security number or PIN.
- ACFCU has an enhanced fraud prevention system with automated call, text, and email options for you to receive notifications and check on suspicious activity and transactions.
- You can immediately text the provided command word, interact with the automated phone system, or speak with a live agent.
- We ask you to keep your contact information up-to-date so we can easily reach and alert you.
- If at any time you're suspicious of a communication from ACFCU, call **703-526-0200** to verify the validity—we're with you and your well-being is our number one priority.

Ensure Your Account Is Protected

Verify your account information today.

Protect your account by making sure your contact info, especially your cell phone number, is up to date. Having current contact info allows us to notify you in case of potential fraud situations.

Follow these easy steps to update and verify your personal information in the mobile app or online banking today.

LEARN MORE

What to Watch For

Unusual Account Activity

- We encourage all our members to regularly check their account transactions for activity they don't recognize, including fraudulent deposits.
- These deposits are often returned as counterfeit after the fraudster has already withdrawn them, leaving you responsible for that amount.
- If you find a suspicious transaction, immediately notify ACFCU for potential fraud to protect yourself.

Skimming

Skimming captures magnetic info from a credit or debit card and uses it for fraudulent purposes. To help prevent your card from being skimmed:

- Don't use an ATM or credit card machine that looks tampered with.
- Protect your PIN with your hand when you enter it into an ATM or credit machine.

Phishing

Phishing scams include "spoofed" emails and fraudulent websites that appear as though they're being sent by a person or organization you already know and ask you to provide or "verify" your personal, private information (passwords, credit card numbers, account numbers, etc.). To avoid phishing:

- Be cautious when using the Internet and responding to telephone solicitations.
- Be suspicious of any email that is marked urgent request and asks for personal information.
- Do not click on the links in an email you're unsure is authentic.
- Look for **"https://"** to appear in front of a web address when giving your debit or credit card info.
- Review your statements regularly.
- Be suspicious of emails that claim to be from your financial institution and request information from you.
- Install a firewall and anti-spyware on your computer.
- Update your browser with security patches regularly.

SMIShing

SMIShing, a combination of "SMS", the technical term for texting, and "phishing," uses text messages to prompt individuals to provide the "SMISher" with their personal, private information. To avoid SMIShing:

- NEVER respond to text messages requesting personal, private information. If suspicious activity has been detected on your account, we will call or text and you can follow the instructions to answer questions regarding your recent card activity.

Identity Theft

Identity theft, the fastest-growing crime in the country, occurs when someone steals someone else's personal, private information and then pretends to be that person. Minimize your risk of identity theft:

- NEVER give out personal information over the phone/internet unless you initiated the transaction.
- Do NOT carry your social security card in your wallet.
- Make copies (front and back) of all cards and pieces of information you carry with you in case your wallet is stolen and keep them in a secure location.
- Destroy all unused preapproved credit card offers immediately.
- Remove mail promptly from your mailbox each day and ask the post office to hold your mail until you return if you plan to be out of town for an extended period of time.
- Check your FREE credit report annually to ensure all information is accurate.

Other Common Scams

Cashier's Check Scam

This scam involves the distribution of cashier's checks that appear to come from ACFCU, but are actually fraudulent. If you receive an unexpected ACFCU cashier's check, immediately contact us before depositing it to determine whether it is legitimate or not.

Grandparent Scam

This long-running scam targets older victims by pretending to be their grandson or granddaughter and requesting they wire money to them for an emergency, without providing too many details. They may say things like "please don't tell Mom or Dad" or "My nose is broken, so I may sound strange."

Jury Duty Scam

Scammers pose as judicial officials or police and call people from a spoofed law enforcement phone numbers or name to let them know they failed to report for jury duty and owe a fine.

Medicare Scam

In 2019, the federal government replaced Medicare cards that featured enrollee's social security numbers with an 11-digit identification number instead to help protect seniors from identity theft. Now, scammers attempt to trick people into giving them their new 11-digit identification number so they can take over their identity.

Sweetheart Scam

This typically involves a dating site account with fake information and photos for a profile that is too good to be true. Once a target has been established, the scam usually escalates to the thief's unveiling of a money problem and may include the request for funds so he or she can travel to meet you in person or to help a sick relative.

IRS Scam

These scammers claim the victims owe money to the IRS and must pay promptly or be arrested, deported or have their driver's license suspended. Sometimes, the caller becomes aggressive, warning people that a sheriff or local law enforcement will show up at their door if they don't pay immediately. **The IRS will never call to demand immediate payment over the phone, threaten to bring in local police, ask for credit or debit card numbers over the phone, or require you to use a specific payment method for your taxes.**

Tech Support Scam

This scam can occur through a phishing email, a phone call, a pop-up ad or a locked screen on your device with a phone number to call to fix it. Legitimate customer, security, or tech support companies will not initiate unsolicited contact with individuals.

Protect yourself from fraud: Contact ACFCU directly if you have any questions or concerns via Secure Messaging in mobile or online banking, an email to **acfcu@arlingtoncu.org** (email is not secure, so don't include any private info) or by calling **703.526.0200 x4**.

The Fine Print
While we do monitor fraudulent or suspicious activity and may proactively contact you about this activity, we will never call and ask for confidential information such as your entire account number or PIN. Contact us: 703.526.0200 x4 if you have provided confidential information. Message and data rates may apply.