Understanding
The Security Behind
Digital Banking

Arizona Federal
Experience the power of Us.
Over the past 20 years, the internet has transformed the way we interact with the world. Everything from video chatting and making phone calls to discovering new information, booking vacations and managing accounts can be done nearly anywhere at any time.

With all of this new technology comes new threats – and those threats can be scary! It seems we’re constantly hearing of data breaches, hacking attempts and phishing scams. Is it better to protect yourself by doing everything in person and limiting how much you’re online?

In all honesty, removing yourself from convenient online systems that make it easier to manage your money won’t make your information more secure and doesn’t limit the amount of information online. Today, it’s nearly impossible NOT to leave a digital footprint. The key to protecting yourself is understanding what is secure and safe and limiting your risks.

To help you, we’ve included some information on how we handle online security with our digital tech options for managing your accounts. We hope you’ll find this information helpful when making the decision to switch to our convenient online options.

**Username and Password**

The username and password is the most basic form of security. The user chooses a unique nickname to be known by in the system. When combined with a unique code, also chosen by the user, the user is given access to confidential information – such as account balances and loan information.

**To make this even more secure:**

- Don’t share your username and/or password with anyone.

- Use a password that includes at least one capital letter, lowercase letter, number and special character.

- Include as many characters as possible. The more you have, the more secure your password is (maximum is 24 characters).

- Avoid common passwords like names, birthdates and the ever-so-popular “password123.”

*Available on:* Online banking, mobile app and CardPower™.
Device Recognition and Two-Step Authentication

When you log in to CU Online or the mobile app, there’s an option for the system to remember this device. Every device (smartphone, tablet or computer) has a unique ID. By selecting this option, you’re telling our system to remember the device’s unique ID the next time you log in. If you don’t select this option (or if you log in from another device), our system will require you to verify yourself with more than your username and password before you can log on.

This additional verification is often referred to as two-step authentication because it requires you to:

- Enter your username and password (step 1)
- Submit a code sent to you by us (step 2).

How do you get this extra code?

The code is sent to you by phone call, text message or email address using the phone number or email address we already have on file for you – you can’t change this when you’re trying to log in. The 6-digit number *changes every time*, enhancing the security of your username and password.

Two-step authentication protects your accounts because a hacker would not only have to know your username and password, he would also need to have access to your phone or email account to receive the one-time passcode.

*Available on:* Online banking and mobile app.

EyePrint ID

There is so much that is unique about each individual person. EyePrint ID uses this individuality to create a log-in code by scanning your eyes and recognizing your blood vessel pattern, which is very difficult to replicate.

On top of that, your “eyeprint” is encrypted and never leaves your phone. That means it can only be accessed through our app on the device you set it up with. While you can share your password with someone (or write it down and lose it), you can’t share your eyeprint; and you definitely won’t forget it!

*Available on:* Mobile app.

Fingerprint Log-in

Similar to the way EyePrint ID works, fingerprint log-in capabilities read your fingerprint (thumb, forefinger, etc) through a sensor on your phone. The app will only allow you to log in if your fingerprint matches the fingerprint pattern you set up on your mobile device. Your fingerprint is not stored on a server but remains on the device.

So, if you set up your thumb as your fingerprint for log in purposes and try to log in using your index finger, the app will not log you in!

*Available on:* Mobile app.
Tokenization:
With an increasing number of data breaches and card compromises occurring, financial institutions have been searching for a more secure way for consumers to pay for things. Tokenization takes a huge step forward in securing your payment information.

**Whenever you use tokenization:**
- The merchant is not provided your account number or debit/credit card number
- They are given a code (called a token) that is only valid for that specific purchase

Because this code is only specific to the purchase, if someone steals information from a merchant’s system, your card and account information is still safe!

*Available on:* Arizona Federal credit or debit cards used through Android Pay, Apple Pay or Samsung Pay. Also available through chip cards when you insert the card to pay, instead of swiping the card to pay.

### Purchases without a token:
- Consumer makes purchase
- Card number is transmitted
- Terminal
- Merchant records (where data breaches occur)

### Purchases with a token:
- Consumer makes purchase
- A token transmits and **not** a card number
- Terminal
- Merchant records (where data breaches occur)
Secure Website

The Arizona Federal website (ArizonaFederal.org) where you log in to online banking contains a security certificate (called SSL), which prevents hackers or fraudsters from stealing your information on our website. The certificate encrypts all of the information using one of the most sophisticated encryptions available today. Here’s how it works:

- When you visit our website, the certificate creates a secure connection between your computer and our website servers.
- The website will start with “https” instead of “http,” indicating a secure connection.
- Information is now scrambled when it is transferred between your computer and our servers, making it virtually impossible to steal.

Available on: Online banking and mobile website.

Other ways we protect your money

In addition to the security features listed above, here are some other ways your money is being protected at Arizona Federal.

- Visa® Zero Liability policy protects you from being stuck paying for fraudulent transactions on your credit or debit card, so you can shop worry-free. If you notice an unauthorized transaction on your account, notify us immediately.
• **Transaction monitoring** is another way we protect against unauthorized activity on your account. If a purchase is made on your account that is out of the ordinary, you may receive an automated call from us asking you to verify if the transaction was made by you or not.

• **CardPower™** is another way to keep your money safe by setting controls for your Arizona Federal debit and credit cards. Once you’ve downloaded the app to your phone, you can:
  
  • Block card transactions by geography (e.g., international transactions)
  
  • Limit specific merchant categories (gas, grocery, etc.) or transaction types (online, ATM, etc.)
  
  • Block high-dollar transaction amounts
  
  • Set alerts so you'll be notified whenever your card is used
  
  • Turn your card completely off, and or back on again only when you want to use it
  
• **IDProtect™**, a no-cost benefit included with your membership, monitors your credit and notifies you anytime there is a change to your credit report. Fraud specialists are available to help you correct mistakes or shut down any fraudulent credit accounts. If you haven’t enrolled already, your financial coach can help get you set up.