Canyon State
Credit Union™
Committed to You.

Online Security Policy

Canyon State Credit Union's goal is to provide you with relevant financial products and services to meet your needs. We are committed to protecting your information and website activity in all situations. This policy provides an overview of what we do, in conjunction with our technology partners, to maintain a secure level of service to all of our members.

Online Banking Security

We strive to provide the utmost security and protection to you on our site, especially when you access Online Banking. Some of the ways we keep you safe include:

> *Username and Password Requirements*

For the greatest security, our Online Banking system requires strong username and password characteristics, as explained during your initial system login. We strongly encourage the following additional guidelines for creating safe login credentials:

- Do not use any part of your member number or Social Security Number in your username or password.
- Make sure your password is hard to guess but familiar to you.
- Do not write down your username or password.
- Change your password periodically for added security.

Your password is encrypted in our technology partner's database, so it is not accessible by Canyon State Credit Union employees or our technology partner's employees. This protection ensures that only you will have knowledge of all authentication information.

> *Incorrect Credential Actions*

Our system allows you to enter your username or password incorrectly five (5) times. After the third failed attempt, the system presumes this is fraudulent activity and the account is "locked"; no further login attempts are allowed until you contact us to regain access to your online account.

Before the third failed attempt, you can utilize the "Forgotten Password" and "Forgotten Username" features to recover or reset your information and gain access to Online Banking.

> *Enhanced Multi-Factor Authentication (EMFA)*

This security feature makes it more difficult for cyber attackers to access your accounts without you knowing it. Passwords alone and challenge questions are no longer adequate forms of authentication due to the advanced technology hackers employ to steal your information.

EMFA requires a one-time passcode be sent to your preferred contact method (email, voice call or text message). After you successfully authenticate with your login credentials and the one-time passcode, you can register your computer, so that you do not have to authenticate with a one-time passcode each time you log in (if you are still prompted for a one-time passcode after registering, see Cookies).

EMFA protects you by requiring your phone (something that you have) and your Online Banking password (something that you know). By doing this, even if an attacker steals your password and tries to use it to log in on their computer, they would be unsuccessful because they would also need your phone.

> *Disabled Auto-Complete Behavior*

To further reduce the risk of fraudulent activity, our system does not permit account credentials to be pre-filled or automatically populated. Some browsers are configured to "remember" information, including passwords in many cases; our login form has been coded to disable this feature. This helps protect against unauthorized access to account information by others that may have access to your computer.

> *Automatic Sign-Off / Session Timeout*

Another security feature of Online Banking is that the system will "time out" or sign you off after a period of inactivity. The system's default session timeout period is 10 minutes. For your security, the timeout setting cannot be changed. Your Online Banking session also ends when you close out of all of your browser windows.

We strongly recommend that you continue to log out of Online Banking by clicking "Log Out" in the top right of the screen, as there is still a risk of others gaining access prior to the session timeout.

Cookies

Cookies are small text files placed on your computer and they are commonly used on websites. Cookies do not harm your computer or your browser. All private data stored in cookies by our online banking system is encrypted and for internal use only. Our system utilizes cookies to remember your devices for a safe, convenient login experience. For example, if you choose to register your computer as “private”, a browser cookie will be placed on the system so that you do not have to continue receiving the one-time passcode as explained in enhanced multi-factored authentication (EMFA).

Cookies must be enabled on your browser for proper functionality.

Note: If you have your browser set to delete cookies or you do a periodic clean-up that involves deleting cookies, you may have to authenticate that computer again with a one-time passcode.

Secure Sockets Layer (SSL) Encryption

Secure Sockets Layer (SSL) encryption is used to provide a secure channel for data transmissions across computer networks. This encryption works by scrambling messages that are exchanged between your internet browser and our server. Browsers that do not support SSL are unable to access Online Banking.

The Canyon State Credit Union website and online banking system utilizes one of the highest levels of encryption (256-bit).

Browser Encryption

The use of SSL encryption requires that you have a capable browser. While older browser versions may support SSL, they may not support the level of encryption you will find on our website, which means you may not be able to access parts of our website and our online banking services.

We recommend that you use the most current browsers to access our site. You can download the latest browser versions from the links below:

- Internet Explorer 9*
- Mozilla Firefox
- Safari
- Google Chrome

*Internet Explorer 7 is not supported by our website and our online banking services.

Web Forms and Email Communication

The forms that are on our website and within Online Banking utilize S/MIME (Secure/Multipurpose Internet Mail Extensions) public key encryption schemes to ensure secure messaging, confidentiality, message integrity and sender authentication.

The purpose of the web forms on our site is to eliminate the need for personal email communication. Regular email messages sent from your standard email account (ie: Yahoo, Gmail, etc.) are not secure transmissions and offer little privacy protection against malicious parties that could intercept them. If you do communicate with Canyon State Credit Union via your personal email instead of a web form, do not include any confidential information such as your account number, Social Security Number or any other personal information you would like to keep private.

Mobile Device Security

With mobile usage on the rise, we understand how important it is to make sure you are secure when accessing Online Banking on your mobile device, too. We employ the following features to keep you safe when you’re on the go:

- Enhanced multi-factor authentication (EMFA)
- Secure Sockets Layer (SSL) encryption
- No stored or cached information on device
- Strong password policies
- Idle session timeout

What We Do to Keep Your Information Secure

We have strict policies and procedures in place to safeguard how member information is stored, transmitted and secured. We do not trade, rent or sell your personal information (including email addresses) to any person or third-party company. Some of the processes we enforce to keep you safe include:

- Fraud analysis and card tracking
- Email encryption
- Data security products

- Data maintenance and backup
- Regular security audits

Remember that Canyon State Credit Union will never ask for any sensitive account information via email or text message. If you receive an email, text message or other suspicious communication that appears to be from Canyon State Credit Union but asks for account or personal information, you should always contact us to verify the integrity of the communication.

What You Can Do

Education is the key to keeping your information safe! We have a section on our website dedicated to our members' security and ways you can help protect your data. In the Security Center, you can learn about the latest scams and threats, the latest types of fraud, how to report identity theft if you become a victim, and more.

Visit our Security Center to learn more!