
CCU Banking Security

The security behind your Online & Mobile Banking usage is our #1 concern.

If a questionable logon attempt is detected, the system will require additional identity verification before allowing access. Online & Mobile members must put in their same Logon ID and Password (Security Code). We store your Security Code in our database in an encrypted form that even we cannot decode. In addition, Enhanced Authentication provides extra protection for your online data and helps guard against phishing scams and identity theft by recognizing your computer and usage patterns.

Your user ID and password will never be included or asked for in any of the text message that you receive from or send to Cornerstone Credit Union.

Other online security measures include:

- Secure Sockets Layer (SSL) protocol to ensure that your connection and any information transmitted is protected.
- 128-bit encryption to make your information unreadable as it passes over the Internet.
- Automatic time out that occurs if you are inactive in the secure area of our site for more than 10 minutes
- There is NEVER any personal data stored on your phone.

If your browser doesn't support SSL or 128-bit encryption, you will need to upgrade your browser.

While we continue to evaluate and implement the latest improvements in Internet security technology, users of the system also have responsibility for the security of their information and should always follow the recommendations listed below:

1. Site best viewed with recent versions of Internet Explorer, Firefox, and Safari.
2. Keep your Security Code confidential.
3. Be sure others are not watching you enter information on the keyboard when using the system.
4. Never leave your phone, mobile device, or computer unattended while logged on to the system. Others may approach your phone/tablet/computer and gain access to your account information if you walk away.
5. Exit the system when you are finished to properly end your session. Once a session has ended, no further transactions can be processed until you log on to the system again.
6. Close your browser when you are finished, so that others cannot view any account information displayed on your computer.
7. Keep your computer free of viruses. Use virus protection software to routinely check for a virus on your computer. Never allow a virus to remain on your computer while accessing the system.