



CAMPUS USA Credit Union

Online Security Policy

Our Commitment

We utilize 128-bit encryption to secure all online banking sessions and end-to-end SSL (Secure Socket Layer) security for mobile sessions to protect your accounts and confidential information. In addition, we employ several other security features to ensure the safety of your accounts, including (but not limited to):

- **“No-activity” sign-off after 30 minutes**- if, while you’re signed into CAMPUS Online, no activity is detected for 15 minutes, we’ll automatically sign you out.
- **Enhanced Log-in Security**- in addition to entering a user name and password to access CAMPUS Online, your device and browser will be registered through a process called Multi-Factor Authentication (MFA). Subsequent logins must be made from this device and browser, otherwise, we’ll ask you to confirm your identity through the use of a Temporary Access Code (TAC) sent through a verified contact medium.
- **The ability to change your password**-experts agree that it is a good idea to change your password on a regular basis to avoid fraud (we require changing your password annually to avoid fraud). Pick something easy to remember but harder for others to guess, and be sure not to pick a password that you’ve used on any other sites.

Your Responsibility

Your use of CAMPUS Online confirms your agreement and understanding of the provisions explained in our: CAMPUS Online: Terms & Conditions, which describes in detail all aspects of using our service. You are responsible for maintaining the confidentiality of your personal identification and access information, member numbers, online passwords and other account data.

CAMPUS USA Credit Union cannot be responsible for member errors or negligent use of the service and will not cover losses due to:

- Misuse of the service or member errors while entering information.
- Failure to maintain confidentiality of or sharing of passwords and/or access information leading to unauthorized access to accounts. This includes storing passwords (through functions such as “autocomplete”) on any PC or device that may be collected and re-transmitted (as in the case with “spyware.”)
- Failure to “Sign Off” when completing an online session, leaving a computer unattended during an online session, or storing identification or password information in a computer.
- Neglecting to report known unauthorized account access within two (2) business days.