CAMPUS USA Credit Union
Online Security Policy

Our Commitment

We utilize a minimum 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):

- **Session Timeouts** - For security purposes, your CAMPUS Online & Mobile Banking session will be timed out after 30 minutes of inactivity or 60 minutes for a fixed session.
- **Enhanced Log-in Security** - In addition to entering a unique User ID and unique password to access CAMPUS Online & Mobile Banking, you will be required to enter a secure access code (SAC) when logging in for the first time from a new device or web browser. The secure access code will be delivered to your pre-existing phone number or email address. You will have the option of registering the device. If the device is not registered, you will receive a secure access code each time you log in. A new secure access code and browser registration is also required any time cookies are cleared from a web browser.
- **Alerts** – We offer customizable alerts to notify you of online & mobile banking activity and to verify online & mobile banking activity was performed by you. We encourage all CAMPUS Online & Mobile Banking users to utilize alerts.

Your Responsibility

Your use of CAMPUS Online & Mobile Banking confirms your agreement and understanding of the provisions explained in our CAMPUS Online Services Agreement, 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 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 is the case with “spyware”).
- Failure to “Log Off” when completing an online session, leaving a computer unattended during an online session, or storing identification or password information in a computer or device.
- Neglecting to report known unauthorized account access within two (2) business days.
- Failure to utilize proper software to prevent viruses and malware from running on your devices and compromising online banking credentials.