

E*Teller Account Access Tips & Tricks

Security/Challenge Questions

- Challenge question answers must be at least 6 characters long
- Each challenge question must be answered uniquely
- A minimum of five challenge questions must be answered

Password Security

You may be asked to reset your password, even if you already have a saved password. Based on security standards, all passwords must meet the following requirements:

- Minimum Length: 8
- Maximum Length:32
- Must contain at least one upper-case letter
- Must contain at least one lower-case letter
- Must contain at least one number or one special character
- Password cannot match the Login ID
- Password cannot contain the Login ID as part of its makeup
- Password cannot contain the word password

Special Characters Allowed in Passwords

The following special characters are allowed as part of the overall content of a valid password:

- ! - The exclamation point.
- # - The pound/number sign.
- \$ - The dollar sign.
- % - The percent sign.
- _ - The underscore.
- -- - The dash.
- - Blank spaces (allowed, excluding at beginning or end of password/phrase).

Other Security Features

In addition to the login credentials, a few additional security features are in place. These security features include:

- Passwords are required to be changed periodically
- Auto complete functionality is disabled for login ID and passwords
- Bad password attempts may result in temporary E-Teller lockouts
- Periodic reviews of challenge questions and email address will be required

Online Security Resources

Whether you're using the web or checking your e-mail, we care about your security and privacy.

Protect yourself

- Use an Internet firewall.
- Whether you're using Windows or Mac, make sure your computer is up to date and is getting updates regularly.
- Use up-to-date antivirus software.
- Use a secure web browser.

Tips for secure browsing

- Always use the most current version of your browser.
- Don't select "remember password" when using a publicly accessed computer.
- Be wary of signing into Online Banking using public computers. They may have keystroke capture devices/software installed on them.
- Perform transactions (such as shopping or submitting personal information) at sites that are well established and that are familiar to you.
- Use the "Log Off" button when exiting online banking. This will exit you properly from your online banking session ensuring someone else can't come in after you and use your session.

ATTENTION MOBILE APP USERS: To update your password or login credentials, you will need to access your account directly from www.envistacu.com. Functionality is coming very soon to enable password resets from the app!

Troubleshooting

Blank Screen

After you attempt to login to your account, if you receive a blank screen, please try the following.

- Wait 15-30 seconds. With each failed login attempt a progressive delay is implemented beginning with 15 seconds. After five failed login attempts, the IP address from where you are attempting to access the account will be locked out and it will be necessary to contact the credit union for assistance.
- If you have www.envistacu.com stored as a favorite, delete it and re-add it PRIOR to attempting to login again.
- Clear browser cache
- Ensure that minimum browser requirements have been met. (see below)

- Contact Envista Member Service at (785) 228-0149 in Topeka, toll free at (877) 968-7528 or email us at member.service@envistacu.com. It may be necessary to reset your password or Login ID.

Browser Requirements

New security features require browsers to support TLS 1.1 or greater. What is TLS? It stands for “Transport Layer Security”. The primary goal of the TLS protocol is to provide privacy and data integrity between two communicating computer applications.

Minimum Browser Requirements for our Website

- Internet Explorer -- IE 11 supports TLS 1.2
- Mozilla Firefox -- Version 27 and newer supports TLS 1.2
- Google Chrome -- Version 30 and newer supports TLS 1.2
- Apple Safari -- Version 7 and newer supports TLS 1.2

Envista is committed to protecting your account information. As a reminder for safe online banking, you should have the latest virus protection and malware scanning software installed on your computer. You should also ensure that all the software you use on your computer has the latest security updates, and keep your Login ID and password private and secure.

If you require further assistance, please contact our member service staff at (785) 228-0149 in Topeka, toll free at (877) 968-7528, or email us at member.service@envistacu.com.