Internet Banking Best Practices

At Astera Credit Union, our goal is to provide you with the best all-around banking experience. We secure all of our online services to help protect you and your finances.

You can also help yourself to be as safe as possible. To help ensure the security of your online banking experience at Astera Credit Union, we recommend that you do the following:

1. Install Real-Time Antivirus and Antispyware (Security) Software

- Make sure to have updated antivirus software installed on your computer. It protects your personal information from being lost due to a virus.
- Make sure to also have updated antispyware (security) software on your computer.
- Allow for automatic scanning and updates of all antivirus and security software.
- Run anti-virus software after using any public Internet or unsecured wireless connections.
- Search for the services of a computer expert to enable you to get the top rated software and services available.

2. Install Security Updates to the Operating System and All Applications as They Become Available

- Keep your computer operating system up-to-date.
- Install security updates to your operating system as they become available.
- Install software patches, operating system updates, legitimate third party application updates and hotfixes.
- Install the latest updates and/or patches for your web browser (Internet Explorer, Firefox, Chrome, Safari, etc.).

3. Use a Desktop Firewall

- Enable the personal firewall that came with your operating system. Personal firewalls assist in preventing cyber-attacks from happening.
- Or, buy a separate personal firewall and install it on your computer.

4. Adopt Safe Email Practices

- Never follow a link in your email to a site and then proceed to enter personal information, especially account numbers or passwords.
- If you want to visit a site to make a transaction. Open a new browser window and enter the URL of the exact, trusted site.
- Do not open attachments or click on links contained in emails received from unfamiliar sources.
- Beware of questionable emails. You may receive emails asking for your personal information such as a password or PIN. Some may even contain what appear to be legitimate bank/credit union logos, and they may be structured to look very much like the official communications that you regularly receive from Astera Credit Union. You can usually detect fake emails because the links usually direct you to questionable Internet addresses. The emails may also contain poor grammar.
- Always delete account sensitive emails that contain any information regarding your account activity.

5. Secure Your Home Wireless Network

- Change the factory-default service set identifier (SSID). Wireless router manufacturers often set the SSID to a default value. Even if your router is not broadcasting your SSID, intruders may be able to find it by trying default settings. These default settings have become well known, so leaving the default setting may allow intruders to access your wireless network.
- Do not broadcast your SSID if possible. Hiding your SSID may not be a perfect method to secure your network, but it is still good practice to hide it.
- Change the default password. Since the default passwords for most brands of wireless routers are published on the Internet where anyone can find them, you should change your password.
- Enable encryption. This is the single most important step in securing your wireless communication. Wireless Protected Access - Pre-Shared Key (WPA-PSK) is the suggested encryption method for a home network.
- Use a software firewall on all computers connected to your network.
- Limit access to shared files and folders on your computers. Set passwords on file shares and provide access only to authenticated users.

6. Create and Maintain a Strong Password and/or PIN

- Don't write your PIN o r passwords down.

- Create a password using a combination of letters and numbers. You should use a password that is at least 8 characters long and combines lower case letters with upper case letters.
- Your password should be unique to you and difficult for others to guess.
- Create passwords that do not contain any obvious information (such as your zip code, year of birth, phone number, address, relative's name, pet's name or nicknames) and never use personal information such as your Social Security Number.
- Avoid using password managers and do not click on the "Remember Me" option when offered.
- When creating a password, don't use a password that you use for any other service.
- Change your passwords every 30 to 60 days. If you suspect your accounts, user names, passwords or PINs are compromised, contact Astera Credit Union immediately and change your passwords.
- Keep your password confidential and do not share it with anyone.
- It's mandatory to establish and use a password to conduct online banking transactions, but you have an option to use passwords to access other electronic devices such as mobile phones and tablets. Choose to protect those other electronic devices by using the password option.

7. Practice Safe Computing

- Avoid performing online banking transactions on a public computer. If you must use a public computer, change your password after completing your transactions.
- Consider using a dedicated computer for daily online banking activity.
- Do not have multiple browsers open while banking online.
- Never leave your online banking account open while your computer is unattended.
- Always ensure that you have signed out (logged off) of online banking and close your browser.
- Do not share or provide any of your banking information to any other party or website requesting this information.
- Ensure you have strong computer expertise to improve the safety of your personal information: Otherwise, avoid shared computers.
- Do not select the Remember Me login option offered on some sites. This is the option in your browser that remembers your username and password, thus allowing automatic log on.
- Disable file sharing software so unauthorized users cannot access your computer and its data.

- Use common sense when you connect. If you're online through an unsecured or unprotected network, be cautious about the sites you visit and the information you release.
- When banking and shopping, check to be sure the site is security enabled. Look for web addresses with "https://" or "shttp://," which means the site takes extra measures to help secure your information. "http://" is not secure.
- Clear the browser cache and history before and after an online banking session. This function is generally found in the browser's preferences menu.

8. Protect Your Personal Information

- Astera Credit Union will never ask you for personal information in an email or text message. Personal information consists of your name, Social Security number, driver's license number or identification card number, account number, credit card number, debit card number, mother's maiden name, security code, access code, password, Personal Identification Number (PIN) or any information that would permit access to your account(s).
- Examine your financial statements and/or account activity on a regular basis.
- If you need to dispose of sensitive documents, shred them.
- Information about electronic transactions is provided within your periodic statements. To protect your account, we encourage you to regularly review your statements and account activity and immediately notify us of any error or unauthorized transactions.
- If you believe your online banking PIN is lost or stolen, or that someone has used or will use your account without your permission, notify Astera Credit Union immediately at 800-323-0048.
- Keep an eye on your account and make sure to report anything that seems to be suspicious activity. You can help stay on top of things by signing up for eAlerts that will inform you when changes have been made to your account.
- If you discover that you have submitted private detail to an unknown source, notify Astera Credit Union immediately at 800-323-0048.