Mobile 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.

Mobile devices (smartphones and tablets) are computers with software that need to be kept up-to-date just like your PC or laptop. Take time to make sure all the mobile devices in your household have the latest protections. This may require synching your device with a computer.

Remember that these devices can contain tremendous amounts of personal information. Lost or stolen devices can be used to gather information about you and, potentially, others. Protect your phone like you would your computer.

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. To help ensure the security of your mobile banking experience at Astera Credit Union, we recommend that you do the following:

1. Practice Safe Mobile Device Usage

- Secure your smartphone and/or tablet with a strong passcode to power on or awake it from sleep mode. A strong password consists of at least eight characters and a mix of alpha numeric and punctuation marks or symbols. See guideline #9 for more detailed information about creating and maintaining strong passwords and PINs.
- Never store usernames and passwords on your mobile devices.
- Keep your device with you or secure the device when not in use.
- For mobile devices using the Android operating system, do not enable Android's "install from unknown sources" feature.
- Do not modify your mobile device as it may disable important security features.
- Learn how to disable the geotagging feature on your smartphone at: http://cnettv.cnet.com/disable-mobile-geotagging/9742-1_53-50101455.html

2. Practice Safe Wi-Fi Usage

- Get savvy about Wi-Fi hotspots. Limit the type of business you conduct and adjust the security settings on your device to limit who can access your phone.
- Don't use public Wi-Fi networks for credit union transactions.

- Turn off your Bluetooth connection when not in use. It will limit the vulnerability of your device to be accessed remotely.

3. Practice Safe App Usage

- Download signed applications (Apps) only from trusted sources, like Google Play and the Apple iTunes App Store.
- Review the privacy policy and understand what data (location, access to your social networks) the App can access on your device before you download.
- Never set the App, web or client-text service to automatically log you in to your credit union account. If your phone is lost or stolen, someone will have access to your money.
- Never set your banking App to auto-populate your username and password.
- Visit http://www.asteracu.com/Mobile_Banking_76.html and follow the links to download the official Astera Credit Union Mobile Banking Apps found on Google Play and the Apple iTunes App Store.
- Always sign out of the Astera Credit Union Mobile Banking App when you have completed your activity.

4. Practice Safe Mobile Computing

- Do not share or provide any of your banking information to any other party or website requesting this information.
- Never provide personal identification or banking information over your mobile device.
- Be aware of your surroundings. Don't type any sensitive information if others around you can see.
- 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 through a mobile browser, 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.
- If you must use a mobile browser, clear the browser cache and history before and after an online banking session. This function is generally found in the browser's preferences menu.

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

- Make sure to have updated antivirus software installed on your mobile device. It protects your personal information from being lost due to a virus.
- Make sure to also have updated antispyware (security) software on your mobile device.
- 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 mobile computing expert to enable you to get the top rated software and services available. Perhaps, start with the customer service representatives at your wireless provider.

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

- Keep your mobile device operating system up-to-date.
- Install security updates to your mobile operating system as they become available.
- Install software patches, mobile operating system updates, legitimate third party application updates and hotfixes.
- Install the latest updates and/or patches for your mobile web browser.

7. Adopt Safe Texting Practices

- Do not respond to text messages requesting personal information, such as Social Security numbers, credit/debit/ATM card numbers, and account numbers. Remember, your bank would never contact or text message you asking for personal or banking information. Assume any unsolicited text request is fraudulent. Giving this information places your finances and privacy at risk.
- Understand the criminal activity of SMShing. SMShing is phishing that happens via an SMS text message. A criminal sends a text message encouraging you to reply with financial or personal information, or they may ask you to click on links that will sneak viruses onto your mobile device.
- Don't respond to a text message that requests personal or financial information.
- Frequently delete text messages received from the credit union.

- Verify the phone numbers that appear in a text message before you place a call, and never give out personal or financial account information over the phone – by voice, text or email.

8. Adopt Safe Email Practices

- Utilize the official Astera Credit Union Mobile Banking App found on Google Play and the Apple iTunes App Store.
- If you must use a mobile device web browser to make a transaction. Open a new browser window and enter the URL of the exact, trusted site.
- Never follow a link in your email to a web site and then proceed to enter personal information, especially account numbers or passwords.
- 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.

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

- Don't write your PIN or 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 uneasy 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.

10. Be Wise With Regard to Your Personal Information

- Astera Credit Union will never ask you for personal information an email or text message or direct you to call a phone number in an email, other than 800-323-0048.

- 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.

11. If You Lose Your Phone or Change Your Phone Number

- If you change your phone number, notify Astera Credit Union as soon as possible.

- If you lose your phone or suspect that it has been stolen, notify Astera Credit Union immediately at 800-323-0048. Also notify your wireless carrier immediately so that your phone can be deactivated.

- Consider using a remote wipe program. This will give you the ability to send a command to your device that will delete any data.

- Keep a record of your mobile device's name, model and serial number in case it's lost or stolen.