Corner Stone BANK

CornerStone
Mobile Banking
Best Practices

Device Best Practices

- Download the CornerStone mobile banking application(s) only from trusted sources and approved App stores.
- Do not modify your device operating system. When you jailbreak or root your mobile phone, you are making it possible for an unapproved app to be downloaded and may remove needed security features.
- Password protect your device using a PIN, Password, Pattern, Fingerprint or other authentication methods available on your device.
- Enable the automatic screen-lock feature.
- Install Anti-Virus (AVS) programs on your device.
- Keep your mobile device operating system and applications up to date with the latest patches.
- Clear browsing history, cache and temporary files frequently. Files stored in the memory may contain sensitive information.
- Consider using tools that allow you to remotely locate or "wipe" your device if it is lost or stolen.

User Best Practices

- Keep your password information safe and use strong passwords. A strong password consists of 8 or more digits, with a combination of numbers and letters.
- Don't access banking or shopping applications using private credentials while connected to a public Wi-Fi connection. Many public Wi-Fi areas are not encrypted and are prime targets for hackers.
- Don't store financial information (account numbers, user id, passwords) on your mobile device.
- Be aware of your surroundings when accessing your mobile banking account.
- Never send financial information in emails or text messages.
- Never respond to "phishing" text or email requests asking for your financial information. CornerStone Bank will never request information in this manner.
- Never access your Online Banking account from a "jailbroken" or "rooted" mobile device.
- Remember to log out of mobile banking when you are finished with your session.

Lost or Stolen Devices

- **Immediately** report lost or stolen devices used for online/mobile banking to CornerStone at 540-463-2222. The bank will disable the device. You may also do this on your computer by logging into your online banking account, selecting the OPTIONS tab and Manage Device(s).
- Notify your wireless provider to suspend/deactivate your device until it is located.
- Change your online banking password.
- If available, use remote locations apps such as "Find My iPhone" or "Locate My Droid".
- Report stolen devices to your local law enforcement.

Other important information

CornerStone Cares about your financial security and providing you with helpful tips to protect it. Our mobile banking apps, text message banking and mobile web banking are provided in a secure encrypted environment. CornerStone has provided the above Mobile Banking Best Practices as a recommendation and form of user education for our customers. Please report any and all suspected bank fraud or suspicious activity to us. CornerStone Bank is not responsible for losses related to security weaknesses within your personal online banking access devices.

◆CornerStone*Cares*◆

www.cornerstonebankva.com