community state bank

Simply Mobile Security Tips

Password Protect your Mobile Device.

Many mobile devices offer a digital locking mechanism that can be enabled to require a pattern to be traced or a password to be entered before the phone will unlock for use. Adding an additional step to access your phone isn't always convenient, but it might be the extra layer of security that prevents a thief from accessing sensitive information on your mobile device.

Avoid Accessing Sensitive Information While Using Public Wi-Fi.

Many mobile devices allow connections to public wireless networks. While they are convenient, public connections are not always secure. Be sure to disable any public or unsecure Wi-Fi connections prior to accessing sensitive information on your phone.

Know What You're Downloading.

While mobile devices are less prone to malware attacks than computers, use caution when downloading apps on your mobile device. It is possible to download an app that could try to access the sensitive information on your mobile device in ways such as keylogging. Keylogging is a process in which all keystrokes entered into your mobile device are recorded – which means you could be sending your passwords and other sensitive information anywhere in the world.

"Jailbreaking" is a process in which a downloaded app "breaks open" a mobile device freeing it from the limitations imposed by its carrier, allowing additional customization or downloading capabilities. Apps that jailbreak phones are unauthorized and could damage your phone. They also make the data on your mobile device vulnerable, and are not recommended.

Research apps before downloading to ensure they have a good reputation.

Don't Follow Links.

It's always a good idea to navigate to a web site directly. You may have heard the term phishing – baiting someone into revealing private information. With a phishing scheme, that bait might be as simple as a text message or email. It may be as complex as a fake Web site designed to mimic a bank's official site, which is called spoofing.

You should never send your account information or password via text message or email. It's a common phishing scheme to send out bogus requests for such information.

You should never follow links sent to you in a text message or email from untrusted sources. These links could lead you to a spoofed site. If you enter your information into one of these sites, you've just handed that data over to thieves. Type websites into your mobile devices and bookmark those that are frequently used. This will help avoid phishing schemes and ensure the security of your sensitive information.

In the event that your mobile device has been lost or stolen, contact us immediately to un-enroll from mobile services. You may also un-enroll by accessing your mobile options within online banking. Contact your mobile provider regarding apps that can lock or wipe the data from your phone remotely.

Practicing good, safe behaviors when using mobile devices is key to ensuring the security of your sensitive information.