Your Mobile Security

How can I protect my security and privacy on Mobile Devices?
Your security and privacy is of utmost importance to CBandT. In addition to our security steps, you can also take these steps to protect your information on your mobile device.

Passwords:

- Protect your mobile device using a PIN, Password, Pattern, Fingerprint, or other authentication offered by your mobile device. Do not share or write down your passwords.
- Use strong passwords on your mobile devices – 8 or more in length with a combination of letters (upper & lower case), numbers and special characters, if allowed.
- Do not create passwords with general personal information such as address, birthday, social security number or information of a close friend of family member. Be original with your passwords.
- Do not store passwords on your device

Downloads, Software, and Applications:

- Install mobile security software (anti-malware – anti-virus) and regularly update security patches on ALL your applications.
- Regularly install operating system and firmware updates
- Avoid malware by only downloading and installing legitimate mobile apps from established sources like Apple's App Store℠ or Google Play™. Use caution when downloading copycats or clones of popular apps or games, as these apps typically come with the threat of mobile malware.
- Consider using tools that allow you to remotely wipe your mobile device if it is lost or stolen. For iPhones and iPads, enable Apple Find My iPhone™ *(https://support.apple.com/en-us/HT205362)* or if you are on an Android device, turn on Android Device Manager™ or download Find My Android Phone™ *(https://play.google.com/store/apps/details?id=com.fsp.android.phonetracker&hl=en)* from Google, to allow you to track your device in the event it's lost or stolen. When enabled, these tools may allow you to locate your device, lock the phone or wipe its memory.

General Security:

- If your mobile device is stolen or lost, contact your bank and reset your password.
- Exercise due diligence with unexpected messages or notifications. Do not click on suspicious links sent via unsolicited text message, email, or suspicious push notification.
- Do not use Public Wi-Fi hotspots (unsecured public networks) to access Online Banking or Mobile Banking. When connected to unsecured public networks, be mindful of the apps you use and the data you send over these networks.
- Do not store financial information on your device
- Never leave your mobile device unattended during sign-in to the CBandT mobile app.
- Exercise due diligence with unexpected messages or notifications. Do not click on suspicious links sent via unsolicited text message, email, or suspicious push notification.
- Disable discoverable mode after enabling Bluetooth™ devices, if your smartphone or tablet does not automatically default to off after adding a device.
- Ensure your home wireless network is configured to use Wi-Fi Protected Access II (i.e. WPA2) Wireless Security Technology.

For additional information regarding our privacy policy, visit www.cbandt.com/policies.