Mobile Security

Security Guides

This guide is intended to provide suggestions on how to make your mobile devices more secure.

ABOUT MOBILE SECURITY

The same mobility and ease of use that make mobile devices popular and convenient also make them more susceptible to security risks, including theft, hacking, phishing, etc. You should be careful when using your device, including making sure that you don't leave your device unattended, be cautious when using unsecured networks, and have both physical and data protections on the device to protect you and your device from harm.

GENERAL TIPS

- Keep your mobile device(s) with you at all times, and don't leave your device(s) unattended. Store them in a locked or secure location when not in use.
- Create a device passcode to block access to your device from unauthorized use. If your device supports it, you should turn off Simple Passcode and use a strong alpha-numeric passcode instead. See your device manual to see if that is available.
- Set auto-lock to the shortest period of time available.
- Enable remote-wipe features, if available. Also, if available, turn on features which auto-wipe data after a number of unsuccessful login attempts.
- Back up your data frequently so that you can restore it if needed. Use cloud services if available to your device to back up incrementally throughout the day.
- Do not "jailbreak" your device, as doing so bypasses many of the security measures native to the device.
- Be very careful when installing software on your device.
- Report lost or stolen devices immediately.
- Keep your phone up to date by making sure that you install phone OS updates and app updates as they become available. These often contain security patches and fixes.

WIRELESS TIPS

- Encryption should be turned on if possible to secure your data, especially when on unfamiliar networks.
- Disable Wireless and Bluetooth when not in use. Not only does this increase battery life, but also reduces the possibility of unauthorized access.
- Turn on "hidden mode" when connecting wirelessly if available on your device.
- Select to confirm before connecting to wireless networks, if available on your device.
- Be careful of information and sites accessed when on public and insecure networks.

APPLICATION TIPS

- Do not install software from unknown sources. Research software before installing to make sure it's legitimate.
- Check permissions of installed software. Restrict access to what is necessary only.
- Keep your phone up to date by making sure that you install phone OS updates and app updates as they become available. These often contain security patches and fixes.
- Remember that any information stored on your device may be accessed if your device is ever lost or stolen. Be careful about storing things such as account information and passwords on your device.