Ten Steps to Smartphone Security (Android)

Smartphones continue to grow in popularity and are now as powerful and functional as many computers. It is important to protect your smartphone just like you protect your computer as mobile cybersecurity threats are growing. Mobile security tips can help you reduce the risk of exposure to mobile security threats.

1. **Set PINs and passwords.** To prevent unauthorized access to your phone, set a password or Personal Identification Number (PIN) on your phone's home screen as a first line of defense in case your phone is lost or stolen. When possible, use a different password for each of your important log-ins (email, banking, personal sites, etc.). You should configure your phone to automatically lock after five minutes or less when your phone is idle, as well as use the SIM password capability available on most smartphones.

2. **Do not modify your smartphone's security settings.** Do not alter security settings for convenience. Tampering with your phone's factory settings, jailbreaking, or rooting your phone undermines the built-in security features offered by your wireless service and smartphone, while making it more susceptible to an attack.

3. **Backup and secure your data.** You should backup all of the data stored on your phone – such as your contacts, documents, and photos. These files can be stored on your computer, on a removal storage card, or in the cloud. This will allow you to conveniently restore the information to your phone should it be lost, stolen, or otherwise erased.

4. **Only install apps from trusted sources.** Before downloading an app, conduct research to ensure the app is legitimate. Checking the legitimacy of an app may include such thing as: checking reviews, confirming the legitimacy of the app store, and comparing the app sponsor's official website with the app store link to confirm consistency. Many apps from untrusted sources contain malware that once installed can steal information, install viruses, and cause harm to your phone's contents. There are also apps that warn you if any security risks exist on your phone.

5. **Understand app permissions before accepting them.** You should be cautious about granting applications access to personal information on your phone or otherwise letting the application have access to perform functions on your phone. Make sure to also check the privacy settings for each app before installing.

6. **Install security apps that enable remote location and wiping.** An important security feature widely available on smartphones, either by default or as an app, is the ability to remotely locate and erase all of the data stored on your phone, even if the phone's GPS is off. In the case that you misplace your phone, some applications can activate a loud alarm, even if your phone is on silent. These apps can also help you locate and recover your phone when lost. Visit CTIA for a full list of anti-theft protection apps.

7. **Accept updates and patches to your smartphone's software.** You should keep your phone's operating system software up-to-date by enabling automatic updates or accepting updates when prompted from your service provider, operating system provider, device manufacturer, or application provider. By keeping your operating system current, you reduce the risk of exposure to cyber threats.

8. **Be smart on open Wi-Fi networks.** When you access a Wi-Fi network that is open to the public, your phone can be an easy target of cybercriminals. You should limit your use of public hotspots and instead use protected Wi-Fi from a network operator you trust or mobile wireless connection to reduce your risk of exposure, especially when accessing personal or sensitive information. Always be aware when clicking web links and be particularly cautious if you are asked to enter account or log-in information.

9. **Wipe data on your old phone before you donate, resell, or recycle it.** Your smartphone contains personal data you want to keep private when you dispose your old phone. To protect your privacy, completely erase data off of your phone and reset the phone to its initial factory settings. Now having wiped your old device, you are free to donate, resell, recycle, or otherwise properly dispose of your phone.

10. **Report a stolen smartphone.** The major wireless service providers, in coordination with the FCC, have established a stolen phone database. If your phone is stolen, you should report the theft to your local law enforcement authorities and then register the stolen phone with your wireless provider. This will provide notice to all the major wireless service providers that the phone has been stolen and will allow for remote "bricking" of the phone so that it cannot be activated on any wireless network without your permission.

Information on how to implement these tips on your Android device can be found at http://support.google.com/googleplay. For more information and resources on mobile and cybersecurity, visit www.fcc.gov and the Department of Homeland Security's Stop.Think.Connect.™ Campaign at www.dhs.gov/stopthinkconnect.