16 Tips to Thwart Mobile Security Threats

Android Security

Android devices are the biggest targets for hackers and cyber criminals – exceeding 99% of all mobile malware. 60% of malware are Trojans in the "Fake Installer" category.

- Infected Apps won't typically be found in or delivered via the Google Play Store
- AVOID apps from forums or Unofficial App stores
- AVOID apps from foreign countries that have only been downloaded a few times, have only a few reviews or bad reviews – READ THE REVIEWS!
- AVOID apps (especially games) that can access or send SMS messages
- AVOID apps that need to access the directory or your location (if not necessary)
- AVOID popular apps (AngryBirds) from unofficial app stores – may be infected
- Keep your Android up to date – install manufacturer updates when you get the notice. Updates provide security enhancements and reduce vulnerabilities.
- Install and run Bluebox Security Scanner to check your phone for Master Key vulnerability (free app in Play Store)
- INSTALL Mobile AntiVirus software and consider VPN security software
- Watch out for Phishing attacks - email and websites can look very legitimate – check the URL
- AVOID text messages with links to websites – a very common way to spread mobile malware

iPhone Security

While iOS devices are not targeted as much as Android, a Trojan targeting iOS devices was detected in the 1st Quarter of 2014 (via a widely used network for rooted/hacked devices). Plus, there are some major security concerns that need to be addressed:

- Camera and microphone can be turned on remotely without your knowledge. Consider ways to cover the camera and mic.
- The name of the iPhone is typically the name of the user (Settings>General>About) and the user can be tracked by this name if Bluetooth is enabled. Someone could potentially track your child (or you) by the name of the device. TURN Bluetooth OFF when not in use.
- Access codes are not very secure. Turn off "Simple Passcode" and setup a more secure passcode that is required to use the phone.
- Advertising Settings in your iPhone can allow stores and hackers to know exactly who you are from the tracking data gathered by your iPhone. Turn ON "Limit Ad Tracking (Settings>Privacy>Advertising) and periodically "Reset Advertising Identifier" so that a new ID is generated for your device (similar to deleting cookies in a Windows PC).
- Frequent Locations – if on, provides history of ALL the places you have been including the address and how long you were there. If your child has an iPhone, TURN THESE SETTINGS OFF for EACH APP (Privacy>System Services>Frequent Locations)