MOBILE PHONE SECURITY

DIGITAL SECURITY: WHAT YOU NEED TO KNOW

WHY IS MOBILE PHONE SECURITY IMPORTANT?

For most of us, cell phones are our portals to the world: a single place where we keep our contacts and calendars, our photos, our private emails, text and voice messages, and where our browsing history gives detailed information about our interests and interactions. Your cell phone automatically reveals your physical location at any given time. You need to be conscious of the information you keep on your phone, and settings that allow your data to be accessed and shared.

BEST PRACTICES MANAGING YOUR PHONE

- Always use a lock code or PIN to lock your phone. Change them from the factory default.
- Do not install unknown and unverified programs on your phone. Only install apps from the official Apple App Store or Google Play.
- Protect your SIM card and any additional memory cards. For example, do not leave them at the repair shop when your phone is being serviced.
- If you plan to dispose of, give away, sell or re-use your phone, make sure that all information is deleted.
- Back up your phone information regularly to a computer. This will allow you to restore the data if you lose your phone or it is damaged or compromised.
- When your carrier makes an update available, install the update. This helps to protect your phone from being compromised.

BEST PRACTICES CONNECTING TO A NETWORK

- Many phones will automatically connect to open WiFi networks around them. Make sure to keep your phone's WiFi switched off until you want to connect to a specific trusted network. Same rule for Bluetooth and Infrared.
- Be very wary when connecting to WiFi access points that don't require passwords, or to WiFi networks in public spaces such as a coffee shop. It may be better to incur data charges than incur the risk of connecting to a public WiFi network.
- Instead of standard text messages, consider using channels such as WhatsApp, Signal, or iMessages on an iPhone, which encrypt messages and provide better protection.

REVIEWING APP PERMISSIONS

- Pay attention to the authorizations on various apps. Check the app's privacy policy and settings to understand how data is being shared and for ways to opt-out.
- In the Settings feature of most phones, make sure you monitor and update:
    - Which apps have access to your location information
    - Which apps have access to your contacts, calendars, photos, microphone & camera
- Your phone may also allow you to "Limit Ad Tracking" (for the iPhone, this appears in Setting > Privacy > Advertising).

HEIGHTENED SECURITY STEPS

- If you are worried that someone may tamper with your phone without your knowledge, you may want to physically mark (draw on) the SIM card, additional memory card, battery and phone with something unique and not immediately noticeable to a stranger so you can detect physical changes to your phone.
- Consider using only trusted phone dealers and repair shops if you are worried that your phone may be tampered with before you purchase it or while being repaired. You may want to use an authorized but randomly chosen phone dealer or service provider.
- Your phone may allow you to disable "Location Services" altogether if there are times you do not want your location to be tracked and made available to third-party apps. Note that your location information will still available to the mobile phone network provider as your phone pings nearby cell phone towers.

Adapted from Security in a Box's Mobile Phone Guide and Smartphone Guide by Tactical Technology Collective and Front Line Defenders