Android Field Guide: Reducing Your Digital Signature (v1.0)

Introduction: Why This Matters

Adversaries are actively targeting DON personnel by exploiting the default settings on our personal devices. They have used this data to track, target, and attack service members. Due to the fragmented nature of the Android ecosystem, many devices are running outdated and vulnerable software, creating a massive attack surface. This guide provides critical steps to harden your Android device and reduce your digital signature. Completing these checks is a matter of personal and mission security.

A Note on Android Versions: The exact path to these settings may vary slightly between manufacturers (e.g., Samsung, Google Pixel, OnePlus).

01: UPDATE YOUR OPERATING SYSTEM

Why: This is the single most important action you can take. Updates contain vital security patches that fix the vulnerabilities adversaries look for. An unpatched phone is an unlocked door.

The Action:

1. Force a System Update Check

IMPORTANT: Only perform updates on a trusted Wi-Fi network (e.g., your home).

Steps:

1. Go to **Settings**.
2. Scroll down and tap **"Software update"** (Samsung) or **"System"** (Google Pixel).
3. Tap **"Check for update"** or **"Download and install."**
4. If an update is available, install it immediately.

2. Enable Automatic Updates

Why: This ensures your device installs critical security patches as soon as they are available, usually overnight while charging, so you are always protected.

Steps:

1. From the **Software Update** screen, look for an option like **"Auto download over Wi-Fi"** or a settings icon (gear). Ensure this feature is toggled **ON**.

02: LOCK DOWN LOCATION SERVICES

Why: Your location is the most sensitive piece of data your phone generates. Limiting access prevents adversaries from building a "pattern of life" on you, both at home and deployed.

The Action:

1. Manage Per-App Permissions

Steps:

1. Go to **Settings > Location > App location permissions**.
2. Review the list of apps. If an app doesn't need your location to function (e.g., a calculator), set its permission to **"Don't allow."**
3. For apps that need location but not constantly, choose **"Allow only while in use."**

2. Disable High-Accuracy Tracking

Steps:

1. Go to **Settings > Location > Location services**.
2. Tap **"Google Location Accuracy."**
3. Toggle this setting **OFF**. This prevents Google from using Wi-Fi and Bluetooth to pinpoint your location with extreme precision, making you a harder target.

03: DELETE YOUR ADVERTISING ID

Why: This is the unique "license plate" adversaries use to track your activity across all the apps on your phone. Deleting it breaks the primary tool they use to profile you. This is the technical fix for the vulnerability that led to the 2019 attack in Iraq.

The Action:

1. Delete Your Ad ID

Steps:

1. Go to **Settings > Security & privacy > Privacy**.
2. Scroll down and tap on **Ads**.
3. Tap **"Delete advertising ID."**
4. Confirm by tapping **"Delete advertising ID"** again. This action is not reversible, but it is the most secure option.

04: REVIEW APP PERMISSIONS

Why: Many apps request access to your microphone, camera, contacts, and files when they don't need it. Each unnecessary permission is a potential vector for data exfiltration or surveillance.

The Action:

1. Audit the Permission Manager

Steps:

1. Go to **Settings > Security & privacy > Privacy > Permission manager**.
2. Tap on sensitive permissions like **"Camera," "Microphone,"** and **"Contacts."**
3. Review the list of apps that have access. If you don't trust an app or it doesn't need the permission, tap the app name and select **"Don't allow."**

Android Security Checklist

Use this list to conduct a quick "security check-up" on your device at any time.

☐ **OS is Updated:** My device is running the latest available software.

☐ **Location is Controlled:** High-accuracy is OFF and apps have minimal location access.

☐ **Advertising ID is Deleted:** My Ad-ID has been deleted.

☐ **Permissions are Minimized:** Camera/Mic/Contacts access has been reviewed and limited.