iPhone 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. While Apple's ecosystem is more controlled, a significant number of devices are still running outdated and vulnerable software. This guide provides critical steps to harden your iPhone and reduce your digital signature. Completing these checks is a matter of personal and mission security.

01: UPDATE YOUR OPERATING SYSTEM

Why: This is the single most important action you can take. Apple releases vital security patches with every update. If you are not on the latest version of iOS, you are exposed to known, unpatched vulnerabilities that adversaries can exploit.

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 > General**.
2. Tap **Software Update**.
3. If an update is available, tap **"Download and Install."** Your device must be plugged into a power source to complete the installation.

2. Enable Automatic Updates (strongly recommended)

Why: This is the "set it and forget it" approach to security. It ensures your device installs critical patches as soon as they are available, so you are always protected.

Steps:

1. From the **Software Update** screen, tap on **"Automatic Updates."**
2. Ensure both **"Download iOS Updates"** and **"Install iOS Updates"** are 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. This is a critical step in reducing your physical vulnerability.

The Action:

1. Manage Per-App Permissions

Steps:

1. Go to **Settings > Privacy & Security > Location Services**.
2. Review the list. If an app doesn't need your location, set its permission to **"Never."**
3. For apps that need location but not constantly, choose **"While Using the App."** Avoid **"Always."**

2. Disable Significant Locations

Why: This is a private log your iPhone keeps of your most visited places. It's a goldmine for an adversary trying to profile you. It is strongly recommended to be turned off.

Steps:

1. From **Location Services**, scroll to the bottom and tap **System Services**.
2. Tap **"Significant Locations."**
3. Toggle this setting **OFF**.

03: DISABLE APP TRACKING (AD-ID)

Why: This is the unique "license plate" used to track your activity across different apps and websites. Disabling it breaks the primary tool advertisers and adversaries use to profile you. This is the iOS fix for the vulnerability that led to the 2019 attack in Iraq.

The Action:

1. Disable App Tracking

Steps:

1. Go to **Settings > Privacy & Security > Tracking**.
2. Ensure the toggle for **"Allow Apps to Request to Track"** is set to **OFF**. This single action prevents all future apps from using your Ad-ID.

04: REVIEW APP PERMISSIONS

Why: Just like location, many apps request access to your microphone, camera, contacts, and photos when they don't need it. Each permission is a potential avenue for data exfiltration or surveillance.

The Action:

1. Audit App Access

Steps:

1. Go to **Settings > Privacy & Security**.
2. Tap on sensitive permissions like **"Contacts," "Microphone,"** and **"Camera."**
3. Review the list of apps that have access. If an app does not need this permission to function, toggle its access **OFF**.

iPhone 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:** Significant Locations is OFF and apps have minimal location access.

☐ **App Tracking is OFF:** The master "Allow Apps to Request to Track" switch is off.

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