Threats to mobile devices are more prevalent and increasing in scope and complexity. Users of mobile devices desire to take full advantage of the features available on those devices, but many of the features provide convenience and capability but sacrifice security. This best practices guide outlines steps the users can take to better protect personal devices and information.

**Bluetooth®**

Disabling Bluetooth® when you are not using it is recommended. Airplane mode does not always disable Bluetooth®.

**Wi-Fi**

Do not connect to public Wi-Fi networks. Disable Wi-Fi when unneeded. Delete unused Wi-Fi networks.

**Location**

Disable location services when not needed. Do not bring the device with you to sensitive locations.

**Recent applications soft key**

Disable Bluetooth® when you are not using it. Airplane mode does not always disable Bluetooth®.

**Near-field communication (NFC)**

Update the device software and applications as soon as possible.

**Biometrics**

Consider using Biometrics (e.g., fingerprint, face) authentication for convenience to protect data of minimal sensitivity.

**POP-UPS**

Unexpected pop-ups like this are usually malicious. If one appears, forcibly close all applications (i.e., iPhone®: double tap the Home button® or Android®: click "recent apps" soft key).

**Applications**

Install a minimal number of applications and only ones from official application stores. Be cautious of the personal data entered into applications. Close applications when not using.

**Untrusted accessories**

Only use original charging cords or charging accessories purchased from a trusted manufacturer. Do not use public USB charging stations. Never connect personal devices to government computers, whether via physical connection, Wi-Fi, or Bluetooth®.

**Software updates**

Update the device software and applications as soon as possible.

**Conversations**

Do not have sensitive conversations in the vicinity of mobile devices not configured to handle secure voice.

**TEXT MESSAGES**

Do not have sensitive conversations on personal devices, even if you think the content is generic.

**Attachments/Links**

Do not open unknown email attachments and links. Even legitimate senders can pass on malicious content accidently or as a result of being compromised or impersonated by a malicious actor.

**Control**

Maintain physical control of the device. Avoid connecting to unknown removable media.

**Case**

Consider using a protective case that drowns the microphone to block room audio (hot-miking attack). Cover the camera when not using.

**Power**

Power the device off and on weekly.

**Do not**

Never connect personal devices to government computers, whether via physical connection, Wi-Fi, or Bluetooth®.

The information contained in this document was developed in the course of NSA’s Cybersecurity mission, including its responsibilities to assist Executive departments and agencies with operations security programs.

*For iPhone® or later, see: support.apple.com/en-us/HT201330

1Bluetooth® is a registered trademark of Bluetooth SIG, Inc.

2iPhone® and iPhone® applications are a registered trademark of Apple, Inc.

3Android® is a registered trademark of Google LLC.
## WHAT CAN I DO TO PREVENT/MITIGATE?

<table>
<thead>
<tr>
<th>Threat/Vulnerability</th>
<th>Update Software &amp; Apps</th>
<th>Only Install Apps from Official Stores</th>
<th>Turn Off Cellular, WiFi, Bluetooth</th>
<th>Do Not Connect to Public Networks</th>
<th>Use Encrypted Voice/Text/Data Apps</th>
<th>Do Not Click Links or Open Attachments</th>
<th>Turn Device Off &amp; On Weekly</th>
<th>Avoid Carrying Device/No Sensitive Conversations Around Device</th>
<th>Lock Device with PIN</th>
<th>Maintain Physical Control of Device</th>
<th>Use Trusted Accessories</th>
<th>Turn Off Location Services</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spearphishing (To install Malware)</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
</tr>
<tr>
<td>Malicious Apps</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
</tr>
<tr>
<td>Zero-Click Exploits</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
</tr>
<tr>
<td>Malicious Wi-Fi Network/Close Access Network Attack</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
</tr>
<tr>
<td>Foreign Lawful Intercept/Untrusted Cellular Network</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
</tr>
<tr>
<td>Room Audio/Video Collection</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
</tr>
<tr>
<td>Call/Text/Data Collection Over Network</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
</tr>
<tr>
<td>Geolocation of Device</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
</tr>
<tr>
<td>Close Access Physical Attacks</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
</tr>
<tr>
<td>Supply Chain Attacks</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
<td>☑</td>
</tr>
</tbody>
</table>

Does not prevent (no icon) | Sometimes prevents | Almost always prevents