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 mobile devices and the sensitive information they contain.

**Airplane mode**

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

**Bluetooth®**

Avoid connecting to public Wi-Fi networks. Disable unused Wi-Fi networks.

**Wi-Fi**

Enable/Disable near-field communication (NFC) as needed. Disable when not needed.

**Location**

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

**Recent applications soft key**

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

**POP-UPS**

Unexpected pop-ups like this are usually malicious. If one appears, forcefully close all applications (i.e., iPhone® 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.

**SOFTWARE UPDATES**

Update the device software and applications as soon as possible.

**TRUSTED ACCESSORIES**

Only use original charging cords or charging accessories purchased from a trusted manufacturer. Never use public USB charging stations. Never connect personal devices to government computers, whether via physical connection, Wi-Fi, or Bluetooth®.

**CONVERSATIONS**

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

**CASE**

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

**PASSWORDS**

Use strong lock-screen pins/passwords: a 6-digit PIN is sufficient if the device wipes itself after 10 incorrect password attempts. Set the device to lock automatically after 5 minutes.

**TEXT MESSAGES**

Avoid 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 accidentally or as a result of being compromised or impersonated by a malicious actor.

**BIOMETRICS**

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

**CONVERSATIONS**

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

**CASE**

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

**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.

**SOFTWARE UPDATES**

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.

**CONVERSATIONS**

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

**CASE**

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

**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.

**SOFTWARE UPDATES**

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.

**CONVERSATIONS**

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

**CASE**

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

**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.

**SOFTWARE UPDATES**

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.

**CONVERSATIONS**

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

**CASE**

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

**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.

**SOFTWARE UPDATES**

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.

**CONVERSATIONS**

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

**CASE**

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

**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.

**SOFTWARE UPDATES**

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.

**CONVERSATIONS**

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

**CASE**

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

**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.

**SOFTWARE UPDATES**

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.

**CONVERSATIONS**

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

**CASE**

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

**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.

**SOFTWARE UPDATES**

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.

**CONVERSATIONS**

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

**CASE**

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

**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.

**SOFTWARE UPDATES**

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.

**CONVERSATIONS**

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

**CASE**

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

**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.

**SOFTWARE UPDATES**

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.

**CONVERSATIONS**

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

**CASE**

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

**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.

**SOFTWARE UPDATES**

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.

**CONVERSATIONS**

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

**CASE**

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

**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.

**SOFTWARE UPDATES**

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.

**CONVERSATIONS**

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

**CASE**

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

**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.

**SOFTWARE UPDATES**

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.

**CONVERSATIONS**

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

**CASE**

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

**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.

**SOFTWARE UPDATES**

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.
## 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>Use Mic-Drowning Case, Cover Camera</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</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>
<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>
<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>
<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>
<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>
<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>
<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>
<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>
<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>
<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>
<td></td>
</tr>
</tbody>
</table>

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