



National Security Agency | Mobile Device Best Practices

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.

- Airplane mode
- Bluetooth®
- Cellular service signal
- Location
- Near-field communication (NFC)
- Recent applications soft key
- Wi-Fi

- Avoid
- Disable
- Do
- Do Not

BLUETOOTH¹

Disable Bluetooth® when you are not using it. 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.

CONTROL

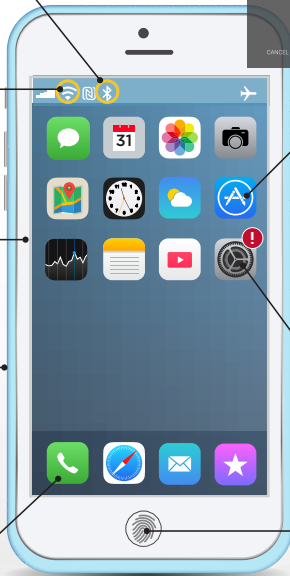
Maintain physical control of the device. Avoid connecting to unknown removable media.

CASE

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

CONVERSATIONS

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



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.

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.

TEXT MESSAGES

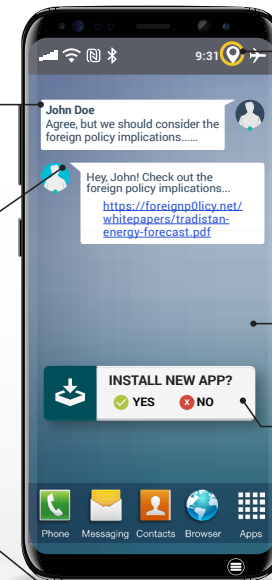
DO NOT have sensitive conversations on personal devices, even if you think the content is generic.

ATTACHMENTS/LINKS

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

TRUSTED 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®.



LOCATION

Disable location services when not needed. **DO NOT** bring the device with you to sensitive locations.

POWER

Power the device off and on weekly.

MODIFY

DO NOT jailbreak or root the device.

POP-UPS

Unexpected pop-ups like this are usually malicious. If one appears, forcibly close all applications (i.e., iPhone®²: double tap the Home button* or Android®³: click "recent apps" soft key).

*For iPhone X^{®2} 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.

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.



National Security Agency | Mobile Device Best Practices

WHAT CAN I DO TO PREVENT/MITIGATE?

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

Does not prevent (no icon)

Sometimes prevents

Almost always prevents

Disclaimer of Endorsement

The information and opinions contained in this document are provided "as is" and without any warranties or guarantees. Reference herein to any specific commercial products, process, or service by trade name, trademark, manufacturer, or otherwise, does not constitute or imply its endorsement, recommendation, or favoring by the United States Government, and this guidance shall not be used for advertising or product endorsement purposes.

NSA Cybersecurity

Client Requirements/General Cybersecurity Inquiries: Cybersecurity Requirements Center, 410.854.4200, Cybersecurity_Requests@nsa.gov.
Media Inquires: Press Desk: 443.634.0721, MediaRelations@nsa.gov.