Mobile Device Application Security Short

Student Guide

September 2024

Center for Development of Security Excellence

Contents

Mobile Device Application Security Short

Opening

Mobile devices are ubiquitous in our daily lives. We rely on mobile applications for entertainment, news, travel, messaging, and more. But there are risks. In a Management Advisory from the Department of Defense, or DOD, Office of the Inspector General, or OIG, a recent audit "determined that … DOD personnel are downloading mobile applications to their mobile devices that could pose operational and cybersecurity risks to DOD information systems."

These risks include unnecessary, invasive permissions that require access to user contact lists and photos; access to the device's sensors, such as the camera, microphone, or global positioning system, or GPS; and malicious code.

Malicious code is especially risky with unauthorized, unmanaged applications. In a study of 100,000 popular mobile applications:

- 83% of shopping applications requested access to the camera.
- 62% of news applications requested access to the photo library.
- 56% of games requested access to the calendar.
- 53% of sports applications requested access to location.
- 40% of entertainment applications requested access to the microphone.

This Short will help you to check your device's privacy and security settings and to take steps to protect your mobile device.

Here is the learning objective:

- Apply best practices when using Android or iOS mobile devices, including the use of applications, downloads, and security settings.

Definitions

"Mobile device" refers to any portable computing device with communication capabilities, such as a smart phone or tablet. The information in this Short applies to all mobile devices and apps, whether personally-owned or DOD-issued. However, if you have a DOD device, additional restrictions will apply.

An approved mobile device, or AMD, refers to a mobile device that is not owned by the government but is approved to store, process, transmit, or display DOD information up to Controlled Unclassified Information, or CUI.

Mobile devices run mobile applications or "apps." These are software programs installed on a device with a mobile operating system, such as Apple iOS or Android. In a DOD environment, apps may be:

- **Managed:** Approved for official DOD business
- **Authorized unmanaged:** Authorized by DOD Components for personal use on DOD devices, or
- **Unauthorized unmanaged:** Downloaded from public application stores and not assessed by the DOD. Therefore, unauthorized unmanaged apps cannot be used to conduct official DOD business or for personal use on DOD mobile devices.

Scenario 1: Invasive Permissions (Contact List)

Suppose you were in the process of downloading a weather app to check the forecast. While downloading you realize that the app permissions granted the app access to your contact list, adding all your contacts to spam mailings! Yikes! In addition to costing resources and time, as a DOD employee or contractor, this could also represent a security risk.

According to the Inspector General's Management Advisory mentioned earlier, "Many seemingly harmless commercial applications also pose a threat to DOD information and information systems when they require unnecessarily invasive permissions on DOD mobile devices". Video games, shopping, or weather applications routinely require access to a device's contact list, messaging platforms, location data, or other personal information, and often lack sufficient security or encryption standards. So what can you do about it?

iOS

If you are protecting an iOS operating system, please open your phone and explore the following:

- First, review your permissions under Privacy & Security and make any necessary changes.
- Next, run an App Privacy Report to see how your apps are using permissions for features like your contact lists, photos, and camera.
- Finally, explore the Contact Key Verification feature.
    - This feature allows you to generate unique codes that you and your contacts can use to verify each other's identities.
    - Contact Key Verification also checks application activity and usage by enabling screen time to see what apps are being used.

Android

If you are protecting an Android operating system, please open your phone and explore the following:

- First, check permissions for each app under Settings and make any necessary updates.
- Next, visit your Privacy Dashboard to see which apps are accessing data, which permissions apps are using, and when apps are accessing your data.
- Finally, you can try sorting your apps by last used in apps. This helps you to determine which apps were recently used. If you know you haven't used an app in a while but it appears near the top of the list, then perhaps that app is actively accessing your data.

Scenario 2: Invasive permissions (GPS)

Now suppose you were in the process of downloading a shopping app to take advantage of some discounts. After downloading you realize that you gave the app permission to access your location while in use. Even some authorized unmanaged applications access features like GPS, which can lead to a real risk to national security. For example, news outlets reported that the locations of sensitive DOD facilities and personnel had been publicly exposed through use of a fitness application. So what can you do about it? First, always consider whether you want the app to know your location, and when you want to grant or deny that information.

iOS

If you are protecting an iOS operating system, please open your phone and explore iOS Location Services. Location Services allow apps to use available information from GPS, Bluetooth, Wi-Fi, and cellular data. When in use, the Location Services icon appears in the status bar. Some apps will make a one-time request for location data, while others will ask for information now and in the future. Please note that you can change an app's access at any time under Location Services in Privacy & Security.

Android

If you are protecting an Android operating system, please open your phone and explore: your location, camera, and microphone permissions. You may be able to choose whether you want an app to access these features:

- All the time (location only)
- Only while using the app
- App should ask every time it accesses these features
- Do not allow access

Note that you can change an app's location, camera, and microphone permissions at any time under App Settings.

Scenario 3: Malicious Code

Now imagine this scenario.

You receive a text message saying that your package is awaiting delivery. The message includes a link. You're anticipating a delivery soon, so you select the link. Oh no! You accidentally download malware.

Most malware is downloaded from public application stores. Lately, however, malware is also being downloaded through text messaging.

Malware can *steal sensitive information* such as your banking credentials, financial data, login credentials, contact lists, e-mails, and text messages. Malware can also *attack your device's platform software* to gain additional privileges and *disable security features* and *install spyware* to control device features like your GPS, camera, microphone, and keystrokes.

So what can you do about it? The most important thing you can do is ensure that you only download known or trusted apps. iOS and Android also have some additional elevated security features available.

iOS

As an iOS user who works for the DOD or cleared industry, you have elevated security needs. You might even be the *target* of state-sponsored spyware. iOS offers a feature called **Lockdown Mode** that you may want to consider. This feature offers elevated security, but note that it could also involve a reduction in performance and usability. Take a moment and use your device to find and explore the Lockdown Mode setting under Privacy & Security.

Android

Android's operating system offers a feature called **Lockdown Mode**. Although this doesn't offer the comprehensive security protections that iOS Lockdown Mode offers, you may find it useful. You can impact your phone's unlocking features by selecting "Lockdown" under Settings. Android Lockdown Mode will turn off fingerprint sensors, facial recognition, and voice recognition until you next unlock your phone.

Review Activity

Select the best response. Check your answers in the Answer Key at the end of this Student Guide.

1. Now consider this scenario. What would you do? You have decided to download a photo editing app to your personal device. This is an unauthorized, unmanaged app but you are not using it to conduct DOD business. Which permissions will you grant after completing the download?

- ○ Your contact list all the time
- ○ Your camera while using the app
- ○ Your camera all the time
- ○ Your location while using the app

2. Now consider this scenario. What should you do? You want to talk to a coworker about DOD business on your personal mobile device. The coworker suggests an app that is available in the app store, but it is unauthorized and unmanaged. What should you do?

- ○ Download a widely used international chat app
- ○ Select a managed app instead
- ○ Select an authorized unmanaged app, then manage its permissions
- ○ Avoid using chat apps on mobile devices

3. Now consider this scenario. What should you do? Your supervisor receives a text message with a link to download an app that seems related to work, but he is not sure. What advice would you give him?

- ○ Only select links with https
- ○ Only download trusted apps
- ○ Only select links with http
- ○ Do not download apps to any of your mobile devices

Conclusion

Congratulations! You have completed the Mobile Device Application Security Short. In this Short, you learned about some of the risks of mobile device apps – and you also learned what you can do to keep your devices safe. You should now be able to apply best practices when using Android or iOS mobile devices, including the use of applications, downloads, and security settings.

Appendix A: Answer Key

1. You have decided to download a photo editing app to your personal device. This is an unauthorized, unmanaged app but you are not using it to conduct DOD business. Which permissions will you grant after completing the download?

- ○ Your contact list all the time
- ⦿ Your camera while using the app (correct response)
- ○ Your camera all the time
- ○ Your location while using the app

Feedback*: You may grant access to your camera while using the app to edit photos. However, ensure that the app is not asking for access to your contact list, your location, or your microphone. These are unnecessary and potentially unsafe permissions for the app.*

2. Now consider this scenario. What should you do? You want to talk to a coworker about DOD business on your personal mobile device. The coworker suggests an app that is available in the app store, but it is unauthorized and unmanaged. What should you do?

- ○ Download a widely used international chat app
- ⦿ Select a managed app instead (correct response)
- ○ Select an authorized unmanaged app, then manage its permissions
- ○ Avoid using chat apps on mobile devices

Feedback*: You should avoid downloading any unauthorized unmanaged apps to your DOD mobile device.*

3. Now consider this scenario. What should you do? Your supervisor receives a text message with a link to download an app that seems related to work, but he is not sure. What advice would you give him?

- ○ Only select links with https
- ⦿ Only download trusted apps (correct response)
- ○ Only select links with http
- ○ Do not download apps to any of your mobile devices

Feedback: *You should tell your supervisor to only download trusted apps.*