Security Risks with Mobile Apps

Applications (apps) on your smartphone or other mobile devices can be convenient tools to access the news, get directions, pick up a ride share, or play games. But these tools can also put your privacy at risk. When you download an app, it may ask for permission to access personal information—such as email contacts, calendar inputs, call logs, and location data—from your device. Apps may gather this information for legitimate purposes—for example, a ride-share app will need your location data in order to pick you up. However, you should be aware that app developers will have access to this information and may share it with third parties, such as companies who develop targeted ads based on your location and interests.

How can you avoid malicious apps and limit the information apps collect about you?

Before installing an app

- Avoid potentially harmful apps (PHAs) – Reduce the risk of downloading PHAs by limiting your download sources to official app stores, such as your device's manufacturer or operating system app store. Do not download from unknown sources or install untrusted enterprise certificates. Additionally—because malicious apps have been known to slip through the security of even reputable app stores—always read the reviews and research the developer before downloading and installing an app.
- Be savvy with your apps – Before downloading an app, make sure you understand what information the app will access. Read the permissions the app is requesting and determine whether the data it is asking to access is related to the purpose of the app. Read the app's privacy policy to see if, or how, your data will be shared. Consider foregoing the app if the policy is vague regarding with whom it shares your data or if the permissions request seems excessive.

On already installed apps

- Review app permissions – Review the permissions each app has. Ensure your installed apps only have access to the information they need, and remove unnecessary permissions from each app. Consider removing apps with excessive permissions. Pay special attention to apps that have access to your contact list, camera, storage, location, and microphone.
- Limit location permissions – Some apps have access to the mobile device's location services and thus have access to the user's approximate physical location. For apps that require access to location data to function, consider limiting this access to when the app is in use only.
- Keep app software up to date – Apps with out-of-date software may be at risk of exploitation of known vulnerabilities. Protect your mobile device from malware by installing app updates as they are released.
- Delete apps you do not need – To avoid unnecessary data collection, uninstall apps you no longer use.
- Be cautious with signing into apps with social network accounts – Some apps are integrated with social network sites—in these cases, the app can collect information from your social network account and vice versa. Ensure you are comfortable with this type of information sharing before you

sign into an app via your social network account. Alternatively, use your email address and a unique password to sign in.

What additional steps can you take to secure data on your mobile devices?

- Limit activities on public Wi-Fi networks – Public Wi-Fi networks at places such as airports and coffee shops present an opportunity for attackers to intercept sensitive information. When using a public or unsecured wireless connection, avoid using apps and websites that require personal information, e.g., a username and password. Additionally, turn off the Bluetooth setting on your devices when not in use. (**See Cybersecurity for Electronic Devices**.)
- Be cautious when charging – Avoid connecting your smartphone to any computer or charging station that you do not control, such as a charging station at an airport terminal or a shared computer at a library. Connecting a mobile device to a computer using a USB cable can allow software running on that computer to interact with the phone in ways you may not anticipate. For example, a malicious computer could gain access to your sensitive data or install new software. (**See Holiday Traveling with Personal Internet-Enabled Devices**.)
- Protect your device from theft – Having physical access to a device makes it easier for an attacker to extract or corrupt information. Do not leave your device unattended in public or in easily accessible areas. (**See Protecting Portable Devices: Physical Security**.)
- Protect your data if your device is stolen – Ensure your device requires a password or biometric identifier to access it, so if is stolen, thieves will have limited access to its data. (**See Choosing and Protecting Passwords**.) If your device is stolen, immediately contact your service provider to protect your data. (**See the Federal Communications Commission's Consumer Guide: Protect Your Smart Device**.)

Get the lastest information from our website. Scan the QR Code to go directly to this page.