


Privacy and Mobile Device Apps



What are the risks associated with mobile device apps? Applications (apps) on your smartphone or other mobile devices can be convenient tools to access the news, get direction, or pick up a ride share, but these tools may 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. Mobile apps may gather information from your mobile device for legitimate purposes. For example, a rideshare app will need your location data in order to pick you up. However, you should be aware that the 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** - only download apps from the official app stores such as your device's app store. Before downloading, make sure you understand what information the app will access. Read the permissions the app is requesting and determine whether the data is asking to access is related to the purpose of the app.
- **On already installed apps** - review the permissions each app has. Install app updates as they are released. For apps that require access to location data to function, consider limiting this access to when the app is in use only. To avoid unnecessary data collection, uninstall apps you no longer use. 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.
- **Limit activities on public WI-Fi networks.** When using a public or unsecured wireless connection, avoid using apps and websites that require login information. Additionally, turn off the Bluetooth setting on your devices when they are not in use.
- **Ensure your device requires a password or biometric identifier to access it,** so if stolen, thieves will have limited access to its data. If your device is stolen, immediately contact your service provider to protect your data.