Why should you always check app permissions before pressing install?

Taking a moment to review your app permissions can save you a lot of privacy and security problems later on!

Every time you download a new app, you should check the permissions it requests. Many apps do need certain access to specific features, like your location, contacts, etc., but some apps go beyond that.

Taking a moment to review your app permissions can save you a lot of privacy and security problems later on!

App permissions can be a privacy nightmare

Essentially, app permissions are requests for access to different parts of your device — camera, microphone, location, contacts, etc. While they may seem harmless, these permissions can be a way to access personal data if you're not careful or don't know how Android app permissions work.

There are flashlight apps that ask for access to your contacts, and photo gallery apps that want your exact location. It's completely ridiculous, but many of us blindly accept it without a second thought. This kind of carelessness is exactly what some developers are counting on.

The truth is, many apps ask for more permissions than they actually need to function. A simple weather app might need your location, but does it really need access to your call history? The answer is a resounding no. When apps gain unnecessary access to your personal information, they can collect data that can be sold to advertisers or, worse, potentially used for identity theft.

What's frustrating is that some developers deliberately design apps to collect as much user data as possible, not just to improve the experience but also to monetize your information. Many people have uninstalled some apps after discovering that they collect data that is completely unrelated to their core function.

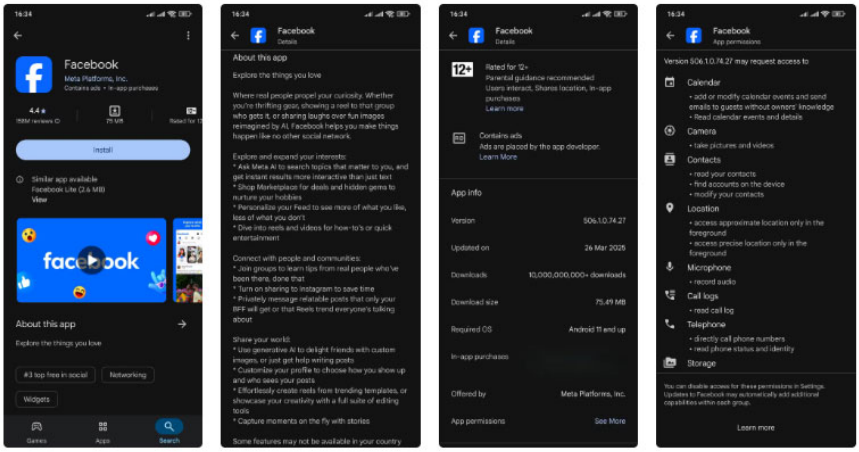
The risks extend beyond privacy concerns. Excessive permissions can drain your battery, use up your data limit, or compromise your device's security. So being vigilant about app permissions isn't just good practice; it's critical.

How to check app permissions before installing

Get into the habit of checking apps before you install them and you'll save yourself a lot of privacy trouble. Checking permissions only takes a minute, but it could save you months of unwanted data collection. Here's the process for Google Play, but you can adapt it for other app stores.

1. Open **Google Play** and find the app you want to download.
2. Scroll down to the **About this app** section .
3. Look for **App permissions** or **Data safety** .
4. Click **See more** to expand the full list of permissions.
5. Review what the app is requesting access to.
6. Ask yourself: "Does the app really need this permission to function?".

If you're unsure of the process, check out our guide on how to download and update apps on Android for more instructions.



If you're on iOS, the App Store works a little differently, but the concept is the same—always check what you're agreeing to before you hit install. Apple's app ecosystem is generally more secure than Android's, though. Still, you should check app permissions on your iPhone and iPad.

When looking at permissions, you should immediately be suspicious of any app that asks for access to features that are completely unrelated to the app's function. Any app that wants access to SMS messages, call logs, or precise location should make you stop and think twice - unless there's a clear reason why the app needs this information.

Storage and camera access are generally safer, especially if the app's purpose requires them. However, always consider whether an app needs persistent access or just grants it when it needs it.

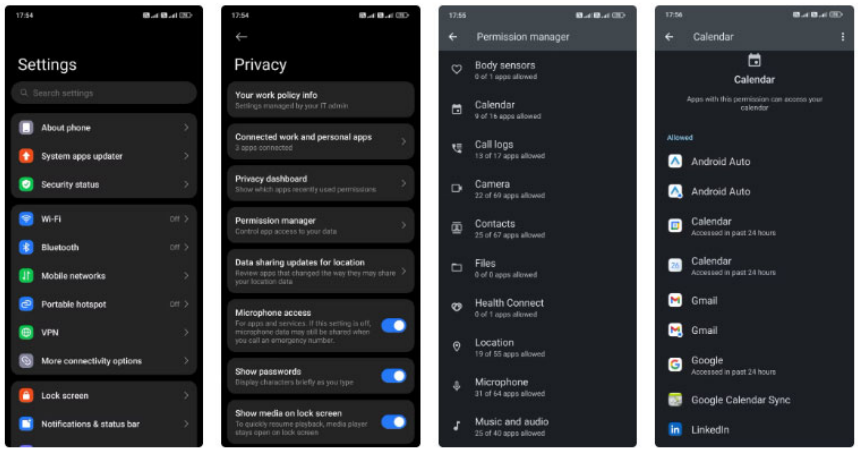
How to manage permissions for installed apps

Installing apps with the right permissions is only half the battle. Many apps sneakily ask for additional permissions after an update. For example, a game that initially only needed access to storage might suddenly want access to your location and contacts after an update. That's why it's important to regularly check the permissions of installed apps.

Set a semi-annual reminder to check what permissions your apps currently have. Here's a step-by-step process for Android devices:

1. Open the Settings app on your device.

2. Scroll down and tap **Privacy** (or **Privacy protection** on some devices).
3. Select **Permission manager** or **App permissions** .
4. Review permissions by category (camera, location, microphone, etc.).
5. Tap any permission to see which apps have access to it.
6. Turn off access for any apps that don't really need that permission.



For iPhone users, the process is similar—just go to **Settings > Privacy & Security** , then select each permission type to see which apps have access.

It's most effective to switch permissions from "Allow all the time" to "Allow only while using the app" whenever possible. Location tracking is especially important to limit, as some apps track movement in the background for no good reason.

The safest approach is to be very selective. The 'Ask every time' option is available for some sensitive permissions like camera and microphone access. Yes, that means tapping through an extra prompt every now and then, but it prevents any app from accessing your camera without your knowledge. Taking a few steps to secure your phone usage will give you peace of mind without much inconvenience.

Eventually, you'll develop an instinct for what permissions make sense. Taking just a few extra seconds to consider permissions before hitting install can save you from becoming an unwitting data point in someone else's profit model.