What To Do Before Downloading An App?

Do you remember the times before App Store came into play? Smartphone users used to rely on applications they downloaded from the internet. In most, there was no guarantee that those apps were legit. Yeesh.

Now, Apple and Google check all apps in their app stores. But they are not all-powerful. Even when you download an app from a trustworthy source, there are some critical things you should check before installing an app on your device.

We'll go over some of the basic steps you should take to ensure the security of the applications you're about to install. Let's go!

Why be careful when downloading applications?

According to a study, an average person has around 80 apps on their phone. Every fourth app has at least one security vulnerability with a high risk. Quick math: if you have 80 apps installed on your phone, 20 have high-risk security flaws. Yikes.

Use an iPhone and think you're in a safe zone ? We have some bad news. According to this study, 38% of iPhone applications have security flaws. The number for Android smartphones is slightly higher, standing at 43%.

As you can see, apps aren't as secure as we would like them to be. Some applications can be insecure on purpose, and people behind them develop such apps to steal your money or data. Let's see what you can do to avoid installing them.

How to make sure an app is safe to download?

Some practices can help you ensure that an app you're about to install is safe.

What are the things to consider before downloading the app?

1. Download apps from trusted sources only

You'll be better off without installing apps from random third-party websites. Installing an app from a third-party source on an iPhone without jailbreak is almost impossible, so we recommend you stick to App Store.

While you can install apps from any website on Android relatively easily, our advice is to go with Google Play. If an app is not there, it might be a sign that it's either illegal or didn't make it through the store's security audit.

2. Pay attention to the reviews in the app store

When considering installing an app, look at what people say about it in the reviews section. Some red flags are the absence of negative reviews or any reviews at all. It may come as a surprise, but all **legit apps have bad reviews**. If an app you're about to get has only positive reviews written in a similar way, be cautious — it might not be what it pretends to be.

3. Check the app's privacy policy

Ugh, those boring docs we all skip to get our hands faster on something. Nevertheless, it's good practice to research how app developers describe their approach to collecting your data by reading the privacy policy.

Try googling the first paragraphs of the app's privacy policy. It may be possible that developers just stole the text from a legit app. If googling returns links to other websites with similar privacy policies, you better not install that app.

4. Check the app store's privacy badges

Recently, Apple and Google introduced special privacy badges on app pages. They are a way for developers to quickly share what kinds of data they collect from users.

Consider having a look at them when thinking about installing an app. You can read more about privacy badges on App Store and Google Play here and here.

5. Make sure the app comes from a legit developer

If you know little about the app you're about to install, try to find more information on the developers or other apps created by them.

In the case of App Store, you'll find the developer's contact information in the "Information" section under the app description. Google Play doesn't make such information easy to find, so you might have to research. For example, if the developer has a website, read more about them.

Make sure that the name of the app developer is spelled correctly. Some criminals make slight changes to the spelling of the legitimate app developer's name and put an app on the store in an attempt to deceive users.

Version History is another place for you to get a sense if the app is safe. Installing an app can be risky if it hasn't been updated in a long time. Additionally, read what developers write in their release notes. This could be a warning sign if it only includes vague and general information.

Another good way to determine whether an app is safe is to read its description. It might be a sign of a scam if it has poor grammar and spelling or is suspiciously detailed. Plus, try googling the app description. Like a privacy policy, it can easily be stolen from another app.

Finally, scrutinize the number of app downloads. The app must have at least 100K or more installs if it is legit.

6. Make sure your OS is updated

If you're done with all the rest of the precautions and sure that the app is safe to install, there's one more thing to be done before you hit the Download button. Double-check that your device's operating system is up to date. It is essential because operating system patches are rolled out occasionally to fix security flaws.

What are the things to consider after downloading the app?

Our journey is not over after you've installed the app. There are several small but important things you can do to ensure the security of your data after you install any application.

1. Check app permissions

It is important to remember that apps can't do most things independently. To do anything on a device, they need permission from you, the user!

Thus, when thinking about permissions, focus on the access the app needs. Does it really need access to your camera or microphone? If it does, and you are unsure why it would need this, consider not giving the app that permission.

For example, if you've installed a Flashlight app that asks for your geolocation, you better not grant it that permission. Plus, if you aren't sure whether you want to enable a feature in the app, you can always say "no" and then allow it when needed.

Here's how to check app permission depending on your platform.

iOS: Open Settings, go down, and select the app you're interested in. Here you can see various app permissions and turn them off.

Android: Open the Settings app, go to the Apps section, and select the app you're interested in. Here you can check the app's permissions and control them.

2. Check app access to your data

In addition to accessing some smartphone features, an app can ask for some of your data, like your contacts or health data. Therefore, you should also check which of your data the app can access. You can do it the same way as you would with app permissions.

3. The general look and feel of the app

Finally, pay attention to the quality of the app experience. Even if everything else shows that the app is legit, you should consider how the app looks and feels.

For example, if the application layout and interface look strange, or it has missing buttons or slow loading times, these can be signs that a malicious developer has built the app.

Conclusion

Ensuring that the apps you install are safe and secure is essential. You can take a few steps to ensure the apps are legit before you install them.

Pay attention to the privacy badges, make sure you only download apps from legit developers, read the app description, check the version history and the number of downloads, and ensure your OS is up to date.

After you've installed the app, check the app permissions and access to your data, as well as the general look and feel of the app. Do not hesitate to uninstall the app if something looks or feels off.

Take care, and have fun with safe apps only