# 1. Only install necessary apps

This first piece of advice is a tough one for many people to swallow. However, you should ask yourself if you really need that random, untrusted game you found in the Google Play Store. The answer is probably not.

This action is important because you never know what kind of malicious code is to be found lurking within an app or an ad framework for an app. In a perfect world, the stock apps found on your device should be enough. When you do want to download a third-party app, make sure it's from a trusted source, such as a large and reputable company.

That said, do your research before downloading.

# 2. Stick to the Google Play Store

Continuing my previous point, stick to safe downloads. Using the Google Play Store makes safe downloads more likely. That's not to say that EVERY app on the platform can be trusted, but most of them have been carefully vetted.

Also, Android has a security feature that will send you a text if the internal security team notices that an app download looks harmful.

Note that a high number of downloads does not mean the app is trustworthy.

# 3. Do NOT tap links in SMS messages from unknown sources

Never, ever tap a link in an SMS from a source you don't know.

Any time you receive an SMS from an unknown source, assume it is an attempt to access your data or insert malicious code onto your device. And even if that SMS message seems to come from a reputable source, chances are still good that it's a phishing attempt or worse.

# 4. Update, update, update

Google releases regular security patches for the Android operating system and it's absolutely crucial that you install them. Those updates don't just contain new and exciting features. They also patch security vulnerabilities to keep you safe.

his process can be completed from the Google Play Store. Simply, **tap your profile image > Manage apps & device > Update all**. You may also be able to set your phone to keep apps updated automatically.

## 5. Don't connect to unsecured networks without a VPN

The second you connect to an unsecured wireless network, you open yourself up to the possibility of having your packets sniffed or your device compromised.

Here are some of the most dangerous apps you should NOT install on your Android device: UC Browser, CLEANit, Dolphin Browser, and SuperVPN Free VPN Client. These are just a few of many harmful apps, so always do some research before downloading.

Find Tips from Tracking your device to setting up security features on your Android Phone:

Advanced and proactive Android device security | Android