Does turning off your Android phone protect you from malware?

Turning off your phone every day can also be one of the things you can do to protect yourself.

Malware comes in all shapes and sizes, and can steal your money and identity or turn your device into a zombie cryptocurrency miner.

While you can rely on Google to keep your Android device free from unwanted and malicious programs, turning off your phone daily can also be one of the things you can do to protect it. self.

How does malware get into Android phones?

Malware often enters your phone as part of a larger package. It can be embedded with a common or useful application such as a spirit level, calculator or flashlight application.

These apps are usually quite useful, fairly harmless, and the kind of tools you might need urgently without caring too much about the source. Sometimes, they are some of the most popular apps on Android.

Malware distributors can buy apps outright or pay developers a small amount of money to add a few innocent-looking lines of code to their apps.

Malware is rarely included in the application itself; instead, additional code is used to download more code from the remote server.

This could be something that runs independently on your device and sometimes sends information back to developers, such as a log of your keystrokes, or malware that could be manipulated. Direct control by a remote operator can add modules and functions quickly.

Once criminals have your login information, they can access your other online accounts and even use them to break into your home network or your employer's.

A sign that an app might be malware is that it requests access to phone functions unrelated to its purpose. The spirit level monitoring app doesn't need access to your keyboard, and the computer has no business listening to your microphone. You should at least check the permissions of all installed Android apps.

How to turn off your phone to keep you safe

To start, if your phone is not turned on and cannot execute code, malware cannot run at all. However, it is pointless to own a communication device that cannot communicate!

Instead, experts recommend restarting your device regularly, usually once per day or once per week - the exact frequency doesn't matter, as long as you power your phone down regularly.

If malware is embedded in an app that you have left running in the background, this will force the app to close and reset the connection.

In many cases, without manually restarting the application, you will not be attacked: The application will not be able to contact the headquarters and cannot transfer your data to criminals over the Internet.

Does turning off your phone always keep you safe from malware?

In short, no. Some apps start running on your phone as soon as it boots. On Android phones, these include all of Google's suite of apps like Google Drive, Google Photos, the default dialer, and the SMS app.

Other third-party apps also have this perk.

If an app that has no legitimate need to launch when your phone restarts has this privilege, it may contain malware.

To test which apps launch immediately after your Android phone boots, enable Developer Mode, close all running apps, then restart your device. From within the Developer Mode menu, click Go to **Running Services** and find applications that should not be running at that time.

Consider whether your computer needs to load in the background when starting up.