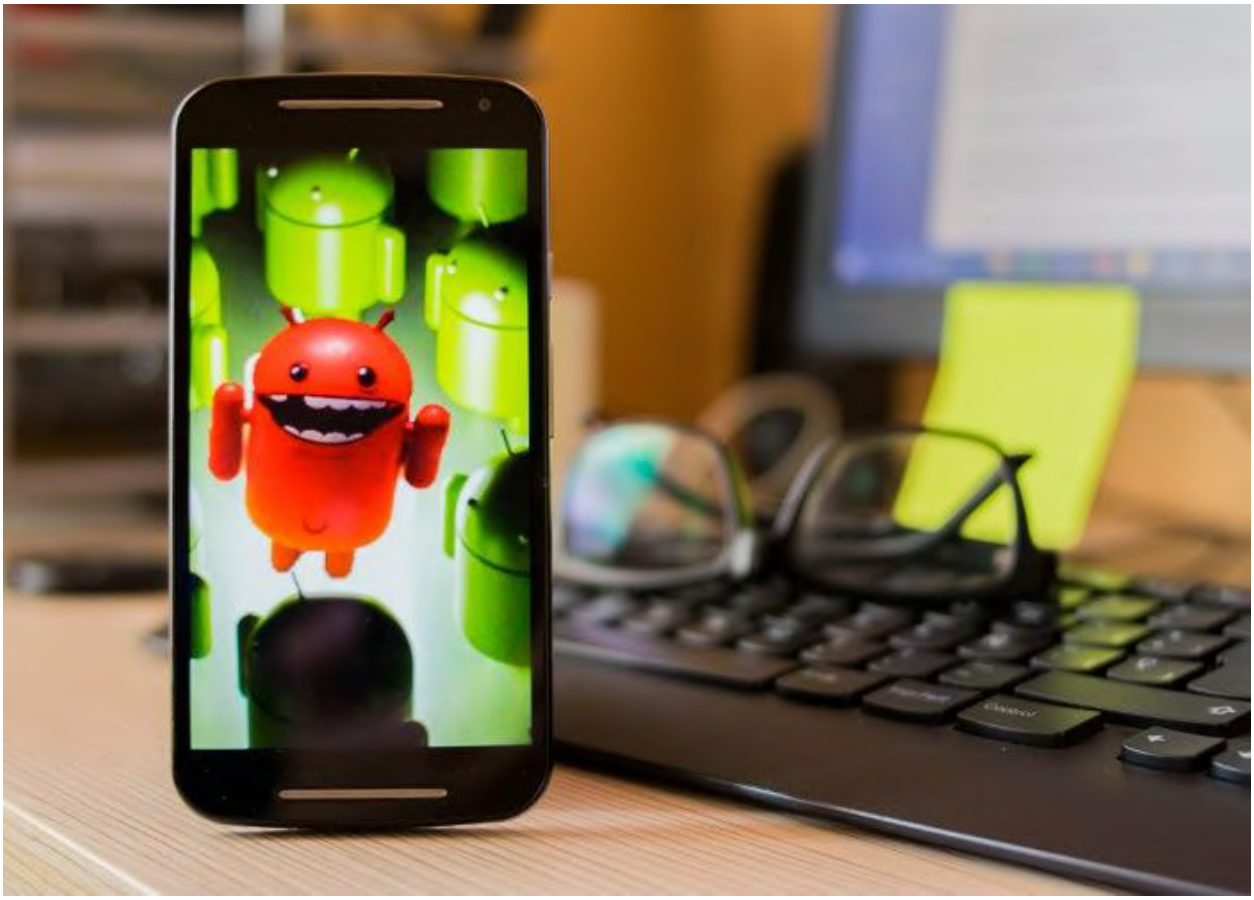
How to Remove an Android Virus

Viruses for Android are becoming more and more common. Here's what to do if you think your phone is misbehaving without an obvious explanation.



Types of mobile viruses

Android viruses come in many flavors, each with its own quirks and entry vectors designed around a certain vulnerability. The following are the most common:

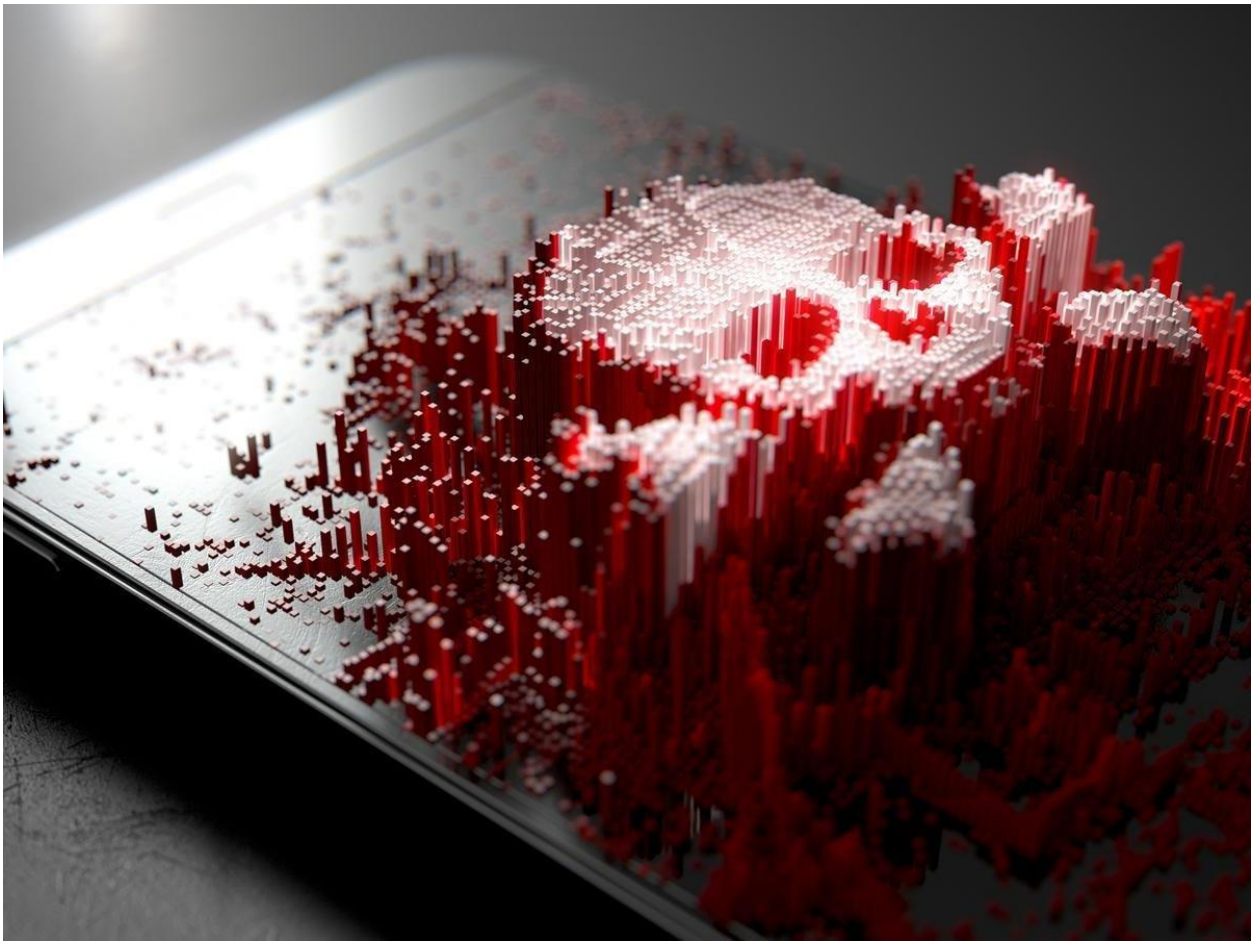
- **Spyware:** This type of malware is designed to stealthily pick up information from your phone, and transmit it back to the C&C (command and control server). Spyware comes disguised as legit applications, which is how the cybercriminal tries to fool the user into installing them. Once installed, they start recording information including SMS/text messages, URLs being browsed, application activity, keys being pressed, usernames, and passwords.
- **Ransomware:** This malicious program encrypts and locks up your important files, then offers to release them only if you pay a ransom. Spoiler alert: They almost never release the files. But given that so many users have very important data on their smartphones, the impulse to give in and pay is strong. (But don’t do it!)

- **Worms:** These are the most aggressive type of Android phone viruses. Designed to endlessly reproduce themselves, worms don't need any user interaction in order to execute. They generally arrive via SMS, MMS, or other digital media.
- **Trojans:** These piggyback on legit applications and infect your phone once it has been installed. Unlike worms, trojans need a user to install them before they can carry out their actions. Once activated, trojans can deactivate certain applications or lock-up your phone for a certain period of time.

Where viruses come from

To make sure none of the above ever happens to you, it's crucial that you know how mobile malware makes its way into your phone. There are four venues viruses come from:

- **Infected applications:** The most common MO of hackers, popular applications are repackaged with the malware and then distributed through app stores. Oftentimes, cyber-criminals will come up with completely new applications designed specially to trick users into installing them.
- **Malvertisements:** Malvertising is the practice of inserting viruses in ads that are distributed through ad networks. Simply clicking on an ad can trigger a virus download, infecting the device.
- **Scams:** Users are sent links to infected web pages that contain malicious code. Simply visiting the page can start a virus downloading to the phone (unless it is protected by an antivirus software).
- **Direct-to-device downloads:** The least likely type, direct-to-device infections require the hacker to attach a targeted device to another, and manually install the malware to it. This is the stuff of much high-profile corporate espionage.



How to Remove an Android Virus

Method 1: Clear the cache

If you're seeing pop-ups or redirects, the best thing to do is clear your browser cache, either within the browser's own settings menu or by going to Apps & Notifications > Chrome > Storage > Clear Cache.

This is much less drastic than performing a system reset, which is the other surefire way to get rid of an Android virus, and possible via the Settings > System > Reset Options > Erase All Data menu.

Method 2: Boot into safe mode

Android antivirus apps such as Bitdefender Mobile Security are a good idea as they can prevent apps laced with malware from making it onto your phone in the first place. There are other options, too, and we've rounded up some of our favourites. They can also detect and remove a virus if you install such as app if your phone is already infected.

But if you know when all the trouble began you can manually remove the malicious app. You'll almost definitely need to enter Safe mode first, because this stops any third-party apps from running. Try to remove an infected app in normal mode and you'll likely be denied permission.

If you don't have an option to access Safe mode in your phone's Power options menu, try holding volume-down as you reboot the phone. You'll know it's worked if you see Safe mode in the bottom left corner of the screen. If not, Google your phone make and model along with safe mode to get specific instructions.

Open Settings and select the Apps & Notifications menu, then scroll down the list and be on the lookout for any suspicious apps that could be behind all the drama - anything you don't remember downloading or that doesn't sound like a genuine Android service. Click the app's name to open its dedicated App Info page.

If this is not a preinstalled app you should see an Uninstall button at the top of this page. Press this if you can. If it's greyed out then it's likely the app has given itself administrator rights, which you can disable in Settings > Security & Location > Device Admin Apps.

With the virus now off your Android phone or tablet, all you need to is restart the device to take it out of Safe mode.

Supposing you've done all the above and your device is still slow, consider that it may be a case of old age or a new software update that doesn't play nicely slowing things down. Also read on below for how to avoid becoming a victim to Android malware once again.

Avoid future Android viruses and malware

- **Don't install apps from outside Google Play unless you know what you're doing:** This functionality should be disabled by default, but do check. In recent versions of Android the ability to install apps from unknown locations has changed from a system-wide permission to an app-specific permission. It's now found in Apps & Notifications > Advanced > Special App Access > Install unknown apps. If you do install an app outside Google Play, such as from another app store or an APK file that came as an attachment on an email or other message, be absolutely certain that it is above board and comes from a legitimate source
- **Avoid cloned apps:** 99 percent of the time you will be safe downloading apps from Google Play, but malicious code has been found within apps there. Avoid downloading what appear to be cloned apps from unknown developers, or apps that simply don't do what they say they do
- **Check app permissions:** No matter from where you are installing an app, check its required permissions before hitting Install. Never allow an app device admin permission, which prevents it being deleted. And does a video player really need to see your contacts? You can also check reviews online and browse the developer's website to see whether it's a genuine operation or cowboy business
- **Keep Android up to date:** The latest version of the Android operating system won't necessarily be available for your phone or tablet, but you should check that it is as up to

date as it can be. Next time you upgrade, consider a brand that is known for its timely operating system updates.

- **Install an antivirus app:** You don't need to install antivirus on Android, but it can give you peace of mind if you're concerned about viruses, and the apps often have other useful functionality too. Be warned that Android antivirus is known to occasionally report false-positives, but if you know an app is okay you know an app is okay. Our favourite antivirus option for Android is Bitdefender, but there's also plenty of other options for mobile security software.