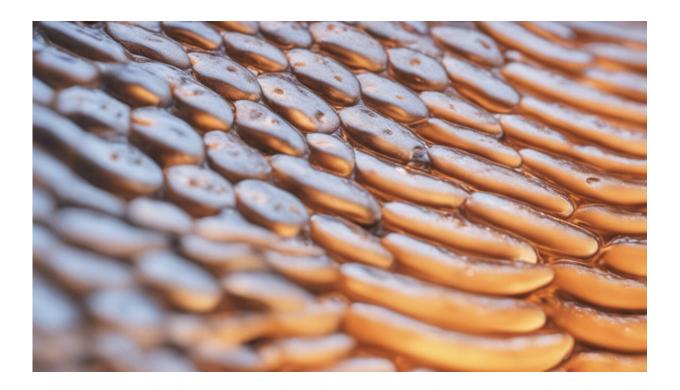# Can your mobile phone get a virus? Yes, and you'll have to look carefully to see the signs

April 28 2022, by Ritesh Chugh

Credit: AI-generated image (disclaimer)

With nearly [84%](84%) of the world's population now owning a smartphone, and our dependence on them growing all the time, these devices have become an attractive avenue for scammers.

Last year, cyber security company Kaspersky detected nearly 3.5 million

[malicious attacks](#) on [mobile phone users](#). The spam messages we get on our phones via [text message](#) or email will often contain links to viruses, which are a type of malicious software ([malware](#)).

There's a decent chance that at some point you've installed [malware](#) that infected your phone and worked (without you noticing) in the background. According to a global report commissioned by private company Zimperium, more than [one-fifth](#) of mobile devices have encountered malware. And four in ten mobiles worldwide are [vulnerable](#) to cyber attacks.

But how do you know if your phone has been targeted? And what can you do?

How does a phone get infected?

Like personal computers, phones can be compromised by malware.

For example, the Hummingbad virus infected [ten million](#) Android devices within a few months of its creation in 2016, and put as many as [85 million](#) devices at risk.

Typically, a phone virus works the same way as a computer virus: a malicious code infects your device, replicates itself and spreads to other devices by auto-messaging others in your contact list or auto-forwarding itself as an email.

A virus can limit your phone's functionality, send your [personal information](#) to hackers, send your contacts spam messages linking to malware, and even allow the virus's operator to "spy" on you by capturing your screen and keyboard inputs, and tracking your geographical location.

In Australia, Scamwatch received [16,000 reports](#) of the Flubot virus over just eight weeks in 2021. This [virus](#) sends text messages to Android and iPhone users with links to malware. Clicking on the links can lead to a malicious app being downloaded on your phone, giving scammers access to your personal information.

Flubot scammers regularly change their [target countries](#). According to cyber security firm Bitdefender, FluBot operators targeted Australia, Germany, Poland, Spain, Austria and other European countries between December 1 2021 and January 2 of this year.

Is either Apple or Android more secure?

While Apple devices are generally considered more secure than Android, and [less prone](#) to virus attacks, iPhone users who "jailbreak" or modify their phone open themselves up to security vulnerabilities.

Similarly, Android users who install apps from outside the Google Play store increase their risk of installing malware. It's recommended all phone users stay on guard, as both Apple and Android are [vulnerable](#) to security risks.

That said, phones are generally better protected against viruses than personal computers. This is because software is usually installed through authorized app stores that vet each app (although some malicious apps can occasionally slip through [the cracks](#)).

Also, in comparison to computers, phones are more secure as the apps are usually "[sandboxed](#)" in their own isolated environment—unable to access or interfere with other apps. This reduces the risk of infection or cross contamination from malware. However, no device is entirely immune.

Watch out for the signs

While it's not always easy to tell whether your phone is infected, it will exhibit some abnormal behaviors if it is. Some signs to watch out for include:

- poor performance, such as apps taking longer than usual to open, or crashing randomly
- excessive battery drain (due to the malware constantly working in the background)
- increased mobile data consumption
- unexplained billing charges (which may include increased data usage charges as a result of the malware chewing up your data)
- unusual pop-ups, and
- the device overheating unexpectedly.

If you do suspect a virus has infected your device, there are some steps you can take. First, to prevent further damage you'll need to remove the malware. Here are some simple troubleshooting steps:

1. Use a reliable antivirus app to scan your phone for infections. Some reputable vendors offering paid and free protection services include Avast, AVG, Bitdefender, McAfee or Norton.
2. Clear your phone's storage and cache (in Android devices), or browsing history and website data (in Apple devices).
3. Restart your iPhone, or restart your Android phone to go into safe mode—which is a feature on Android that prevents third-party apps from operating for as long as it's enabled.
4. Delete any suspicious or unfamiliar apps from your downloaded apps list and, if you're an Android user, turn safe mode off once the apps are deleted.

As a last resort, you can back up all your data and perform a factory

reset on your phone. Resetting a phone to its original settings will eliminate any malware.

Protecting your phone from infection

Now you've fixed your phone, it's important to safeguard it against future viruses and other security risks. The mobile security apps mentioned above will help with this. But you can also:

- avoid clicking unusual pop-ups, or links in unusual text messages, social media posts or emails
- only install apps from authorized app stores, such as Google Play or Apple's App Store
- avoid jailbreaking or modifying your phone
- check app permissions before installing, so you're aware of what the app will access (rather than blindly trusting it)
- back up your data regularly, and
- keep your phone software updated to the latest version (which will have the latest security patches).

Continually monitor your phone for suspicious activity and trust your gut instincts. If something sounds too good to be true, it probably is.

This article is republished from The Conversation under a Creative Commons license. Read the original article.

Provided by The Conversation