Can iPhones Get Viruses? A Guide to iPhone Virus Removal and Protection

With the number of reliable functionalities that Apple has instilled in its iPhones over the years, is it any wonder that many owners of these devices use them for all manner of things in their lives: work, photos, videos, gaming, to name a few? However, with such exposure to every facet of the digital world comes the eventual risk of infection from a virus. And although research may suggest that iPhones are less vulnerable to cyberattacks than Android phones in general (in part because of Apple's largely closed ecosystem for its developers), it doesn't mean that your iPhone is 100% safe from infiltration by a cybersecurity threat.

So, if your iPhone has been behaving strangely or is loading everything more slowly than usual, you might need to check it for a virus. Fortunately, we've written this guide explaining how iPhones get viruses, how to spot if your iPhone has been infected, how to remove them from your iPhone, and how to protect your iPhone using antivirus software in the future.

Can iPhones Get Viruses?

Fortunately for Apple fans, iPhone viruses are extremely rare, but not unheard of; over the past few years, some iPhone users have been able to recall the effects of Pegasus (a form of spyware spread through text messages) or AdThief (a form of adware that served unwanted advertisements from a pirate network). Whilst generally secure if you stay within Apple's operating parameters, one of the main ways iPhones have become more vulnerable to viruses is through the practice of "jailbreaking" or purchasing a "jailbroken" iPhone. Jailbreaking an iPhone is a bit like unlocking it (but less legitimate). It involves obtaining root privileges that bypass the security restrictions, which normally limit the operation of software on the device. Apple takes issue with jailbreaking its devices and tries to patch vulnerabilities in its iPhones that allow it to happen through its updates.

The backstreet practice of jailbreaking iPhones gives users more control of the operating system on the phone. For example, it gives users the ability to customize how the system looks, delete pre-installed apps, and download apps from places other than the App Store. Although this may sound appealing to some extent, opening your iPhone up to unverified applications essentially gives hackers the opportunity to place multiple backdoors in your system through malicious and pirated apps. So, in short, while the answer to the question "Can iPhones get viruses?" is "generally not", iPhones have been known to get viruses, especially when they are jailbroken.

Why are iPhone Viruses So Rare?

There are a number of reasons iPhones are less likely to get viruses (some are mentioned above). However, the best way to understand why iPhone viruses are so rare and what Apple does differently is to understand what a virus is and how it works.

Viruses are malicious bits of computer code that replicate themselves. They spread throughout a system and may damage, delete, or steal your data. In order to spread, a computer virus needs to be able to communicate with various programs that make up a system. However, the Apple operating system that iPhones use makes this process more difficult. This is because Apple's operating system is designed so that each app runs in its own separate virtual space. Essentially, the interactions between apps are restricted, making it hard for a virus to spread from application to application.

Added to this is the fact that all applications that Apple users download to their iPhones have to be downloaded from the official App Store. Apple has a very strict vetting process for all the applications that sit in its App Store, which means it's incredibly unlikely for any malware-infected apps to end up available for download in the first place.

Does your iPhone have a Virus and How to Check?

Although iPhones are less susceptible to viruses, it's wise to ask yourself some simple safety questions:

Is your device jailbroken? As discussed above, if your iPhone has been jailbroken (especially with a popular open-source program like "JailbreakMe"), it is more vulnerable to viruses. If you've bought your device second-hand, look for jailbreaking apps on the phone or seek help from an official Apple representative if you're concerned.

Have you spotted apps you don't recognize? Unfamiliar apps may be a sign of malware on your device. We recommend keeping a list of all the applications you download and uninstalling any apps that you do not recognize or seem suspicious.

Are your applications repeatedly crashing? If your applications are crashing consistently and for no clear reason, it may mean your phone is infected with some form of malware.

Has your data usage gone up? Increased data usage that is not explained by you using your phone differently may be caused by malware. We recommend keeping a close eye on your data usage with Apple's own pre-downloaded monitoring apps.

Have you got any unexpected charges on your online accounts? Some types of malware can send messages to premium services or hijack your shopping applications. So, if you have an unexpectedly large bill on any of your online accounts, a virus may be the reason.

Are you seeing pop-ups when your browser is closed? This should not happen if all is well with your iPhone's system. Pop-ups that appear when your browser is closed are a sure sign of a virus.

Is your battery draining quickly? Some energy-intensive malware (like mining software or adware) can drain your battery more quickly than usual. If you keep running out of charge unexplainably, your phone may be infected with a virus.

Is your phone overheating? In some cases, your phone may heat up more than usual from background malware and pirated applications using your phone's resources. So, be aware that overheating can be a sign of malware activity as well.

Since viruses are rare on iPhones, it's also important to consider what other parts of the device might be causing your system to behave strangely. In general, there are 3 things to look out for:

- There's a "buggy" or malfunctioning application which needs updating or deleting. If you think you know which app is causing your system to slow down, you can either search for updates for the app or simply delete it. Otherwise, you may have to roll back your system (if you have backups) to a time when your system was fully functioning.
- Often, iPhones stop functioning normally when the phone is running out of memory space. We recommend regularly offloading your data to an external device to keep your iPhone running smoothly.
- In some cases, your iPhone's functionality can be reduced because your battery needs replacing. However, a battery that drains fast is also a sign of a virus, so you may need to seek external help if you want to determine the exact nature of the problem.

How to Get Rid of a Virus From an iPhone

If you're sure that your iPhone is infected with a virus, here's how to clear it from your iPhone manually:

Update your iOS: If the virus is known to Apple's development team, updating your iOS to the latest version (which contains the relevant patch) may solve the problem. **Settings** > **General** > **Software Update** and tap **Download and Install**.

Delete apps that look suspicious: Delete any apps you do not recognize or that you downloaded around the time the problem started.

Clear your data and history: Go to **Settings** and then click on **Safari**. From there, tap **Clear History and Website Data**.

Power off and restart: Hold down the power button and slide to turn off. Then hold down again to restart. This may fix the problem. If the problem remains after these measures, try the next two options (be aware, you may lose some of your recent data).

Restore your phone from a previous backup: Try earlier backup versions (if you have activated this feature) and keep trying them until you find one that does not have the problem/is malware free.

Restore factory settings: If all else fails, return your phone to factory settings, but make sure you back up your important files first (providing they are not infected). To do this, go to **Settings** > **General** > **Reset** > **Erase All Content and Settings** and select **Erase Now**.

How to Protect Your iPhone from Viruses

So, now you know how iPhones can get viruses and how to manually remove them, it's important to learn how you can prevent your iPhone from being infected by viruses and other malware in the future.

Antivirus Software - Purchasing good antivirus software is one of the simplest ways to keep your iPhone safe. We recommend protecting your phone with Kaspersky Premium. Our software provides vital security enhancements, notifications about relevant security incidents, and a tool that checks for "weak" system settings.

Only download apps from the App Store: As we previously mentioned, Apple has a thorough vetting process on its application store. Downloading apps from the App Store means they are highly unlikely to contain malware.

Check the developer descriptions on the App Store: Generally, it is always wise to read about who developed the app that you are about to download in the description. You can also further research the company online to check its credentials.

Read app user reviews: Always read app reviews from other users, as they tend to be the quickest way of discovering a bad application. Remember, real reviews normally raise both good and bad points about products.

Check out the number of app downloads: A great rule of thumb on app store applications is to check the number of downloads your chosen app has had. Apps with millions of downloads are less likely to be malware.

Check permissions requested by the app: What permissions is the app requesting? Do they seem reasonable? If what is being asked for sounds suspicious, avoid downloading the app or remove it if you've already installed it.

Do not click on unverified links: Mark all spam emails as junk and avoid opening them. If you accidentally open a spam email, make sure you don't click on the links it contains.

Keep the iPhone's operating system (iOS) updated: Update your operating system regularly. This ensures your phone is protected by the latest security updates that Apple has to offer.

Keep your applications updated: Update all of your apps regularly where possible. This will reduce the possibility of criminals exploiting vulnerabilities in third-party apps that could compromise your security.

Be mindful of using free Wi-Fi: Avoid online shopping and banking on public networks because they are the ideal vectors for cybercriminals. If you must use free Wi-Fi, try using a VPN connection like Kaspersky VPN Secure Connection. This protects your connection by encrypting your data via a digital tunnel.