5 ways to tell if your Mac is infected with a virus.

Is your Mac behaving strangely? Whether you're seeing ads you can't explain or your system is unusually slow, you might assume the problem is malware. And you could be right in this case.

Is your Mac behaving strangely? Whether you're seeing ads you can't explain or your system is unusually slow, you might assume the problem is malware . And you could be right in this case.

Back in 2009, many people wondered whether Macs needed virus scans. The general consensus at the time was "no," but Macs have become so popular since then—and therefore, it's not surprising that malware infects them.

The number of Macs infected with viruses and malware is increasing, and if you notice any of the following symptoms on your computer, consider the possibility that it has been infected.

What is Mac Malware?

There have been cases of Macs being infected with viruses. Here are some examples:

1. Wirelurker is transmitted via pirated software. It will infect any iPhone or iPad plugged into infected Macs, spreading from one platform to another and collecting unique device IDs in the process. No one is sure what the goal of this malware is.
2. iWorm infects users who download pirated software from The Pirate Bay. Macs infected with iWorm become part of a global botnet .
3. CoinThief infects users by impersonating legitimate software and stealing any Bitcoin stored on the infected Mac.

Lessons from these examples

All malware has one thing in common: they infect Macs through software installed outside the Mac App Store. In some cases, pirated software is the primary cause of the problem. In other cases, the cause is software from unreliable sources.

Simply put: if you never install software outside of the Mac App Store, you have nothing to worry about. There will certainly be some browser-related exploits from time to time, and Java is also a concern, but if your OS X and browsers are updated, virus infections like the one above are highly unlikely.

And if you install software outside of the Mac App Store, be sure to carefully review it before installing (search on Google for the official download), and you'll have nothing to worry about.

On the other hand, if you use pirated software or install plugins as required by websites that provide pirated movies, you may encounter problems. Here are a few signs that your computer may be infected with a virus :

Symptom 1: Unwanted ads and pop-ups

Adware is becoming a bigger problem than ever on the Mac platform. If you're seeing ads in places where they didn't appear before, chances are you've installed something problematic. This is especially true if you're getting pop-up ads even when you're not browsing the web.

Symptom 2: Your Mac is slow for no reason.

As mentioned above: some malware on Macs turns your Mac into a botnet, a global network of computers used for all sorts of purposes. If your Mac is infected, it can help launch denial-of-service (DDoS) attacks on a website, mine Bitcoin, or secretly use your CPU for similar purposes.

1. 6 ways to fight botnets

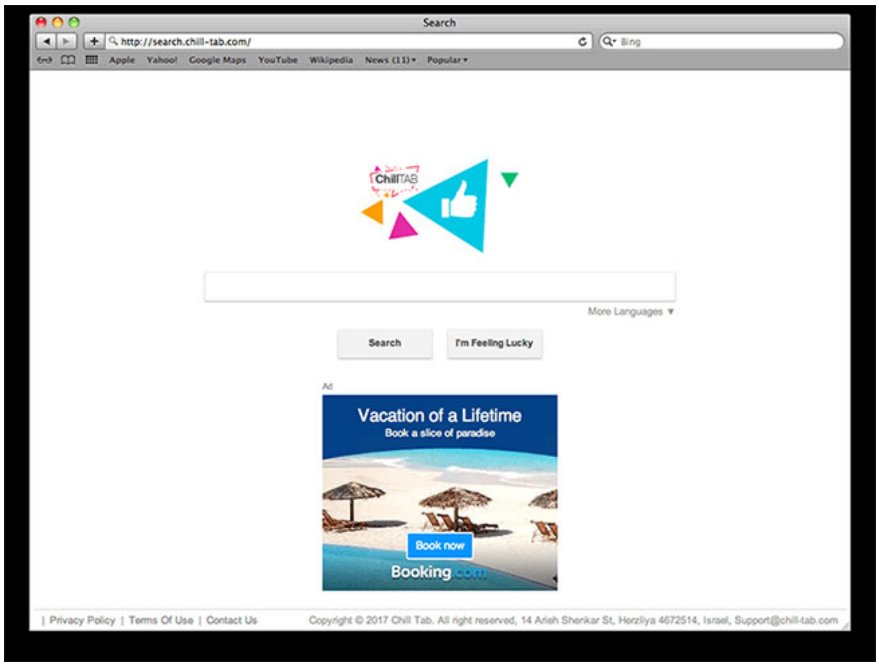
If your Mac is consistently slow, even when you don't have any programs open, this could be a possibility.

However, it's highly likely that malware isn't the cause of your Mac's slowness. You should read our article on how to speed up your Mac . If none of the methods in that article improve the situation, then you should consider the possibility that your Mac is infected with a virus.

Symptom 3: The browser is redirected to unwanted websites.

This is a warning sign that your Mac has been infected with browser hijacker malware. This type of malware, once granted sufficient privileges, modifies system settings and alters how your default web browser works. Typically, a hijacker is an aggressive plugin that replaces custom internet browsing configurations with fake values ??without administrator approval.

Following these changes, your preferred browser—perhaps Safari, Chrome, or Firefox—begins forwarding traffic to spam websites randomly or every time you launch it.

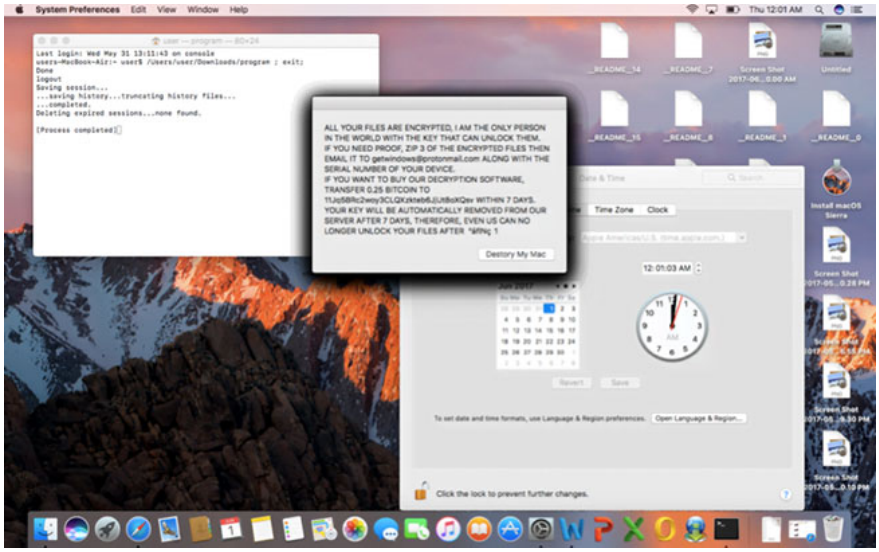


Most landing pages are clones of conventional search engines, lacking built-in information lookup features and instead returning results hosted by third-party providers. The goal of most browser viruses is to intercept a user's traffic and exploit it to display ads on these search results pages.

Essentially, this is a money-making tactic done in a malicious way. Sometimes you might end up on fake warning pages saying your Mac is infected with a virus – another way to advertise scare-inducing software. Virus redirection also tends to spread through bundles, where users are unaware of the extras being installed alongside what appears to be some convenient free application.

Sign 4: Personal files are encrypted and inaccessible.

Unlike Windows, this isn't a common occurrence for Macintosh computers, but the ransomware threat shouldn't be underestimated . There have been several ransomware outbreaks specifically targeting Macs. Notable examples are the MacRansom and KeRanger campaigns. Both are ransomware Trojans that encrypt victims' personal data and provide ransom notes demanding decryption. These Trojans can also add an extra extension to the hostage files, such as the *.encrypto* string , which is a clear sign of an attack.

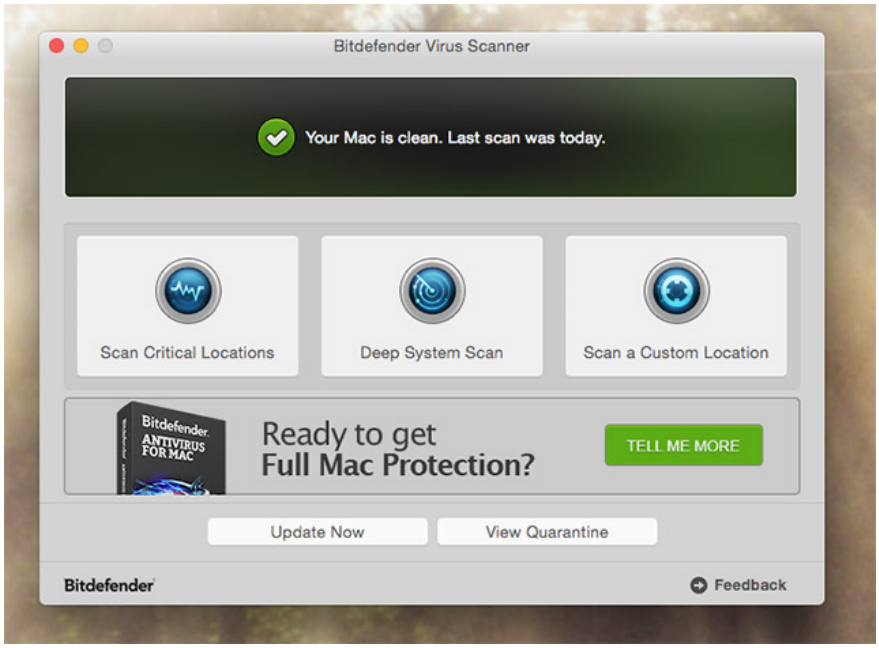


Browser Lockout is a specific type of ransomware targeting Macs, with a much milder negative impact. It only affects Safari, causing it to display a fake ransom warning claiming to be from the FBI or other law enforcement agency. The lock screen typically states that some prohibited documents have been found on the computer and demands the victim pay a fine to avoid legal action. Fortunately, the fix is ??simple – all you need to do is clear your browser's cache .

Sign 5: Malware scanning software confirms your Mac is infected with a virus.

Do you think your Mac might be infected with a virus? To be sure, use software to scan it. Here are a few free programs you can use to scan your Mac and find out about any virus issues:

1. BitDefender Virus Scanner for Mac is a free tool. It won't remove malware for you, but it will show you where to remove it using Finder.
2. AdwareMedic scans and removes several common adware programs on Macs. It's a quick scan, so give it a try if you're seeing too many ads. You'll receive a donation request. Please donate if this program is helpful to you.
3. ClamXAV is the Mac version of ClamAV, a popular open-source malware detection tool. This software is also worth considering.

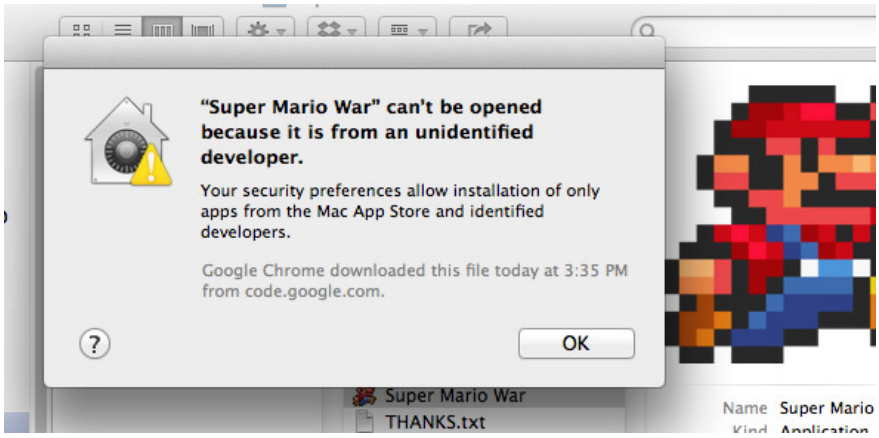


If none of these tools show anything unusual, then your Mac is not infected with a virus. Or, for peace of mind, you can try these 9 best antivirus software for Mac .

What kind of security features does a Mac have?

Your Mac has built-in protection to keep it safe from malware, although implementing all such measures isn't entirely easy. Here are a few reasons why you don't need to worry too much:

1. **Gatekeeper:** Helps protect your Mac, preventing users from installing unsafe software. By default, this means anything not from the Mac App Store can be configured to block, especially apps from unknown developers. Of course, many Mac users disable Gatekeeper entirely so they can run any software they like, including things they've built themselves. Hopefully, all users will research the applications they run before installing them.
2. **Sandboxing:** Applications installed through the Mac App Store have very limited access to the larger system, a limitation designed to prevent one application from disrupting the entire system.
3. **XProtect:** Officially known as File Quarentine, is an anti-malware program you might not know you have. Part of OS X since 2009, unlike typical Windows antivirus software, it's completely invisible to most users. You can't open the program and scan yourself, and you can't manually install updates. But if you are infected, it will notify you. It also prevents you from opening infected files.
4. **Obscurity** is another advantage of Macs. Macs have a growing market share today, but for a long time there were very few active computers running OS X on the network, so malware creators didn't bother targeting them. This is known as "Security Through Obscurity" (STO). Of course, today, with the growing Mac user base, STO is no longer an advantage for macOS users – however, Windows remains a primary target for malware producers.



Your computer isn't infected with a virus, but you still want to be notified if one appears in the future? If you want to be notified about malware on your Mac, this article recommends using TheSafeMac.com. Consider signing up if you want to be notified.

Remove viruses or malware from your Mac.

Many Mac users believe they are immune to viruses, spyware, worms, or other malware. This is not true, although fewer viruses and malware target Macs than Windows laptops and PCs. Some well-known examples of malware for Mac computers include:

1. MacDefender
2. MacProtector
3. MacSecurity

These names sound like antivirus products, but they are actually malicious and designed to trick Mac users into sending their credit card details or Apple ID account information. Don't download them!

The two main risks Mac users face are false alarms and pre-installed malware. If you see any kind of message while browsing the internet that says "an issue has been detected with your Mac," it's very likely an attempt to trick you into downloading malware. Instead, make the following tips a part of your daily Mac usage routine.

Ignore notifications

If you have downloaded anything from the website, exit Safari (or whatever browser you are using), go to your **Downloads** folder , and drag any items from there to **the Trash.** Then empty **the Trash.** Avoid accessing the website again as it may have been hacked.

Exit the infected application.

If you suspect malware has been installed on your Mac—especially if you see pop-up messages asking for your Apple ID or credit card details—quit the application or disable the software that you think may have been infected.

Open **Activity Monitor** and find the application in question, or search for malware from the list of names above. Once you've identified the malware, click the **Quit Process button,** then exit **Activity Monitor .** Next, go to the **Applications** folder and drag the unwanted software to **the Trash** and empty **the Trash.**

Update software and applications.

Finally, make sure all your software and applications are up-to-date. Also, ensure your Mac is running the latest operating system and that you've installed all updates directly from Apple.

Just like with Windows PCs, you should equip your Mac with robust protection. Check out: 9 best antivirus software for Mac to find the right option for you!

See more:

1. Completely remove malware from your Windows 10 computer.
2. 9 things to do when you discover your computer is infected with malware.
3. What should you do if your computer gets infected with a virus?