5 ways malware can easily infect a Mac

There are actual Mac security threats and many problems resulting from user behavior. Here are some dangerous practices that can infect malware on a Mac.

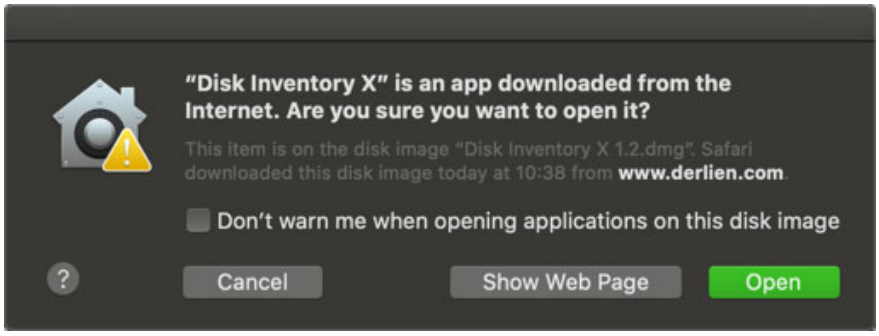
Most Mac users don't have to worry about security too much. Because the majority of malware targeting Windows and macOS does a good job of keeping users safe, users are easily complacent.

However, there are actual Mac security threats and many problems resulting from user behavior. Here are some dangerous practices that can infect malware on a Mac.

Things that make your Mac more vulnerable to malware

1. 1. Download dangerous software or violate copyright
2. 2. Skip the application updates and macOS
3. 3. Run Flash Player and Java
    1. Uninstalling Flash Player on Mac
    2. How to remove Java from Mac
4. 4. Disable the integrated protection feature of Mac
5. 5. Ignore basic danger signs

1. Download dangerous software or violate copyright



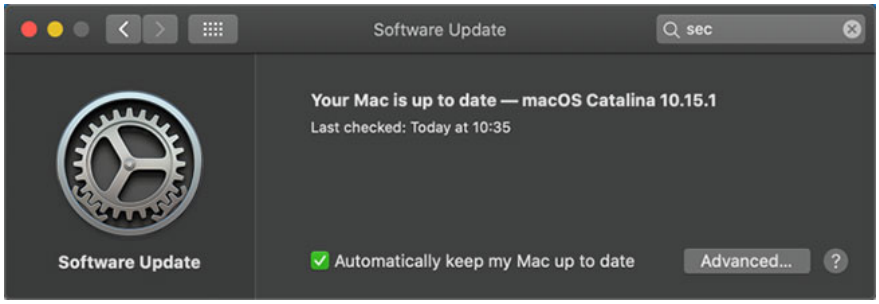
The easiest way to mess up the system is to install unintended randomized Mac apps on the web.

In many cases, pirated software distributors are only interested in providing paid tools at no cost. However, you can never fully trust the cracked software, as there is no guarantee that someone will not add malware in the process. Indeed, historically, many examples of macOS malware have appeared in pirated software.

The safest place to install Mac apps is the Mac App Store and directly from trusted developers. By default, the Gatekeeper feature of macOS will only allow you to run applications from authorized developers and display a warning if you try to run an untrusted application.

Usually, a legitimate developer may not be able to afford to register with Apple. You can ignore this warning when it's displayed, but it's important to make sure that you truly trust the application when doing so.

2. Skip the application updates and macOS



Everyone gets tired of seeing a prompt for Mac or software updates. But leaving the system out of date makes you much more vulnerable.

Typically, macOS system updates fix known vulnerabilities to keep users safe. If you keep running an outdated version for months, you could be the victim of an attack that Apple has patched long ago. Keeping your system running the latest operating system version is extremely important.

The same is true of desktop applications, especially the browser. Historically, there have been cases of common Mac applications being infected with malware, such as BitTorrent client Transmission in 2016. Users installed the application on the system, but never minded. updating, may become 'prey' for the attacker.

Thankfully, macOS makes it easy for users to update applications and systems. On macOS Mojave and newer, open the **App Store** and check the **Updates** tab to download new versions of the App Store app. You will find macOS software updates in **System Preferences> Software Update** .

For applications downloaded from other sources, you will need to open them and check for updates manually. You will often find the **Check for updates option** in the **Help** menu or the application menu. Or maybe, you'll find it in the apps menu on the **About [app's name] page** .

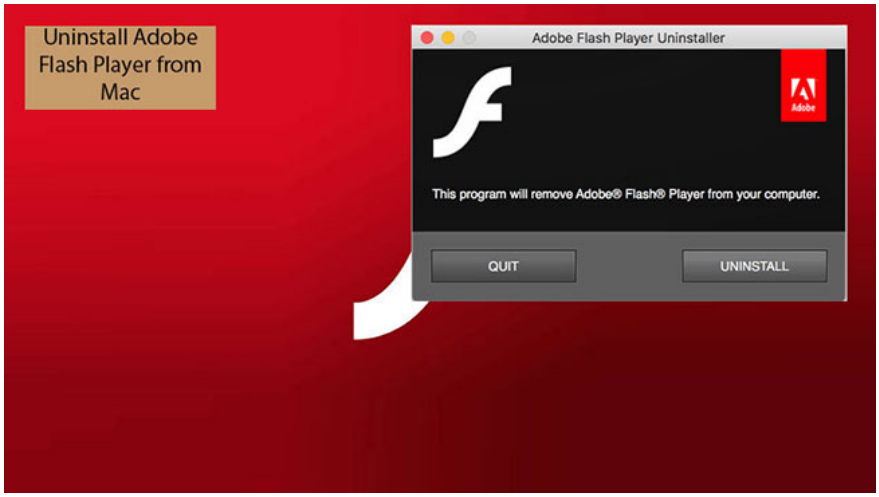
3. Run Flash Player and Java

In the old days, browser plugins like Flash Player and Java were essential parts of the web, as they allowed you to enjoy multimedia content on all types of websites. However, with the current web, they are no longer popular and almost no one needs to use anymore.

Very few websites require Java or Flash at the moment. Adobe plans to kill Flash by the end of 2020, and nearly all browsers have blocked Java for years. So it is unlikely that you will be attacked in this way, but checking if you use these plugins and removing them if any is still a wise action.

To check, open **System Preferences** in the Apple menu. If you see an item for Flash Player or Java, you have already installed it.

Uninstalling Flash Player on Mac



Remove Flash Player by visiting Adobe's Mac Flash Player uninstall page at:

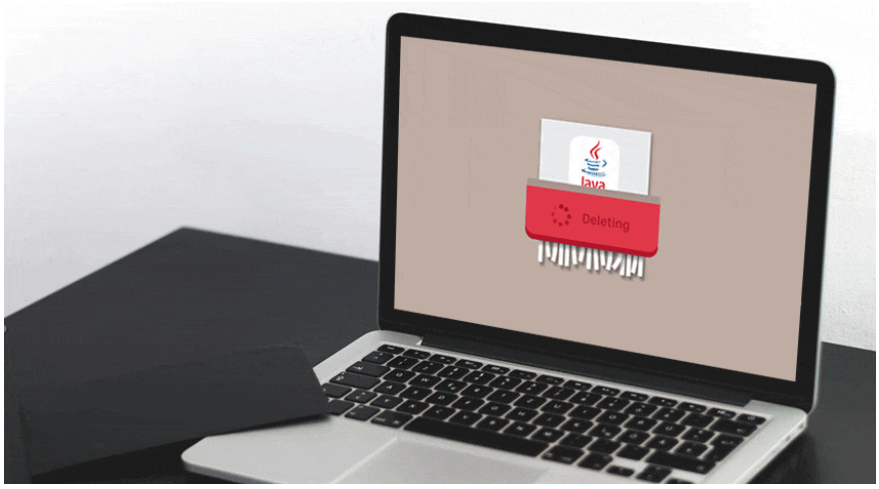
`https://helpx.adobe.com/flash-player/kb/uninstall-flash-player-mac-os.html#OS_X_`

Under the heading **Download the Adobe Flash Player uninstaller** , click the **Download button** next to Mac OS X, version 10.6 or later. Run the tool and it will delete Flash Player.

To complete the uninstallation, you should also delete the following files from your user directory:

`[USER]/Library/Preferences/Macromedia/Flash Player [USER]/Library/Caches/Adobe/F`

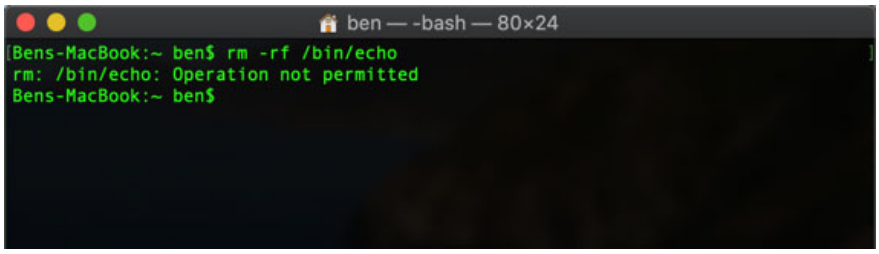
How to remove Java from Mac



Removing Java from macOS is a bit more complicated than installing it. First, press `Cmd` + `Space` to launch Spotlight search and open Terminal. Once the Terminal window is open, paste each of the commands below and press `Enter` to run them:

```
sudo rm -fr /Library/internet Plug-Ins/JavaAppletPlugin.plugin sudo rm -fr /Libra
```

4. Disable the integrated protection feature of Mac



As mentioned earlier, macOS has several built-in protection layers. One of these is System Integrity Protection (SIP), introduced with OS X El Capitan.

Basically, SIP prevents users and programs from making changes to the core of the operating system.

The addition of SIP prevented many deep system tweaks on the Mac. Therefore, you can find ways to disable SIP so that you can use these old tools again. While this can be disabled, doing so is a bad idea, because disabling SIP significantly reduces the security capabilities of the system.

1. Why shouldn't you disable the System Integrity Protection feature on Mac?

Without a barrier to protected operating system files, malware can invade and sabotage them. There are certain troubleshooting situations that you need to turn off SIP for a short time, but you must always turn it back on immediately to minimize the risk to your system.

In the case of Gatekeeper, the feature that prevents unauthorized applications from running on the system is similar. As mentioned, macOS only allows installation of applications from the App Store or from specified

developers. You can enable the **Anywhere** option with Terminal, but this is not a good idea.

5. Ignore basic danger signs

Just because you use a Mac doesn't mean you should skip basic security practices. While it is difficult to detect something that is problematic on a Mac, you should keep an eye out for common online attacks.

Do not click links or attachments in emails unless you are sure you trust them. And avoid clicking on fake links or pop-ups that prompt you to install updates.

You should also know how to identify malware on a Mac. If you think you might have done something to make your Mac vulnerable, scan for malware with a tool like Malwarebytes for Mac.

It is good to be aware of common security vulnerabilities such as Meltdown and Specter or KRACK WiFi exploit. While these not only affect macOS, they still make Mac users vulnerable to attack in other ways.

As you can see, most Mac users hope to never encounter a malware attack. The biggest threats to your system come from third party software, so it's important to check what is authorized to run on a Mac. A bit of proactive thinking will help keep your system safe in the long run.