How secure is a Mac and are Macs really more secure than Windows?

Macs are safer than PCs, but how much more secure are Macs, and what should you do to protect yourself? We run all the ways Apple keeps you safe.

By Karen Haslam Managing Editor, Macworld MAR 27, 2025 4:01 am PDT

While it's true that Macs are less likely to be attacked on the basis that there are fewer Macs than PCs, Mac users can be a very lucrative target and hence considered worth the effort. As a result Macs can get targeted by malware and viruses.

Indeed, even Apple's software chief Craig Federighi said (in the 2021 trial between Apple and Epic) that: "Today, we have a level of malware on the Mac that we don't find acceptable." While his motive was to point out that there is a benefit to forcing iPhone and iPad users to only install apps via the iOS App Store, the point is that even Apple staff admit there are Mac viruses. (Here's What to do if you think your Mac has a virus.)

Macs are generally safer than PCs though. This is partly because the Mac operating system is Unix-based and therefore more difficult to exploit, it's also because Apple has such tight control over the hardware and software, and Macs are safer due to the various protections and security measures built into the Mac and the Mac operating system that makes Macs more difficult to exploit.

But that doesn't mean you should believe your Mac impenetrable. Macs have been targeted by hackers and viruses and over the years Apple has had to get serious about the measures included in macOS to keep its users safe.

In this article we will run through the various ways Apple keeps your Mac secure, and the things you can do to stay safe. For more advice about how to keep your Mac secure read our Mac security tips.

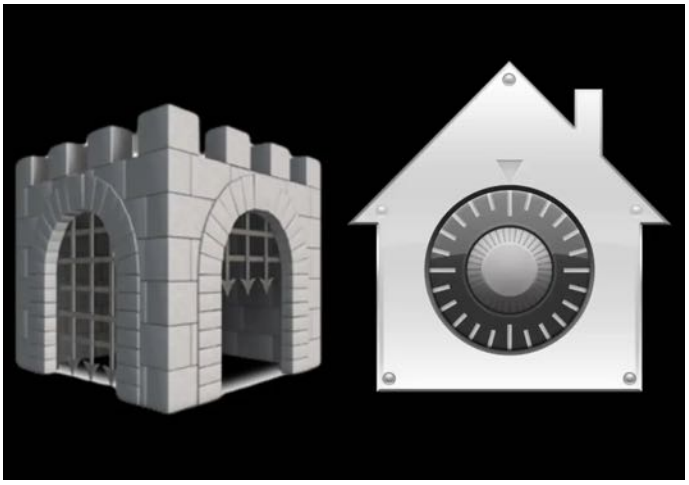
Another thing to note is that the M-series chips that Apple started using in November 2020 are considered more secure than Intel processors. However, malware known as Silver Sparrow was found on the M1 Mac shortly after launch.

How Apple protects your Mac

There are various ways that Apple protects your Mac from malware and viruses as you will see if you read on. There are, of course, other things you can do to supplement these measures, such as running an antivirus software or using a VPN to encrypt your traffic. We have separate advice about the best antivirus for Mac and best VPN. You must also be cautious and not open mysterious emails or click on questionable links– you might be sure you wouldn't do that, but could you be so sure that your parents wouldn't?

Luckily there are protections baked into a Mac that should mean that even the least tech-savvy people are protected. We'll outline them below.

Apple antivirus



Gatekeeper and XProtect are one of the barriers that malware has to cross to get onto your Mac

On the software side, macOS includes its own antivirus software built in. XProtect detects and blocks any known malware. Apple monitors for new malware infections and updates XProtect regularly. XProtect will check for malware when an app is first launched and if it has been changed. If XProtect detects malware it will block the software and remove it.

In addition to the protection offered by XProtect is Gatekeeper. Gatekeeper is a feature of macOS that is designed to stop users from installing malware in the first place. Gatekeeper checks that any app you download from the internet has been verified by Apple and checked for malicious code. If the app is considered a risk Gatekeeper will stop you from installing it. For more advice about downloading and installing apps read: How to install apps on the Mac

Explore frequently asked questions

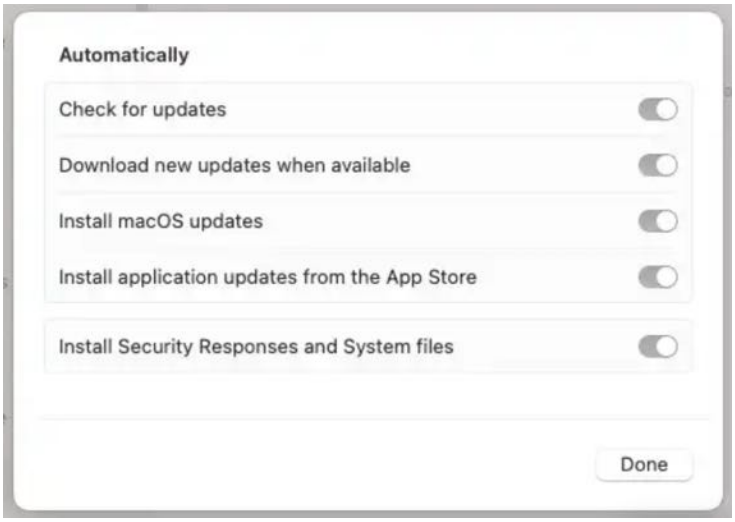
Gatekeeper isn't infallible, it has been bypassed in the past, and XProtect isn't always right up to date, so malware has slipped through. But both offer a level of protection that should give you peace of mind.

If you want an extra layer of protection our top recommendation in our best antivirus for Mac round-up is Intego Mac Internet Security.

Software and security updates

Apple ensures that security updates are pushed out to Macs regularly – so it is important to keep your Mac software up to date. However, only the past three versions of macOS are supported with security updates. In spring 2025, Apple only supports macOS Sequoia, macOS Sonoma and macOS Ventura with security updates. this will change in September, when the launch of the next version of macOS will mean that Ventura loses it's support.

This means that the oldest Macs supported right now are from 2017, and in some cases, 2018–and come September 2025, when Apple updates macOS, those Macs will no longer be supported. This means that if your Mac dates from 2018 it may not be safe to use in the near future.



Your Mac can automatically check for updates and even install security updates without you needing to do anything
Foundry

Apple makes this easy by making it possible for your Mac to update automatically, so you don't need to do anything. To set your Mac to check for updates and update software automatically follow these steps:

1. Open **System Settings**.
2. Click **General**.
3. Click **Software Update**.
4. Make sure that **Automatic Updates** are On.
5. To ensure that background updates are applied as soon as they are issued by Apple Install Security Responses and System Files should also be selected (click on the i to see these options).

This should mean that the software is downloaded to your Mac when issued by Apple.

You will still need to restart your Mac to install a normal software update update, however, some security updates can be pushed to your Mac by Apple and installed as background updates without requiring you to restart.

Rapid Security Responses take this a step further and will speed up the delivery of security fixes on iPhone, iPad, and Mac. Apple introduced this feature in macOS

Ventura 13.2 (and iOS 16.3). Now, when you restart a Mac, any Rapid Security Responses will be instantly applied. Approaching security updates in this way means Apple can issue them faster without them being part of a wider update.

App protections

If you want to be confident that every app you install is safe, it is wise to stick to apps on the Mac App Store. Every Mac App Store app has been reviewed by Apple, so you can be confident that it will not pose a risk. In fact, Apple goes a step further by ensuring that apps are upfront about how they are using your data, so you can be sure that there is no risk that any of your information will be shared with anyone without your knowledge.

But even apps that you don't install from the Mac App Store will be checked by Apple before you can install them – that's the purpose of Gatekeeper, which we mentioned above. Gatekeeper checks the developer is verified by Apple and checks the file for malware and malicious code. There may be times when you want to open a Mac app from an unidentified developer, you should exercise caution if this is the case.

Another reason to choose App Store apps over others is that all apps sold via the Mac App Store must work with sandboxing. The sandbox restricts the access apps have to a Mac's resources and data.

Since macOS 10.15 Catalina launched in 2019 all Mac apps need to be notarized by Apple to launch, in addition, it is now a requirement for all Mac apps to get your permission to access your files – whether they are on your Mac, in iCloud Drive or on an external volume. The macOS will also ask for your permission before an app is able to access the camera or microphone, or log what you type, for example.

Safe surfing

The above is designed to protect you from rogue apps, but the biggest threats can be from phishing emails, websites and services you might use online.

Apple's web browser, Safari also offers various ways of protecting you online. Safari will warn you if a website is suspicious and will prevent it from opening. Every web page is loaded as a separate process in a separate tab – so if there is a problem it will be possible to close that tab without Safari itself crashing.

Another way Apple protects Mac users is by keeping Flash off Macs. Flash is one of the most common means of malware getting onto computers. Apple stopped preinstalling Flash with Safari back in 2010. Following that the only way of adding Flash was for users to install it themselves – which meant that people got used to living without it. In early 2020 Apple stopped supporting Flash and in 31 December 2020 even Flash developer Adobe stopped supporting Flash.

JavaScript also brings a number of vulnerabilities. It is easy to disable JavaScript in Safari. Just click on Safari > Preferences > Security > and deselect the box beside Enable JavaScript. Note that if you do this some visuals on the internet may stop displaying, if that becomes an issue reapply it.

As well as protecting your security online Apple also protects your privacy. For example, Apple uses Intelligent Tracking Prevention to stop advertisers tracking users around the web. Users can see a Privacy Report, including details of all the cross-site trackers Apple has stopped from profiling you.

Lockdown Mode

This is a new layer of security that arrived in macOS Ventura that helps when confronted with a cyber attack. You can use it to increase your Mac's defenses and apply strict limits so that the attacker can't exploit you. Read about how to turn on Lockdown Mode on your Mac or iPhone.

To turn it on follow these steps:

1. Go to System Settings.
2. Choose Privacy & Security.
3. Click Turn On next to the Lockdown Mode label.
4. Enter your administrator password.
5. Click Turn On & Restart.

When you believe the danger has passed, you can disable Lockdown Mode and restart again.

Password protections

Apple also monitors your passwords, helping you change them to a more secure option, suggesting strong passwords, and you'll even see an alert if Apple believes your password is involved in a data breach.

On that note, Apple also offers iCloud Keychain, a password management system that works across all your Apple devices so that you can log into software and services on any of your devices without having to remember individual passwords and login details. The benefit of this is that you can have strong rather than memorable passwords (which Apple can generate on your behalf). All your passwords are locked away behind your main password, which is protected by two-factor authentication (2FA) for added security.

Another way Apple helps to protect you is with Passkeys, which arrived in macOS Ventura and iOS 16 as an easier and safer way to sign in. Passkeys are safer because there is no password that could be leaked and everything is end-to-end encrypted. A

specific passkey is generated for any site or service, and then stored on your device and in your iCloud Keychain so you have access on your other Apple devices. You just use your Face ID or Touch ID to authenticate. Read: How to use the new Passkeys on your iPhone, iPad, and Mac.

In macOS Sequoia Apple gave passwords even more attention with the arrival of the Passwords app. This is an evolution of iCloud Keychain, where all passwords are currently stored and unlocked with a master password. The new Password app will just make the management of these passwords a bit easier. There are other Password Managers that you might also want to consider, such as 1Password.

Built-in hardware protections

“For software to be secure, it must rest on hardware that has security built in” says Apple. This highlights the main benefit of Macs: Apple makes the software and the hardware and therefore controls every aspect of the machine. This is a key reason why Macs are more secure than PCs.

Apple

Apple builds protection into the Mac hardware. This is particularly true of the Macs with Apple’s M-series of chips. The M1 system on chip, introduced in November 2020, and all other M-series chips since, have a built-in Secure Enclave that protects your login password and automatically encrypts your data. But even Intel-powered Macs with the T1 or T2 security chip can encrypt storage and offer secure boot, for example.

The Secure Enclave is dedicated to security functions and, because it’s separate silicon to the main chip, it minimizes the attack surface so any malware can’t do as much damage. Within this separate silicon is the Boot ROM (so your Mac can boot securely) and AES hardware that encrypts files as they are written. Your face and fingerprint data from Face ID and Touch ID are also kept in this Secure Enclave.

iCloud Private Relay (almost a VPN)

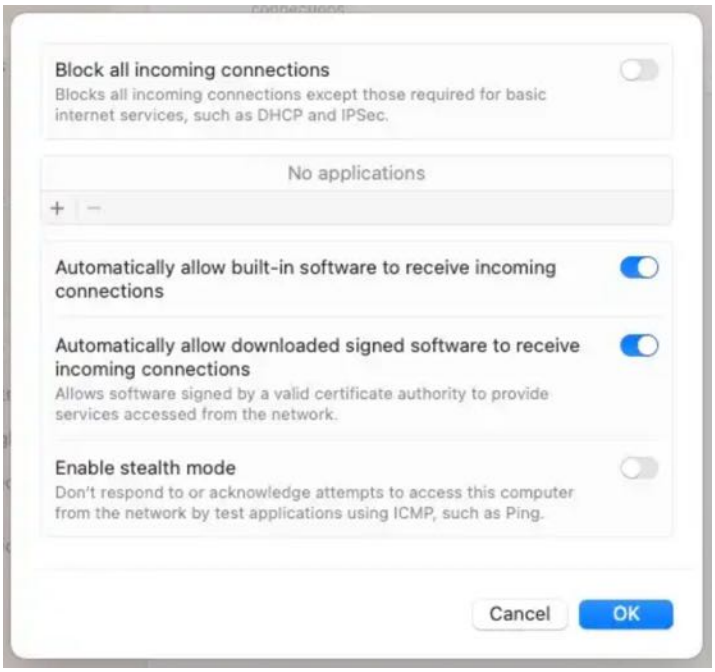
iCloud Private Relay isn’t available to all, it’s part of an iCloud+ subscription, but it can protect your privacy when you browse the web in Safari. It arrived in iOS 15.

We cover iCloud Private Relay in detail in our iCloud Private Relay Q&A, but in summary, with Private Relay enabled, all of your browsing activity in Safari is routed through Apple’s proxy server and encrypted so your ISP can’t see your web browsing.

It's a little like a VPN, but not quite. There are a lot of reasons why a VPN is a better option. Apple's solution only works in Safari and it can't hide the region you are connecting from (a key reason why people use VPNs).

If you would like to use a VPN on your Mac take a look at our best VPN round-up, our top choice is NordVPN.

macOS Firewall



You can set up a Firewall to protect your data
Foundry

A firewall can add an extra layer of security, protecting you when connected to the internet or an untrusted network. Luckily your Mac has one that you can turn on.

Here's how to turn on the Firewall on a Mac

1. Open **System Settings**
2. Click **Network**
3. Click **Firewall**
4. Click on the slider to turn it on.
5. If you want to specify additional security settings click on **Options**.

Pre Ventura (note Macs not running Ventura will not be getting security updates).

1. Click the Firewall tab in the System Preferences > Security & Privacy pane.
2. Click the padlock icon at the bottom left to unlock system settings (you'll need to type your login password when prompted).
3. Click the Turn On Firewall button.
4. Then click the Firewall Options button and, in the dialog box that appears, click the Enable Stealth Mode box. This last step means your computer will be largely invisible on public networks, such as shared Wi-Fi in a cafe.
5. In the Firewall tab, click Firewall Options to make changes. Here, you'll see a list of apps and services which are able to receive inbound connections. To add one to the list, if, say you try to run an app and it displays an error telling you it has been prevented from accepting an inbound connection, click the '+' beneath the list.

It's important to note that macOS's Firewall, while useful, offers only limited protection from malware. That's because it shields you from inbound traffic only. Its job is to limit which apps and services can accept incoming connections. It doesn't provide any control over outbound connections i.e. apps and services that initiate connections. So, for example, if you download a piece of malware, macOS's Firewall won't stop it from connecting to the internet.

Some people choose to block outgoing network connections too so that certain apps can't "phone home" without their knowledge. This also means accidentally installed malware is unable to leak your data without you being made aware.

However, macOS offers no built-in way of blocking outgoing connections. Luckily third-party apps like Little Snitch, or an outbound firewall found in anti-malware tools from the likes of Intego, Sophos and Norton, will do the job with aplomb.

There may be times when you need to allow some apps and services access through the firewall, more on how to do that here: How to open specific ports in Mac firewall.

FileVault

Apple offers FileVault as a way to encrypt your data (and keep it safe if your Mac is taken or someone gains access to it).

If your Mac has an M-series chip this encryption goes a step further and uses specific hardware to protect your login details.

We explain How to encrypt your Mac with FileVault 2 in a separate article, but you'll find the settings over in System Settings > Privacy & Security in Ventura.

Just remember that you will need to use your login password or a recovery key to gain access to your data, so there is a risk you will lose your data without one of these.

Find My & Activation Lock

Apple also has other technologies to assist you if your Mac is stolen, from Find My which enables you to track, and potentially locate your lost Mac, and wipe it so that your data can't fall into the wrong hands. The Macs with the T2 chip and M1 Macs also offer Activation Lock, a feature of Find My, to remotely lock your Mac so that only you are able to use it.

The Touch ID fingerprint scanner available on some Macs also adds another layer of security. It can be used to unlock your Mac, to log onto software and services, and for Apple Pay.

Thus Apple protects your Mac if it is stolen, or if someone with malicious intent gains access to it. Apple also protects you from malicious software, and gives you a say over whether you data is accessible and control over how it is used.

If your Mac has an M-series chip, or the T2 security chip which is found in some Intel Macs, you can use Activation Lock so that if you lose your Mac, or it is stollen, only you can erase and reactivate it.

All of these measures help to make the Mac much safer than a PC, but there are other things you can do to protect yourself further and we will run through these here: 10 ways to protect your Mac from malware and viruses.

Author: Karen Haslam, Managing Editor, Macworld

Karen has worked on both sides of the Apple divide, clocking up a number of years at Apple's PR agency prior to joining Macworld more than two decades ago. Karen's career highlights include interviewing Apple's Steve Wozniak and discussing Steve Jobs' legacy on the BBC. Having edited the U.K. print and online editions of Macworld for many years, more recently her focus has been on SEO and evergreen content as well as product recommendations and buying advice.