Macworld Do Macs need antivirus software?

Karen Haslam, Managing Editor, Macworld

Summary

Macs have built-in security features like XProtect and Gatekeeper, but they may not be enough to protect against all malware threats. While Apple regularly updates XProtect, third-party antivirus software may provide more comprehensive protection. Lockdown Mode, introduced in macOS Sonoma, enhances security by isolating devices and data during cyberattacks.

Do you need antivirus for Mac? Macs do get viruses and malware, but Apple includes its own virus protections in macOS that should keep you safe. We explain what they are and why they may not be enough.

By Karen Haslam Managing Editor, Macworld OCT 25, 2024 8:38 am PDT

Do Macs get viruses? Do Macs need antivirus software? The answers to these questions aren't as simple as they might seem. In this article, we look at the dangers faced by Mac users, and the pros and cons of using Mac antivirus software.

Historically, the Mac has been considered safe and secure for a number of reasons that we will go into below, but in recent years the consensus has fluctuated. The number of Mac viruses is growing each year. In 2021, according to security expert Patrick Wardle, eight new Mac malware families were identified. Then, in 2022, 13 new Mac malware families were discovered. That number grew again in 2023, when a total of 21 new Mac-targetting malware families were discovered. That might not doesn't sound a lot, compared to the world of Windows, but the number is growing and that is a good reason not to ignore it. We list the various Mac malware instances in our log of all the Mac viruses.

Even Apple software boss Craig Federighi acknowledged (back in May 2021) that Mac malware is a problem, although it's worth bearing in mind that at the time he was trying to make the case for iOS's very different approach to security. He said: "We have a level of malware on the Mac that we don't find acceptable," Federighi revealed that 130 different cases had been documented since May 2020, and that one of these had affected more than 300,000 Macs. He even admitted that members of his family had got malware on their Macs.

When the judge asked about the fact that Mac users can purchase and download software from various places on the Mac, rather than being limited to the Mac App Store, Federighi said: “Yeah, it’s certainly how we’ve done it on the Mac and it’s regularly exploited on the Mac. iOS has established a dramatically higher bar for customer protection. The Mac is not meeting that bar today.”

Federighi noted that Mac users don’t download as much software as iOS users, and argued that if iOS was as open to third-party downloads there would be a real problem for that platform. “If you took Mac security techniques and applied them to the iOS ecosystem, with all those devices, all that value,” he said, “it would get run over to a degree dramatically worse than is already happening on the Mac.”

Do I need antivirus for Mac?

So should Mac users start panicking? No. Mac malware does pose a risk that users should be aware of, but it doesn’t follow that Macs absolutely must be equipped with antivirus software. Such products have their advantages and you may choose to install one for more peace of mind, but we don’t view them as essential for the Mac.

For one thing, there are measures put in place by Apple at the operating system level that should protect Mac users from the worst malware threats. Macs come with antivirus and other built-in security features make attacking a Mac particularly challenging. They include Gatekeeper, which blocks software that hasn’t been digitally approved by Apple from running on your Mac without your agreement, and XProtect, which is Apple’s own antivirus built into macOS and inspects every app for malware.

Apple goes to great lengths to protect you from malware by making it almost impossible to install it. Before you can install an app, your Mac will check it against a list of malware, and even if there is no reason for concern it will not make it easy for you to open an application from a developer that hasn’t been approved by Apple. Additionally, Apple does a pretty good job of keeping on top of vulnerabilities and exploits; if your Mac needs to be protected from these, a patch will quickly be pushed out over auto-update.

These features and other protections built into macOS (which we will discuss in more detail below) mean it’s not an essential requirement to install antivirus software on your Mac.

However, as good as these protections are, there have been occasions when malware has managed to infiltrate the Mac platform, and times when Apple hasn’t responded to a threat as quickly as Mac

users might hope. If you want the very best protection from threats, therefore, consider adding a dedicated Mac security suite such as our top pick Intego Mac Internet Security. You'll find Intego in our roundup of the best antivirus for Mac, among other free and paid-for antivirus apps that might give you some peace of mind, including McAfee and Norton.

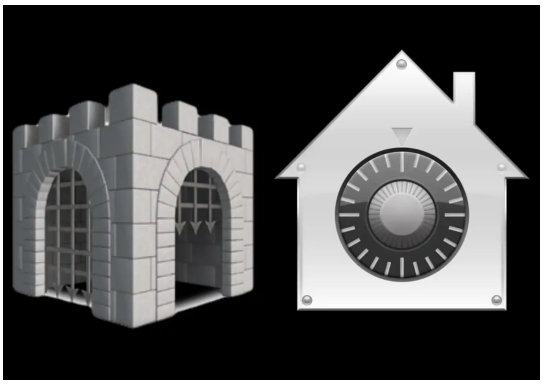
Read on to find out more about how Apple's security measures work–and why they may not be enough to keep your Mac secure.

How Apple protects Macs from viruses

Macs are generally safer than PCs, but with threats to the Mac growing due to the platform's increasing popularity, Apple has had to build in protections for macOS and the Mac hardware itself.

In this section, we will look at the built-in protections in macOS to establish whether they are enough, or if you should also install antivirus software on your Mac.

How XProtect works



Gatekeeper and XProtect are two elements of Apple's macOS security.

Apple has its own antivirus software built in. The Mac's malware scanning tool, XProtect, works invisibly and automatically in the background and requires no user configuration. Apple has a list of malicious applications that it checks against when you open downloaded applications. XProtect is regularly updated by Apple, and it updates in the background, so you should always be protected.

The presence of XProtect is similar to having antivirus software from a third-party software developer running on your Mac, with the bonus of being written into the operating system and therefore not hampering performance. With XProtect running, if you download and try to open files contaminated with malware, you may see an explicit warning that the files will "damage your computer," along with a reference to the type of malware. In that case, you should delete the file immediately.

This is great news for Mac users, but is it enough? How does XProtect compare to the antivirus solutions out there? Well, XProtect may not be as up-to-date as some third-party products and it tends to focus on known malware threats and doesn't look for as many strains of malware. But updates to XProtect do happen regularly to include cover to macOS malware, for example on October 12, 2023 Apple updated XProtect

adding cover for Atomic Stealer and Adload malware. There was another update to XProtect Remediator in October 2024. This is why it is important to keep your Mac software up-to-date. macOS checks for new updates every day and starts applying them in the background, it will send you a notification to confirm that the update is ready to install – so make sure you do.
…

How Gatekeeper works

Gatekeeper on your Mac ensures that all apps from the internet have already been checked by Apple for known malicious code. Thanks to Gatekeeper, macOS blocks downloaded software that hasn't been digitally signed, a process whereby Apple approves the developer and issues a certificate. This certificate tells Apple who the developer is and if it's blacklisted, and if the software has been tampered with since leaving the developer for distribution.If you try to install unsigned software you will see the message: "[This app] can't be opened because it is from an unidentified developer." One change to Gatekeeper that arrived in macOS Catalina a few years back was that software is checked for malware and other issues every time it runs, rather than just the first time you install it.

For maximum protection, GateKeeper can be set to only allow software to be installed if it was downloaded from the Mac App Store. Or you can set it to allow you to install software from the web, but from verified developers only.

You can adjust these settings via the Privacy & Security section of System Settings (previously System Preferences > Security & Privacy > General):

1. Open System Settings.
2. Select Privacy & Security.
3. Scroll down to the Security section.
4. Choose from the options underneath Allow Applications Downloaded From.
5. Choose App Store or App Store and Identified Developers.

The safest option is App Store only, but if you also want to be able to install legitimate software from the web then App Store and Identified Developers is the best plan. There used to be a further option to disable the feature by choosing 'Anywhere,' but this option is no longer available.

All software downloaded via the App Store is signed, but should you attempt to open an app you've downloaded from the web that isn't signed, you'll see a Gatekeeper warning like the one below:

This may mean you've almost installed malware. On the other hand, of course, it may be a legitimate app. In which case (and if you're sure) you can bypass Gatekeeper's protection and install it.

To do so, go to the Finder and locate the app there. Now hold down Ctrl when you click on the app, and then select Open. This will mark it as being trusted. For more details, read how to open an app from an unidentified developer.

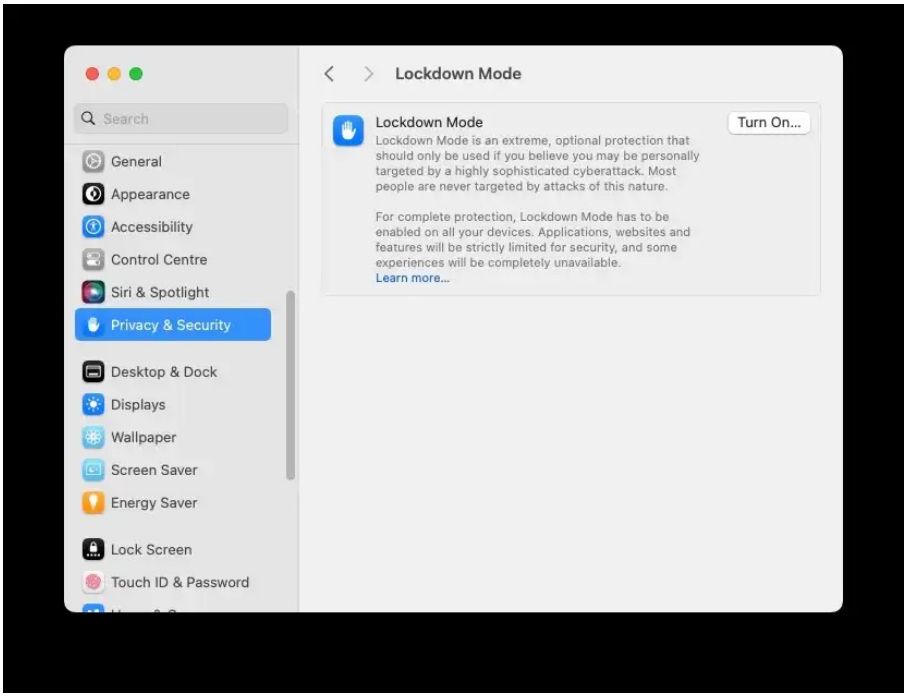
Being able to download unsigned software might sound like a benefit, but it essentially enables you to bypass the protections offered by Gatekeeper. That's a mixed blessing, and more and more malicious apps are instructing users to do exactly this when they are installed.

Lockdown Mode

Lockdown Mode is a feature that arrived in macOS Sonoma in 2023 that makes it easy to protect your Apple devices and your data if you are the victim of a cyberattack.

Just activate Lockdown Mode and all your Apple devices will be protected and the hacker will find it a lot harder to steal your data.

You'll find Lockdown Mode in the Security section of System Settings > Privacy & Security.



Sandboxing and related protections

Software that is approved by Apple is also sandboxed. App sandboxing isolates apps from the critical system components of your Mac, your data and your other apps, so they shouldn't be able to modify other apps without permission. It doesn't protect you from malware getting into the system, but it does limit the extent of what the malware can do once it's in there. The main problem

here is that while apps sold on the Mac App Store have to be sandboxed, other Mac apps don't.

Another issue with Sandboxing was highlighted in August 2023 when software developer Jeff Johnson released details about a flaw in App Management that involves the Sandbox. App Management is a security feature introduced in macOS Ventura that is intended to prevent malicious software modifications by keeping an eye out for attempts by software to modify other apps on the Mac. Should this happen, App Management will block the modification and alert the user. The concern was that users could grant permission for such a change without being warned that it is a sandboxed app, thereby bypassing a check by App Management.

Since macOS 10.15 Catalina arrived in 2019 it has been a requirement for all Mac apps to get your permission before they can access your files. macOS will also ask for your permission before an app can access the camera or microphone, or log what you type. A potential issue here is that users see these alerts so frequently it becomes second nature to approve them without consideration.
Another change that arrived with Catalina is that macOS itself is now stored on a separate disk volume. This means that your important system files are all completely separate and therefore more challenging to access. Apps can't get to your system files where they could cause problems.

Background Task Manager

With macOS Ventura in October 2022, Apple added Background Task Manager, a tool used by macOS to monitor for "persistent" software and notify the user of any suspicious activity.

In August 2023, Mac security researcher Patrick Wardle criticized the tool suggesting that it can easily be bypassed so that malicious software can run without the user knowing it.

Wardle discovered ways to disable the notifications that Background Task Manager sends to the user when a persistence event is recognized. One method requires root access, which means that the threat agent needs full control of the Mac to disable the alert, but Wardle found two other methods that can be deployed remotely. So an attacker could disable the notifications and allow the malware to run unnoticed.

Wardle wrote: “[Background Task Manager is] a good thing for Apple to have added, but the implementation was done so poorly that any malware that’s somewhat sophisticated can trivially bypass the monitoring”.

Security updates

Apple regularly issues security updates for the Mac. While these can serve to demonstrate that the Mac isn’t infallible, with Apple all too frequently having security flaws pointed out to it, they are generally issued promptly.

These security updates have generally been issued as part of a larger macOS update: for example, macOS Monterey 12.2.1 closed a security vulnerability in WebKit that would have made it possible to execute malicious code. Because these security fixes were issued as part of a macOS update, which often requires the computer to reboot during the installation process, Mac users may be less likely to install the update promptly, even though these updates can be set to install automatically.

Since the launch of Ventura, however, Apple has started separating out the security updates from wider macOS updates and rolling them out automatically. This way the update can happen in the background, without a restart.

Generally, Apple can respond quickly as it makes the software and the hardware. But the problem is more prevalent when Apple has less control over the issue, as with Intel’s Downfall processor vulnerability that affected Macs with Intel chips built between 2016 to 2020. Intel patched the issue, but released that its Downfall patch could slow some CPUs. If you have a Mac that uses Apple Silicon (an M1 or M2-based processor), you have nothing to worry about. It’s a good reason to consider upgrading if you have an Intel-powered Mac.

This is why it is important to instal updates from Apple – but not just Apple. It’s important to install updates for all your apps regularly. Developers fix security issues via updates. The Mac App Store usually does a good job of keeping apps updated automatically, but we recommend checking at least once a month for any updates that might not have been installed. When it comes to apps you’ve downloaded from outside the App Store, you need to check for updates in the app’s menu bar option.

Password protection and Passkeys

Apple’s iCloud Keychain is a password manager that was introduced in 2011 with Mac OS X Mavericks (and iOS 7). It was an evolution of Apple’s Keychain software for managing passwords and login information that arrived with MacOS 8.6 in 1999, but brought this capability to all Apple devices, allowing for passwords to be synced and

used across devices. So password management is nothing new on the Mac. However, Apple is moving it up a notch in macOS Sequoia.

The main change that arrived with Sequoia is how easy it will be to find your passwords. Currently users have to look in Settings: go to System Settings (System Preferences) > Passwords. There it is possible to unlock with the main password to see every other password ever used. (View this same information on an iPhone in Settings > Passwords.) With the arrival of Sequoia (and iOS 18) users will see a dedicated app for password management, rather than it being hidden in Settings (which will probably help some people discover it).

The benefit of iCloud Keychain and the Password app is that it is only necessary to remember one password to unlock all the passwords you need. No need to memorize a lot of different passwords – or more likely use one easy-to-remember (and crack) password for everything. Apple will also help you create a strong password and will warn you if your password is easy to hack, if you have reused a password, and if it has appeared in a leak. If it ever detects a security concern, Password Monitoring will alert you.

Over the years Apple's password protections have improved. For example, in Monterey a new authenticator was added, so you can set up verification codes instead of using an authentication app. To add a setup key you need to click on a password and then choose Enter Setup Key, which you should be able to obtain from the provider. Once input the 2FA verification codes should automatically fill.

In macOS Ventura Apple introduced Passkeys. Apple explains: "Passkeys use iCloud Keychain public key credentials, eliminating the need for passwords. Instead, they rely on biometric identification such as Touch ID and Face ID in iOS, or a specific confirmation in macOS for generating and authenticating accounts." Passkeys are more secure, according to Apple. Essentially your device will hold one part of a cryptographic key pair and the other part will be stored by the website or service you're logging into. Your device will authenticate you biometrically (with Touch ID or Face ID) and log you in. For more information, read How to use Passkeys.

In macOS Sonoma, Apple simplified the use of 2FA. Safari automatically fills in the code you are sent (as a text or email) and automatically deletes the email or text afterwards.

Another new feature added in Sonoma is a simplification of the process for sharing passwords with friends and family. Users can create a group and share a set of passwords to that group. It's end-to-end encrypted.

Recording alerts

In macOS Monterey Apple added a Recording indicator in the menu bar so you'll know if an app is recording you. A bit like the light that indicates the mic is in use on your iPhone.

Pasteboard alerts

Similarly, as of macOS Ventura, any app that wants access to your pasteboard has to request permission.

Safari protections

Anti-phishing technology in Safari will detect fraudulent websites. It will disable the page and display an alert if you visit a suspect website.

Anti-phishing isn't the only way that Safari protects you when you're surfing. Apple also allows users to prevent advertisers tracking them around the web. You can see a Privacy Report including details of all the cross-site trackers Apple has stopped from profiling you.

You'll also notice that plug-ins such as Silverlight, QuickTime, and Oracle Java won't run if they aren't updated to the latest version, another way of ensuring your Mac is safe. And of course now that Adobe has discontinued Flash people should hopefully no longer fall for malware hidden in Flash Player.

Safari will also flag up weak passwords and make strong password suggestions when you open an account on a website. This strong password will be saved in your iCloud Keychain so you won't have to remember it. It's a lot safer than using the same password you always use. For more on this subject, read about How Apple plans to retire passwords.

In the past, one issue with Apple's suggested passwords has been that sometimes they don't match the website's requirements. For example, a website may require one upper-case letter, one special character, one number and so on. As of the launch of Ventura, macOS allows users to edit suggested passwords so they meet these requirements.

New in Safari 15 were improvements to the Intelligent Tracing Prevention that arrived in Safari 14. Now web trackers won't be able to see your IP address so they won't be able to create a profile about you. Check this by choosing Safari from the Safari menu > Preferences > Privacy > Hide IP address from trackers.

The Safari Private Browsing feature improved with macOS Sonoma. You can set a new Private Browsing Lock to appear on the screen to stop onlookers from viewing your screen when you aren't present.

Private Browsing also stops web-based trackers from recording data about you via tracking codes by removing those codes. Tracking information is even removed if you links via Messages or Mail.

Photo privacy

A few years ago there was a lot of bad publicity for Apple when celebrities reported that their iCloud photos had been stolen. (For more on this, read How to stop photo hacks on iPhone.) There have been a number of security enhancements in iCloud since this happened, and Apple has given users other ways to protect their photo privacy: for example, the ability to hide photos and albums. In Ventura, Apple expanded this so that hidden albums, and the Recently Deleted album, are locked by default, and only authenticated by Touch ID or Face ID.

Mail protections

macOS Monterey brought a new feature in Mail on the Mac. Mail Privacy Protection improves privacy for users. For example, it stops email senders from being able to track whether you've opened an email, or even determine your location from your IP address. Check that the feature is working for you by opening Mail > Click on Mail in the menu > choose Preferences > Privacy > and make sure Protect Mail Activity is selected. It should be by default.

There are additional Mail protections if you're an iCloud subscriber. Hide My Email allows you to create an alternative email address that you can give out. The email will still be delivered to your inbox, but you can easily delete the alternative email later.

You can turn this on in System Preferences > click on Apple ID > and select Private Relay (currently in Beta).

In Ventura Hide My Email was extended to third-party apps.

iCloud+ protections

If you're an iCloud subscriber, you'll be interested in a feature that arrived in Monterey (part of the upgrade from iCloud to iCloud+) called Private Relay. It's a bit like a VPN in that it encrypts your network traffic and routes your DNS lookup requests through two servers, one of which is not controlled by Apple. However, it's not a VPN, because it only works in Safari and obviously it lacks the other usual features of a VPN. (If you

want a VPN, by the way, check out our roundup of the best VPNs for Mac. You may even be able to save some money if you take a look at our roundup of VPN deals, or try one of these free VPNs.)

You can manage your Private Relay settings in System Preferences > Apple ID > click on Options beside Hide my email. Here you will see any fake email addresses you're using; just click on Turn Off if you want to stop those emails arriving. You can also change which email address they are forwarded to.

Safety Check

A new feature in macOS Ventura is Safety Check, a feature that will allow anyone who is concerned that they are in danger from a person known to them to revoke any access they have granted to that person. So, for example, that person won't be able to access their location, their photos, or anything else that could help them to be traced.

File encryption with FileVault

FileVault–Apple's name for full-disk encryption–makes sure your data is safe and secure by encrypting it. Intel Macs that featured the T2 Security Chip and all M-series Apple silicon Macs have encryption built in at the bottom level of macOS. The startup internal volume is always encrypted, and you can't turn it off. FileVault also encrypts external volumes.

With FileVault on your Mac's drive is completely encrypted and encryption keys (protected by your account password) are required to unlock it. If your Mac is encrypted with FileVault, an attacker will be locked out, macOS won't even unlock your drive for access at startup without a valid account password or an associated Recovery Key (just be aware that if someone hacked your Apple ID they could potentially gain access to the Recovery Key and unlock your Mac's drive).

The main problem is that without that Recovery Key you are also locked out and won't be able to access your data, so do look after it. See How to find your FileVault recovery key in macOS.

Read our tips for keeping your Mac secure, of which using FileVault is one.

Warnings about spyware

Apple announced in November 2021 that it would warn its users of state-sponsored espionage attacks, such as the well-publicized Pegasus spyware, on their iPhones,

iPads and Macs. The notification will come via email or a message. The same warning will be displayed on the user's Apple ID page at appleid.apple.com.

The warning will offer advice about how affected users can protect themselves against attack. There's more information on Apple's site.

Find My

Not every threat to your data comes from malware. Sometimes a criminal might get hold of your Mac, in which case Apple's Find My service will come into its own.

The Find My app can relay the location of your lost or stolen Mac back to you. If you're concerned that it might not be recoverable, you can wipe the contents of the Mac so that your data can't be accessed. For more on this, read How to find a lost or stolen iPhone.

In addition, every Mac with an M1-series, M2-series, or T2 chip has an Activation Lock feature which means they can be erased remotely and only you can reactivate the Mac.

Siri, ID and Apple Intelligence

There are new AI features coming to macOS Sequoia and iOS 18. There may be concerns about how this will affect privacy and security as, while in most cases the processing will be done on the device, in some situations tasks that need more processing power will be sent to Apple's servers. During WWDC 2024 Apple explained that this will all be done securely and that the data will never be accessible to anyone, including Apple. Apple's Craig Federighi said: "Private Cloud Compute uses your data only to fulfill your request, and never stores it, making sure it's never accessible to anyone, including Apple. And we've designed the system so that independent experts can verify these protections."

When Apple's security measures aren't enough…

The security measures detailed above are great, but unfortunately, there have been cases when they haven't been enough.

Gatekeeper, for example, has occasionally been bypassed because malware has got an approved developer signature. For example, OSX/CrescentCore was signed by a certificate assigned by Apple to a developer. It took Apple a few days to retract that certificate.

In the case of OSX/Linker, meanwhile, a zero-day vulnerability in Gatekeeper was exploited. Apple normally reacts quickly to such threats, although there have been cases where the company has ignored an identified vulnerability; on one occasion a teenager reported a flaw in the group FaceTime feature that meant someone could listen in to a call, and Apple failed to act.

Intel-based Macs released between 2018 and 2020 with the T2 security chip had a security flaw that was never fixed. Researchers found a vulnerability in the security chip that could allow someone with physical access to the computer to potentially bypass security features. Silicon Macs do not suffer the T2 vulnerability, but they're not flawless. The "Augury" and "GoFetch" flaws in M-series chips are hardware issues that cannot be patched without serious performance hits. Nobody has actively exploited these vulnerabilities, and as long as nobody gets their hands on your Mac, you should be safe – but it does emphasis the importance of looking after your Mac, for example, not leaving it on a table in a coffee shop while you visit the bathroom.

When Apple is made aware of a threat the company usually issues a security update to the latest version of macOS and to the two versions prior. This way Apple will protect users from vulnerabilities and flaws that could be exploited by hackers.

Normally our advice would be to install security-related updates immediately. However, on occasion, these can themselves cause difficulties. A Sierra and High Sierra security update in July 2019, for example, had to be pulled after people experiences problems after installing it.

How Apple responds to security threats

Apple has its own security research team, but it depends on users and independent researchers to help by reporting any flaws they find in Apple products.

To this end, Apple has an incentive program that rewards such discoveries with payments of up to $200,000, depending on the seriousness of the flaw. But it was the last major tech company to set up such a scheme. (Microsoft set up its own bug-reporting incentive program in 2013, and was itself criticized at the time for leaving it so late.)

On August 4, 2016, Apple security boss Ivan Krstic announced the Apple Security Bounty Program. "We've had great help from researchers in improving iOS security all along," Krstic said. "[But] we've heard pretty consistently… that it's getting increasingly difficult to find some of those most critical types of security vulnerabilities. So the Apple Security Bounty Program is going to reward researchers who actually share critical vulnerabilities with Apple."

The top reward of $200,000 is given to those who discover vulnerabilities in Apple's secure boot firmware components; for less critical flaws the bounties drop through a series of smaller figures to a bottom tier of $25,000. Wired has the details.

We imagine most Mac users will be pleased to hear that Apple has an incentive program to encourage more widespread reporting of its vulnerabilities. Incentivizing security researchers to let Apple know about a flaw instead of passing it on to hackers (which may still, sadly, be more lucrative) makes Apple products safer for everyone.

One such flaw was the High Sierra root bug, discovered on November 28, 2017. This flaw in macOS 10.13 could allow access to settings on a Mac without the need for a password. Apple immediately issued a statement confirming that it was working on a fix and that an update should be issued within days.

How to keep your Mac safe from malware

Apple does a lot to keep your Mac safe, but you have to do your bit: by installing updates when they arrive, not clicking on suspicious links in emails, not installing Flash, and so on. There are also some third-party antivirus apps you could try. We have a complete guide to the best antivirus for Mac.

Here are a few of the things you should do:

1) Keep macOS up to date

To reduce the impact of these risks, you should keep regular backups and install security updates as soon as possible.

Apple addresses Mac flaws and vulnerabilities by issuing updates to the operating system. It's therefore important to keep your Mac up to date. Checking regularly for OS updates is a key part of a sound security strategy.

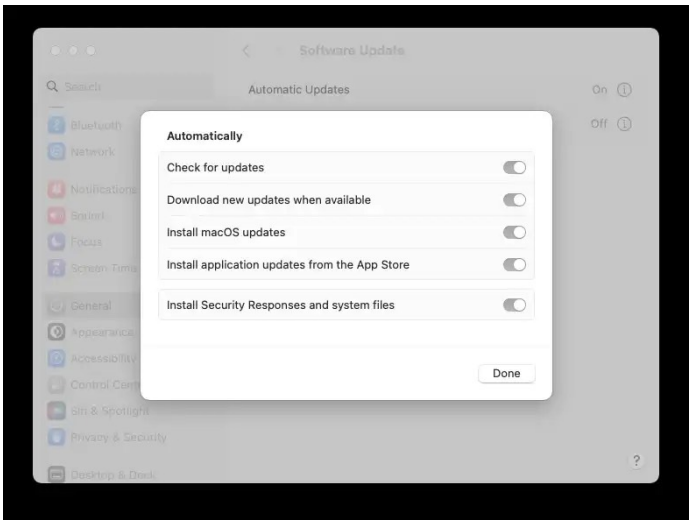
You can find out about the latest version of macOS here: macOS Ventura latest version information.

You can set your Mac to automatically update as soon as a new version of the operating system is made available. Follow these instructions to set that up:

How to automatically install macOS updates

1. Open System Settings.
2. Click on General.
3. Click on Software Update.

4. Click on the (i) beside Automatic Updates.
5. Make sure that the options are selected.



On older versions of macOS you needed to go to System Preferences > Software Update and you could be able to click on Advanced and select precisely which actions you want to happen automatically from Check for updates, Download new updates when available, Install macOS updates, and Install app updates from the App Store.

How to manually install macOS software updates

If you'd rather not let your Mac automatically update, you should periodically check to see if there is an update to your version.

- Go to System Settings > General > Software Update and your Mac will check to see if there is an update to install.

In macOS Mojave and older the Software Update pane was found in System Preferences and in macOS High Sierra and earlier updates were via the Mac App Store.

For our in-depth guide to updating Mac operating systems, see How to update macOS.

2) Don't connect to public Wi-Fi networks

Beware of connecting to a public Wi-Fi network as there may be someone spying who could gain access to your passwords and other private information, or you could have your session hijacked. Snoopers can set up their own Wi-Fi hotspot, pretending to be your hotel or coffee shop, then once you have connected they can grab any data you send over it.

3) Don’t install Flash

Adobe discontinued Flash on 31 December 2020 with good reason. Intego, Malwarebytes and other security companies have recommended that you shouldn’t install Flash Player, because fake Flash Player updates have often been used to trick people into installing malware. You might be looking to download a popular movie or TV series for free, for example, and see a search result that leads to a request to update Flash Player in order to view the content. This is unlikely to be legitimate.

There is simply no need to install Flash Player now that HTML5 has made Flash obsolete. Our advice is simple: Don’t use Flash!

4) Keep Java up to date on your Mac

If you must use Java (which is also problematic) then make sure it’s up to date. Vulnerabilities in Java have highlighted the fact that there are cross-platform threats that even Mac users need to be aware of. Apple blocks Java by default, leaving it up to the user to decide whether to install those tools. If you do need to update them, be very careful where you download updates from!

5) Avoid falling foul of phishing emails

Protect yourself from phishing attacks by not responding to emails that require you to enter a password or install something. You could also use free software such as BlockBlock. That way, even if you were to carry out the steps to launch the malware, it would not be able to write files or mark itself as launching on startup.

6) Don’t fall for Facebook scams

Facebook scams are usually designed to harvest data. If it seems like it might be too good to be true, it probably is, and you’d be wise not to share it on Facebook. At best you’ll look silly and those scammers will start to target you with more scams; at worst they may succeed in accessing your personal data and that of your friends. Don’t click on a link just because a friend shared it, and definitely don’t give out your personal data on Facebook.

Why you need to protect Windows users

Macs are pretty safe from malware, but one reason to run an antivirus is to protect your Windows-using friends and colleagues. An unprotected (and carelessly used) Mac could become a sort of Typhoid Mary of Windows viruses; in other words, you

could be harboring viruses that won’t affect you, but could be problems for Windows users.

How to tell if a Mac has a virus

Look out for the following signs that your Mac has been infected with malware:

1. Aggressive web page banners and browser pop-ups recommending software.
2. Web page text turning into hyperlinks.
3. Programs appearing that you haven’t authorized.
4. Mac crashes.
5. Mac runs hot.
6. Mac speeds up for no reason.

If you think something suspicious is happening, open Activity Monitor and click on the CPU tab. Check what software is running, especially if something is hogging a lot of your resources.

We discuss how to identify and deal with Mac viruses in a separate article: How to remove a virus from a Mac. We also recommend reading How to protect your Mac against attack for more advice on avoiding digital infections.

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.