INSIDE: ULTIMATE MAC TROUBLESHOOTING GUIDE

Macworld

APRIL 2023

SECURITY SPECIAL

BEST AV SOFTWARE, VPNS & MUCH MORE

CONTENTS

Credit: Getty Images/Orhan Turan

NEWS

NEWS ANALYSIS

SECURITY SPECIAL

Cover Image Credit: Getty Images/BlackJack3D

Credit: Getty Images/Sakorn Sukkasemsakorn

MACOS TIPS & TRICKS

HELP DESK

Credit: Getty Images/Prykhodov

Apple may have just outed its own big spring MacBook surprise

A listing in the Bluetooth Launch Studio database points to an unreleased Mac with Bluetooth 5.3. **Michael Simon** reports

Rumours are swirling that Apple is planning to release a new MacBook Air within the next couple of months, with an M2 processor and a larger 15-inch screen. And now a filing by the Bluetooth Launch Studio (fave.co/3kpjbXk) suggests the new machine may have Bluetooth 5.3 too.

On 18 February, Apple apparently began the Bluetooth Qualification Process for a new Mac with Bluetooth 5.3. There are no products listed under the declaration, meaning they have not yet completed the full qualification process. Had the products in question been the new M2 Mac mini or MacBook Pros, the first Macs to use Bluetooth 5.3, the model numbers would have been listed.

While it makes sense for the 15-inch MacBook Air to use Bluetooth 5.3, it would also give it an upgrade over the 13.6-inch MacBook Air, which is unlikely to be updated until the M3 chip arrives in 2024. It's not something that's likely to sway anyone's purchase, mind you, especially since Apple doesn't offer any features or accessories that require Bluetooth 5.3.

The new machine would also presumably have Wi-Fi 6E, which is available on the M2 Mac mini and MacBook Pros as well. Elsewhere, the new MacBook Air is expected to have similar specs to the 13.6-inch model, including two Thunderbolt ports, MagSafe for charging and 256GB of entry-level storage.

The device could arrive at Apple's next event in March or April, although that event is in some doubt this year, given the reported delays affecting the AR headset project that was expected to be its headliner. In the absence of an event, the new Air could instead drop quietly via a press release and update on Apple's website, as was the case for January's Mac launches.

Apple reportedly snatching the entire early 3nm supply for iPhones and Macs

TSMC is catering almost exclusively to Apple's chips needs. **Michael Simon** reports

When Apple releases the new iPhone 15 Pro this autumn, it could offer a significant jump in performance and power efficiency than the past few models. That's because of the A17 chip, which is almost certain to use a new 3nm chip-making process that is significantly faster and more efficient than the current 5nm process.

And it could be a while before any other chip comes close. According to DigiTimes, Apple is going all-in on 3nm for the iPhone in 2023, reportedly snatching up TSMC's 'entire initial 3nm supply'. Apple is a priority customer for TSMC and it pays a premium to get first dibs on new manufacturing process technology – prior reports have said that TSMC charges $20,000 per wafer, which typically yields several hundred chips.

It's not unusual for Apple to grab all, or nearly all, of the initial supply of a new process technology out of TSMC. We don't know how big 'initial supply' is or how long Apple's order will last, but as we've seen in other years, Apple will almost certainly be the only company with a mass consumer product using this manufacturing technology for several months.

Apple's order sets up the company for a 3nm A17 Bionic chip in the iPhone 15 Pro as well as the Mac's M3 processor that will likely arrive in late 2023 or early 2024. The move to 3nm is an improvement over the current enhanced 5nm process that increases the transistor density significantly and allows for more and more powerful processing cores, more cache, more everything while having a lower power demand. So we could see jumps in performance that are more than the typical increase from year to year. Apple first moved to a 5nm process with the A14 chip in the iPhone 12.

The new 3nm A17 Bionic will likely be exclusive to the iPhone 15 Pro, with the iPhone 15 using the 5nm A16 Bionic, which will further differentiate the pro and non-pro phones. On the Mac side, there's a chance Apple could make the jump to the 3nm M3 at an October event, though recent reports claim the first M3 Macs wouldn't arrive until 2024. We're also expecting Apple plans to ship a new 15-inch MacBook Air this spring as well as a new Mac Pro, both of which would likely stick with the 5nm M2-series chips.

According to reports from TSMC, the gains from the 3nm chips are bigger than expected. That would be welcome news to iPhone and Mac fans, who were somewhat disappointed by the A16 and M2.

Apple isn't the only company moving to 3nm. Qualcomm and MediaTek will make 3nm chips eventually, but not in time for any 2023 Android phones. Intel plans to do 3nm, too, but it will be at least another year before it makes the move, according to DigiTimes.

The 2nd-generation Apple silicon iMac might take three years to arrive

The next edition will sport an M3 processor. **Roman Loyola** reports

It looks like the 24-inch iMac with the M1 processor is going to stick around for a while longer. In his latest Power On newsletter (fave.co/3YVctY7), Bloomberg's Mark Gurman reports that the next generation iMac might not see an upgrade until late 2023.

Gurman wrote that he has not "seen anything to indicate there will be a new iMac until the M3 chip generation", which would mean the 24-inch iMac skips the M2 generation altogether. The M3 chip will be manufactured using the 3-nanometre process, which could bring performance improvements that are better than the 20 percent we've seen between the M1 and M2, both of which are 5nm chips.

Gurman says the M3 models "won't arrive until the tail end of this year at the earliest or next year". Apple released the redesigned 24-inch iMac at an event in the spring of 2021, so a 2024 release would be a full three years between models.

While Mac users have learned a lot about the tech behind Apple's M-series chips and how they perform, there's still a lot to learn about Apple's release cadence with the chips. A 32- or 36-month gap would be the longest time yet between updates. For example, the M1 MacBook Air stuck around for about 20 months before the M2 model arrived, but the M1 Mac mini had a near-26-month shelf life. However, Apple and its production partners are still feeling the effects of the supply issues that occurred because of the pandemic, so it remains to be seen if the consumer-level chip release cadence develops a more predictable pattern.

Gurman's report did not mention any changes in the design or other features of the 24-inch iMac. In past reports, Gurman has mentioned Apple's plans for a larger iMac Pro to complement the 24-inch model, which could be released this year.

Apple may let the Mac Studio languish, so more people buy the Mac Pro

A new report claims Apple's powerful desktop Mac will keep its M1 chips for the foreseeable future. **Michael Simon** reports

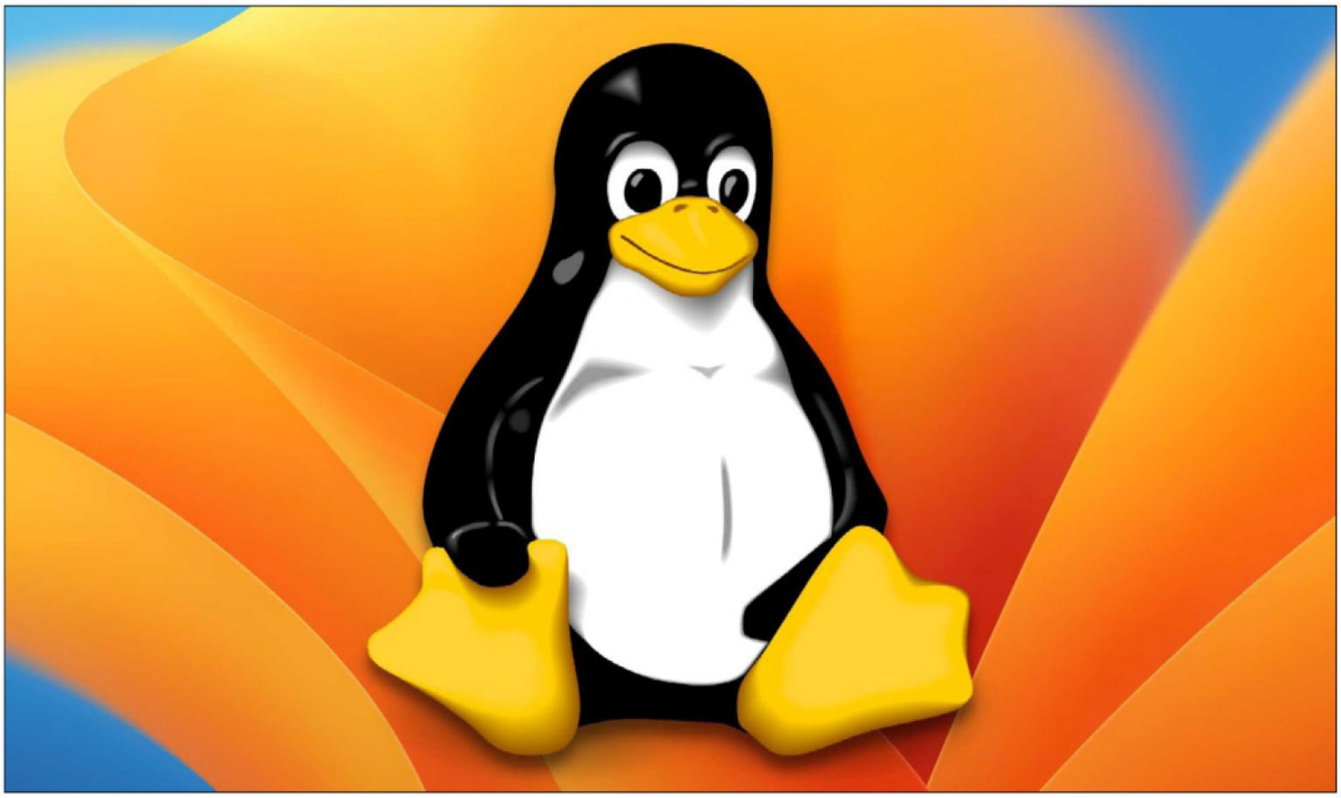
It's been about a year since Apple surprised us with the launch of the Mac Studio with M1 Max and M1 Ultra chips, which was largely seen as a precursor to the Mac Pro. According to a new report by Bloomberg's Mark Gurman (fave.co/3IpuC9h), it's a little too close to the Mac Pro.

In his latest Power On newsletter, Gurman claims that Apple is unlike to launch a new Mac Studio "in the near future". As he explains, the upcoming Mac Pro "is very similar in functionality to the Mac Studio", and Apple will likely delay its chip upgrade by at least a generation so buyers aren't confused.

Gurman says Apple is more likely to “never update the Mac Studio or hold off until the M3 or M4 generation” when it “may be able to better differentiate the Mac Studio from the Mac Pro”. The Mac Pro is expected to have an M2 Ultra chip, but few expandability options beyond internal storage slots.

In our review of the new M2 Mac mini, we noted the potential for overlap with the Mac Studio. As it stands, the M2 Pro Mac mini with 32GB of RAM and 1TB of storage costs £1,999, the same price as the Mac Studio with an M1 Mac processor, 32GB of RAM and 1TB of storage. If the Mac Studio was to get an M2 upgrade, there would be little reason to buy an M2 Pro Mac mini.

Apple is expected to announce the Mac Pro this year, either at WWDC or in the autumn. It is the final Mac to still have an Intel processor, following the launch of the M2 Pro Mac mini in January to replace the aging Core i5 Intel model.



Linux 6.2 is up and running on M1 Macs, but still missing many key features

The latest Linux build can technically run on Apple silicon, but you won't be able to do much. **Roman Loyola** reports

If you've been waiting to run Linux on your M1 Mac, we have good news: Linux 6.2, which was released this week, adds upstream support for the M1 Pro, M1 Max, and M1 Ultra. However, there are some serious caveats.

The new Linux 6.2 is considered stable enough for distribution, but according to an Asahi Linux support document, many features on Apple silicon are still labelled as a work in progress and not ready for wider testing or distribution, such as Thunderbolt, speakers, and microphones. Other features, including the webcam, Touch ID, and the Touch Bar are listed as TBA (to be announced), which means that they're not even being worked on at the time of the posting.

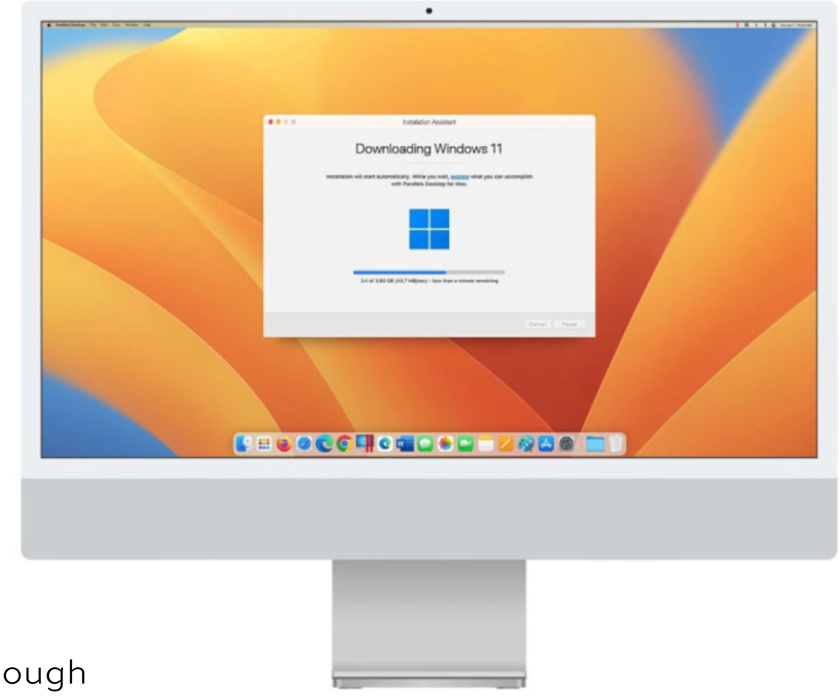
Despite the missing features, Linux 6.2 is functional enough for a user to do some work and is expected to be used as the default kernel for popular Linux distributions such as Ubuntu and Fedora. Linux 6.2 also includes support for Intel Arc graphics, the Nvidia GeForce RTX 30 series GPU, and updated drivers.

Linus Torvalds, the lead developer of the Linux kernel, says version 6.2 is "not a sexy LTS [long-term support] release", but the support for Apple silicon is definitely notable. Getting Linux to run on Apple's M-series chips has been an arduous task for the Linux community. The first build of Linux to run on an M1 Mac mini was created by Asahi Linux last July.

RIP Boot Camp: Microsoft endorses Parallels for Windows on M1 and M2 Macs

If you want to run Windows 11 on an M1 or M2 Mac, you need to use virtualization. **Roman Loyola** reports

Apple's switch to its own silicon has a lot of advantages on the Mac, but there is one major feature that was lost in the transition from Intel processors: Boot Camp, Apple's utility that allows Macs to natively run Windows alongside macOS. While Boot Camp (fave.co/3SEMNwE) is still



Installation Assistant

Downloading Windows 11

Installation will start automatically. While you wait, explore what you can accomplish with Parallels Desktop for Mac.

3.4 of 3.80 GB (43.7 MB/sec) – less than a minute remaining

Microsoft has authorized Parallels as a solution for running Windows for Arm on an M-Series Mac.

supported in Ventura, you won't find it on an M1 or M2 Mac.

If a user wants to run Windows on one of those newer Macs, the solution is to use the Arm-version of Windows through virtualization software. However, Microsoft's licensing restrictions didn't officially allow users to run Windows for Arm on an M-series Mac – even though technically, it could be done.

However, in February Microsoft announced through a support document (fave.co/3EFSBjo) that Parallels Desktop 18 (fave.co/3SByxob) is now 'authorized' to run Arm versions of Windows 11 Pro and Windows 11 Enterprise on M1 and M2 Macs. The authorization is a big deal because it means that in business environments, Parallels and Windows on Arm can be deployed, and users can get support if they run into problems.

Microsoft's announcement specifically names Parallels as an authorized solution. Microsoft does not sell Windows for Arm as a standalone product, but you can download and install Windows 11 directly through Parallels. VMware Fusion (fave.co/3IYDjZC), QEMU (fave.co/3XYDJni) and other virtual machines don't offer a way to get Windows for Arm (though they can run it), and these VMs appear to be still unauthorized. (When I asked Microsoft PR about unauthorized VMs, they referred me to the aforementioned support document and said that they have nothing further to share at this time.) The only other authorized option for running Windows on a Mac is to use Microsoft's Windows 365 online service and run a Cloud PC.

THE FINAL NAIL IN BOOT CAMP'S COFFIN

Boot Camp became an official part of the Mac operating system in 2006 as part of Mac OS X Leopard. 2006 also was the year that Apple switched from Motorola processors to Intel, and since Windows runs on Intel silicon, Apple was able to provide the benefit of running Windows (as well as Linux) natively on Mac hardware – though Apple always reminded users that it did not provide support for Mac hardware running non-Mac operating systems.

Apple's M-series chips use the Arm architecture, which is different from the x86 architecture in Intel processors, so the version of Windows that runs on Intel PCs will not work on M-series Macs. With Apple's transition to the M1 processor in 2020, the company decided to not develop Boot Camp for the M-series Macs. While Apple says the M-series Macs can run Windows for Arm, it's not going out of its way to do it and there are no indications that development is happening. Since Microsoft's Windows for Arm licence has explicit details on the hardware it supports, presumably, Windows for Arm running natively via Boot Camp would be unauthorized.

For the small number of users who need to run a different operating system natively on a Mac, Boot Camp was a convenience, and users' pleas to Apple to bring back the feature fell upon deaf ears. Microsoft's announcement dashes any hope that users had for a Boot Camp revival because it now gives Apple an official solution to point to. Apple can now simply refer users to the Parallels set-up whenever the Boot Camp conversation arises. End of discussion. Apple has continued work on the Intel version of Boot Camp – it was last updated in August with an update to the Precision Touchpad driver – but those updates are likely to end soon as Apple stops putting resources into Boot Camp as the percentage of Intel Macs in the installed base continues to shrink.

Using virtualization software works for most users, but there is a performance compromise, though the compromise gets smaller and smaller as time goes by. If you absolutely need to run Windows or Linux natively, you now have a reason to hold on to that Intel Mac – or buy a PC.

Apple pushes out a stealthy security update to macOS

There's a new version of the XProtect antivirus utility. Here's how to get it on your Mac. **Roman Loyola** reports

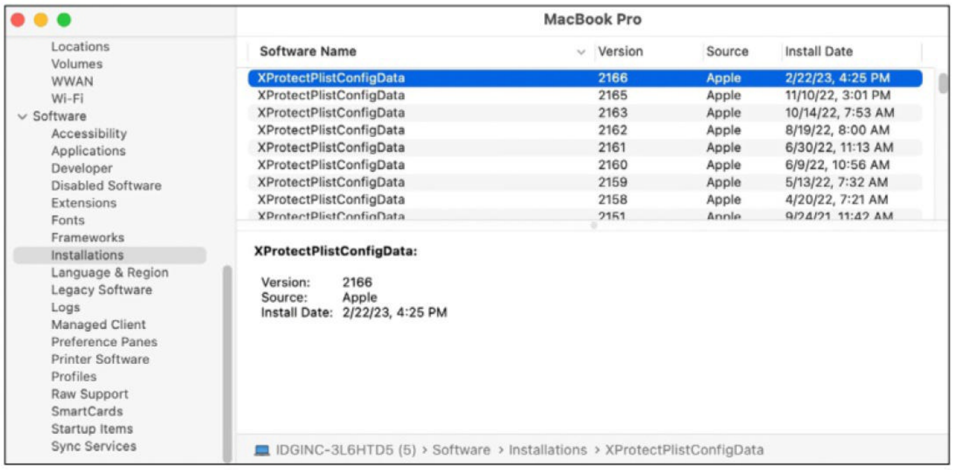
Apple recently updated XProtect (fave.co/3SzySHT), the software built into macOS that protects the operating system from viruses and malware. The update, version 2166, was issued on 22 February, and was installed automatically, which is the usual method for XProtect.

A recent blog post by Howard Oakley (fave.co/3kwfkb4) points out the new version, and although Apple doesn't issue security notes about the update, Oakley says that XProtect was updated with new Yara (fave.co/3IWBYmc) definitions for two exploits, MACOS.KEYSTEAL.A and HONKBOX_A, B, and C. Oakley also says that Apple usually obfuscates the identities of the exploits in its definitions, but this time Apple used their recognized names.

To see if the update was installed on your Mac, you can use the System Information app that's located in Applications > Utilities. Once you launch the app, look for the Software section in the left column, and click on Installations. In the main section of the window, a list will appear, and if it's sorted by Software Name, you can click the header to reverse the list (or scroll to the bottom) to see the entry for 'XProtectPlistConfigData'.

The update is version 2166, and is available for versions of macOS starting with El Capitan.

The update should install automatically, but you can force the installation by using one of the utilities Oakley has created: SilentKnight, which checks if macOS's security has been updated, or LockRattler, which checks if macOS's basic security functions are working. These free utilities can be downloaded from Oakley's website (fave.co/3kplqdn).



Software Name	Version	Source	Install Date
XProtectPlistConfigData	2166	Apple	2/22/23, 4:25 PM
XProtectPlistConfigData	2165	Apple	11/10/22, 3:01 PM
XProtectPlistConfigData	2163	Apple	10/14/22, 7:53 AM
XProtectPlistConfigData	2162	Apple	8/19/22, 8:00 AM
XProtectPlistConfigData	2161	Apple	6/30/22, 11:13 AM
XProtectPlistConfigData	2160	Apple	6/9/22, 10:56 AM
XProtectPlistConfigData	2159	Apple	5/13/22, 7:32 AM
XProtectPlistConfigData	2158	Apple	4/20/22, 7:21 AM
XProtectPlistConfigData	2151	Apple	9/24/21, 11:42 AM

XProtectPlistConfigData:

Version: 2166
Source: Apple
Install Date: 2/22/23, 4:25 PM

IDGINC-3L6HTD5 (5) › Software › Installations › XProtectPlistConfigData

You can see if the XProtect update has been installed in the System Information app.

Credit: Getty Images/Orhan Turan

Best AV software for Mac

AV software is a must if you want to keep your Mac safe. Over the following pages we reveal our favourites. **Karen Haslam** reports

Macs may be a far less tempting target for malware and viruses, but they're not immune from attack. Even if you don't care about adware or being used as means to infect users on other platforms, it's still possible to fall victim to ransomware or password theft.

Accordingly, good antivirus for Mac software will protect your Mac on all of these fronts. It'll catch malware that's still spreading or in circulation; block ransomware; protect older systems with out-of-date software from security vulnerabilities; prevent your Mac from acting as a carrier for malware aimed at other operating systems; and keep infected files off of any virtual machines you're running.

As to the question of which Mac antivirus software you should choose, our current top pick is Intego Mac

Internet Security. However, you will find several other recommendations below that may suit you better, depending upon the type and number of devices that need protection and also how much you want to pay.

Our top contenders in our round up dominate by posting perfect (or virtually near perfect) scores from security research labs, passing our own malware detection tests with flying colours, offering well-designed interfaces, and even throwing in extra features like a firewall or password manager.

DO MACS NEED MAC ANTIVIRUS SOFTWARE?

Plenty of Mac aficionados will tell you that Apple computers are inherently secure and don’t require protection. We’d argue that they are wrong – or overconfident, at the very least.

In 2021, the Silver Sparrow malware was detected on Macs powered by the M1 processor and infected hundreds of thousands of Macs in total. The bad guys, then, are still very much targeting Mac users and they’re getting smarter and greedier. As a result, cybersecurity is something you can’t afford to ignore, and good Mac antivirus is a very good place to start if you want to stay safe.

Macs are generally more secure than their Windows brethren for two reasons. On the technical side, macOS is a Unix-based operating system. As a Unix-based operating system macOS is sandboxed.

Sandboxing is like having a series of fire doors: even if malware gains access to your Mac, it is unable to spread to other areas of the machine. They are more difficult to exploit than Windows PCs, but Macs are not unhackable.

HOW TO CHOOSE THE BEST MAC ANTIVIRUS

Features fundamental to all packages are two ways to find viruses: on-demand protection and via always-on protection. The former finds viruses by examining one file after another during scheduled scans or when you choose to undertake a scan, perhaps because you’re worried your Mac might be infected. The speed at which the Mac antivirus app can do this is important, because some take a long time and also hog the Mac’s CPU while they do so. Waiting six hours to find out if your Mac is infected is neither convenient nor relaxing.

Always-on malware protection is what protects the user outside of the times when scans are run. If

Credit: Getty Images/solarseven

Waiting six hours to find out if your Mac is infected is neither convenient nor relaxing.

some malware arrives, perhaps via an email or a downloaded file, then the always-on protection should be able to detect it and either quarantine it (copy it to a safe folder so the user can decide what to do with it), or simply delete it. Usually a notification is shown when malware is detected in this way, but not all antimalware apps show the same amount of explanation of what's happened – and this was one of the factors we examined in our testing.

Outside of direct malware detection, many security suites include additional tools such as ransomware protection. Ransomware is a type of malware that, once it's infected a computer, encrypts all the user's files and then demands a fee to decrypt them. To protect against this infection, anti-ransomware features typically block any app from writing to a user's home folders, such as Documents or Photos, unless the app's pre-approved (a process called whitelisting). Lots of apps come already pre-approved of course, such as Microsoft Word, or Apple's own Photos app. But you can add others.

Several products also include virtual private network (VPN) add-ons. These protect an Internet connection by encrypting it, and this is useful when utilising unsafe open Wi-Fi such as that provided by a café or hotel. In our experience, these are not replacements for separate paid-for VPN services as many do not unblock video streaming services and some are cut-down versions which constantly nag you to pay extra for the full, premium versions.

Web protection via browser

plug-ins or extensions is also a common component and aims to stop you (or your children) doing anything you regret online, such as visiting fake or infected websites or handing over personal information.

There are usually different options from each vendor, and you get more extras with the top packages, and far fewer with free ones. They might include password managers, parental controls, cloud storage – the list goes on. Generally, the underlying antimalware engine is the same in all products from the same company, so you can save money if you don't need those additional features.

Do bear in mind that all antivirus for Mac apps are sold as yearly subscriptions. That's right, you can't just pay once and use forever. Often there's a hefty discount for that first year's subscription, but this can burn you when automatic renewal occurs a year later and the full retail price is charged: often 100 percent more. Alternatively, you can purchase several years' subscriptions at once for a bigger discount.

Some of the best Mac antivirus subscriptions allow you to install the software on more than one computer (including Windows and Android devices), which can sometimes add significantly to the value – all computers, phones and tablets within a household can be protected with one subscription.

HOW WE TEST

Each software package is evaluated creating a clean installation of macOS, cloning it for each antivirus product and then booting separately into each one to install

Some Mac antivirus subscriptions allow you to install the software on more than one computer.

a different package. This was to ensure that previous app installations didn't interfere with new ones – sometimes AV software treats other AV software as an infection.

In addition to visiting malicious websites, downloading known malicious software and even running said malware, we also reference the most recent reports from two labs that regularly cover macOS malware: AV Comparatives (fave.co/3Izhn4P) and AV-TEST (fave.co/35Cvaco). These laboratories test AV software against sets of known malware as well as products that are grouped as potentially unwanted applications (such as adware).

The latter doesn't damage or expose your computer or its files but may consume power and CPU cycles. Because the testing effectively looks at a combination of virus databases and behaviour, they remain good gauges even after many months. When an antivirus software package lacks a rating from a known security research lab, we do more extensive testing with real malware.

Finally, while we gave props for different features and behaviours, we marked products down if they lacked any or all of the following:

- A nearly perfect score on macOS malware detection.
- Ransomware monitoring.
- Native browser plug-in or system-level web proxy.
- A high score on Windows malware detection.

PRIVACY CONCERNS

Using an antivirus product, especially any that includes tools to also improve your online privacy, may lull you into believing you're safe from personal and private information leaking out. That's not quite the case. While there's no reason to panic, you should consider a few reasonable issues.

First, an antivirus product may upload the complete text of files flagged to the cloud, where it can be analysed by separate tools hosted there. This practice is normal and sensible: Some malware can detect when a running process may examine it, and will then engage in subterfuge. Antivirus software makers also can access their massive databases to examine files with characteristics that trigger their algorithms – certain elements that match known malware. As a result, security researchers discover new viruses, worms, Trojans horses, and the like.

However, helping the greater

good means you'll have to be comfortable with trusting a third-party with your file contents. Where appropriate, we noted privacy policy issues in individual reviews.

Secondly, this software may also rely partly or entirely on cloud-based checks of URLs, malware, and so on. Accordingly, an AV package might upload every URL you visit, metadata about files, signatures of files, information about your computer's hardware, a list of running or installed applications, and more. Companies vary on their disclosure of such policies, and may not let you opt out of this kind of sharing. We note issues in each review as available.

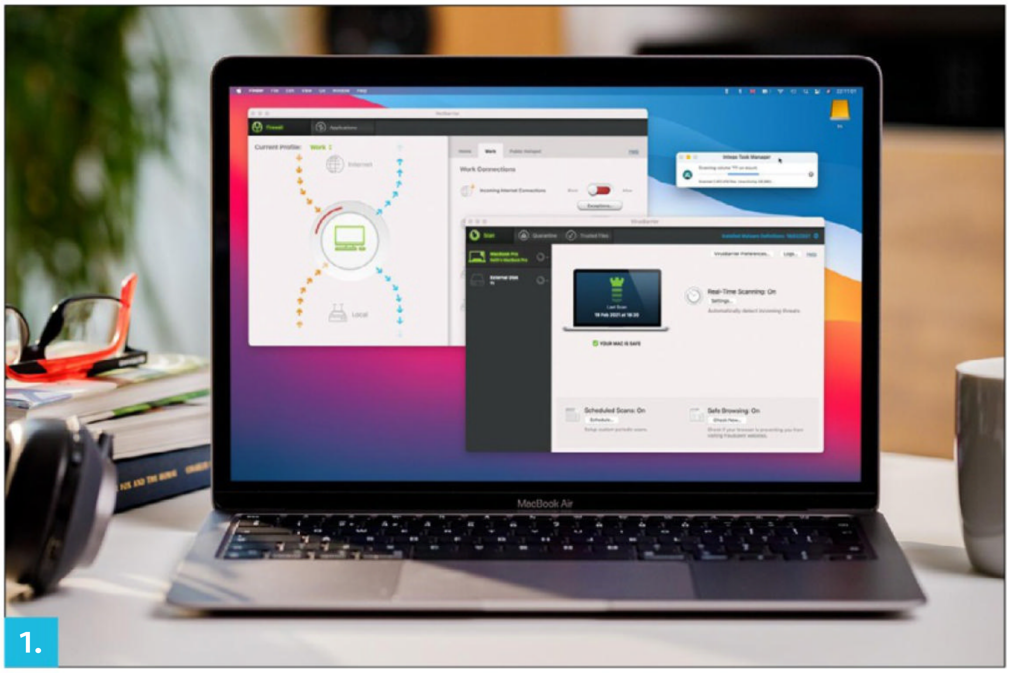
Finally, antivirus software makers also get a sense of what behaviour is happening on your computer that's being monitored or blocked, and may use that information for their own purposes. In some cases, you can opt out of this information gathering.

1. INTEGO MAC INTERNET SECURITY X9

Price: £20.99 per year from fave.co/3ZfMqLO

Intego's Mac Internet Security X9 suite is a pair of utilities designed to help you keep your Mac safe and running smoothly. These are VirusBarrier and NetBarrier, which catch and kill malware threats plus spot potential intrusion attempts from outside as well as outgoing attempts from rogue software.

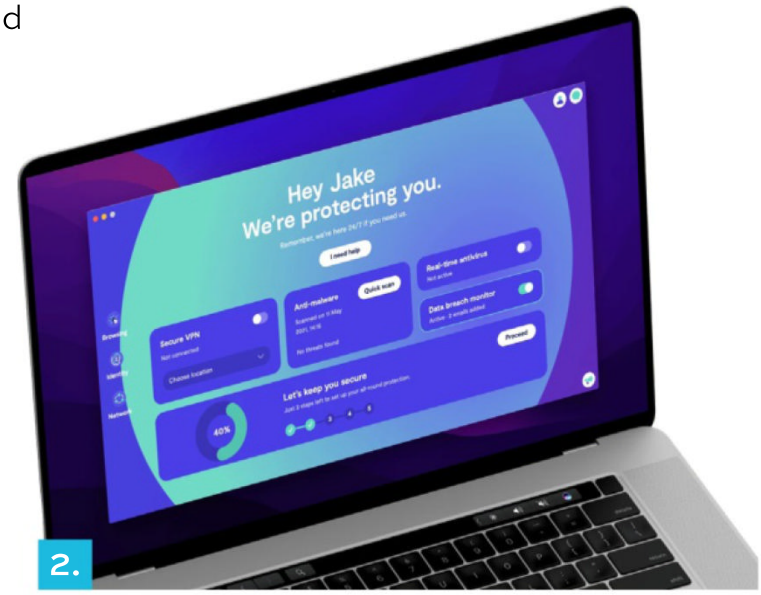
The Mac Premium Bundle X9 adds three more sets of capabilities to these: the backup prowess of Personal Backup (a good 'belt' addition to your Time Machine 'braces'), the useful cleaning, tidying and general speed optimizing



1.

tricks of Mac Washing Machine, and finally the multi-user safe surfing intelligence of ContentBarrier.

Sure, that last one is not something everyone needs, but it's great for parents. Whichever one of these software suites you choose, you can be sure they offer some of the best protection available for your Mac.



2.

2. CLARIO ANTIVIRUS 1.5 FOR MAC

Price: £50 per year from fave.co/3KAJynU

Clario 1.5 for the Mac is much more than an antivirus package, it packs a healthy amount of security into one package, including real-time and on-demand malware scanning, ad blocking and website trackers, a VPN, and data breach monitoring to alert you if your email is caught and potentially exposed in a cyberattack. There's also 24/7 live support.

Payment is by subscription, and currently costs £50 per year (billed at £4.17 a month). The three devices included in the plan can include a combination of Macs and iOS or Android devices. There's also a seven-day free trial.

Set up is quick and painless with a wizard that takes you through configuration of all the key features while allowing you to evaluate the different options and determine which ones you want to enable. Once installed you can access information about the security of your Mac and monitor the status of your online accounts and personal data. The VPN will kick in if Clario detects you using an unprotected network. And from the Dashboard you can trigger a quick virus scan, which is actually quite thorough. We did encounter some issues with performance, with the program sometimes running slow before we were fully set up, but once we were fully configured everything ran smoothly.

Whether you're a novice or advanced user, Clario is an effective and supportive security program.

3. AVG ANTIVIRUS FOR MAC

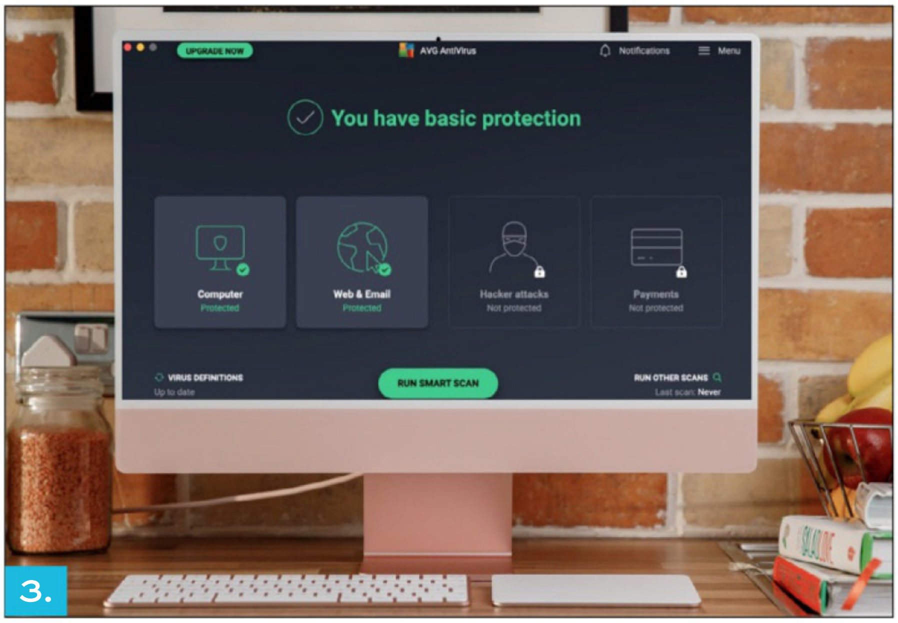
Price: Free (paid upgrades available) from fave.co/3WzFS8A

AVG Antivirus for the Mac is one of a handful of free antivirus for Mac programs. As such it is basic, but its effective at protecting you from viruses, spyware, and malware.

Despite being free, AVG covers all the bases: blocking viruses and malware from websites, downloads and email attachments. AVG will scan applications and check every file and remove threats from your Mac. It auto updates so you shouldn't miss out on protection from the latest threats.

Though it lacks the advanced features of paid antivirus products, it handles the core tasks cleanly and seamlessly. However, if you need to resolve any advanced issues you will need to pay to upgrade to the full version of the software, which is about £2 per month for a one-year subscription. There is a 60-day free trial though, which could be enough for your purposes.

All in all this is a great option, despite being basic. You get much more than you 'pay' for.



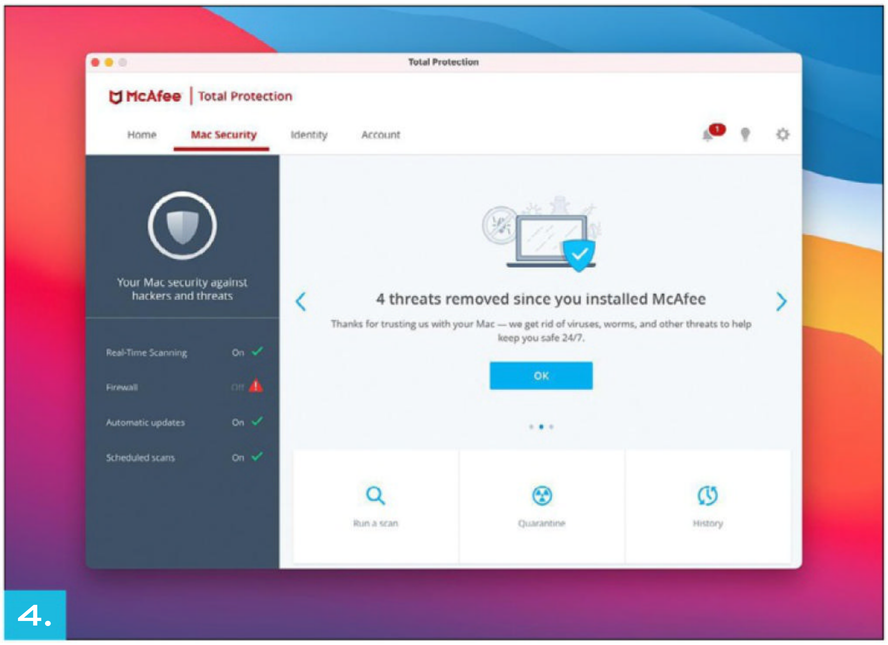
3.

4. MCAFEE TOTAL PROTECTION

Price: £34.99 per year from fave.co/3kzPaUL

McAfee Total Protection is a dedicated software security tool that will monitor your Mac as you work, looking for unauthorized software activity such as browser search engine hacks, attempts to trick you into installing unwanted software, and actual malware and virus attacks.

It is very simple to use; once you've walked through the guided steps for giving it permission to work behind the scenes it is essentially something you can just leave to get on with its job.



Your Mac security against hackers and threats

Real-Time Scanning On ✓

Firewall Off ⚠

Automatic updates On ✓

Scheduled scans On ✓

4 threats removed since you installed McAfee

Thanks for trusting us with your Mac — we get rid of viruses, worms, and other threats to help keep you safe 24/7.

OK

4.

Total Protection also offers WebAdvisor as an option, steering you from known problem sites and warning you when you visit questionable ones. It also offers a software firewall for two-way network traffic monitoring.

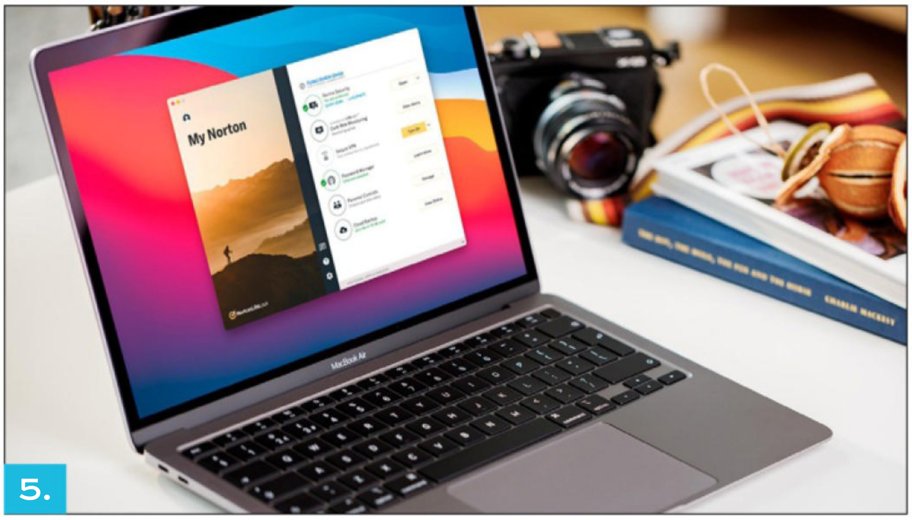
We noted some occasional performance impacts as it ran in the background, but it was largely unobtrusive in its efforts. The option of protecting other devices is useful as well, covering smartphones and Windows PCs as you require. It's worth adding that the Windows version in particular offers more features, such as a native VPN, which you don't get in the Mac app.

5. NORTON 360 DELUXE

Price: £29.99 per year from fave.co/3ITpRq1

Norton 360 Deluxe is a security utility that performs a range of different monitoring and safeguarding operations to keep your Mac free from threats such as browser hacks and search engine hijack scripts to intrusion attempts and actual malware.

It focuses on catching unwanted software, but it also offers some useful additional features including a VPN for securing personal data



5.

while online, and a tool for managing passwords, bank card details and similar data.

There are three different versions, two of which can also be used to secure your iPhone as well as Android smartphones and Windows PCs, should you require that. In tests it proved to have little to no detectable impact on performance, and it spotted all the challenges in our test macOS set-up.

Note that the Cloud Backup feature doesn't work on macOS, but that is more of an extra rather than a vital part of the package.

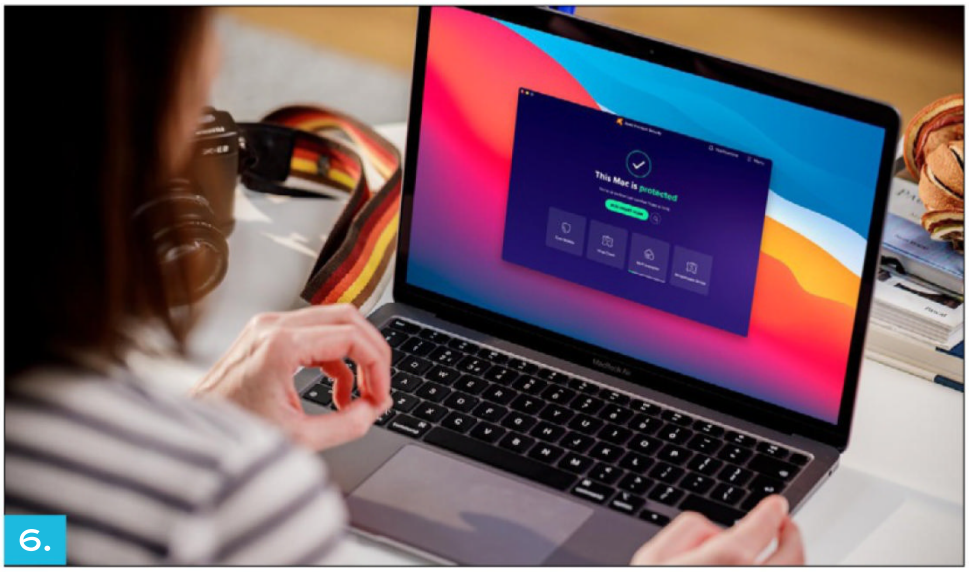
6. AVAST PREMIUM SECURITY

Price: £27.99 per year from fave.co/3Szre0m

Avast Premium Security for Mac does its job well overall. There are a few niggles such as the unwanted upselling for Cleanup Premium and the fact that the File Shield monitoring slows down file copy times a bit.

Otherwise, it's a well-featured suite which will protect from all sorts of nasties including watching for browser script hacks, potential ransomware and other remote attack activity. It will, of course, also scan for potentially unwanted programs and actual malware threats, whether on your Mac or your removable media or in email attachments.

Custom scheduled scans can be set up, although the automatic background monitoring teamed with occasional specific manual scans is likely to be enough for most requirements. Wi-Fi network monitoring for vulnerabilities is another feature this software offers, and the Real Site option watches for fake sites pretending to be legitimate shopping or banking sites, a serious risk that goes beyond just watching for unwanted files on your own Mac.



6.

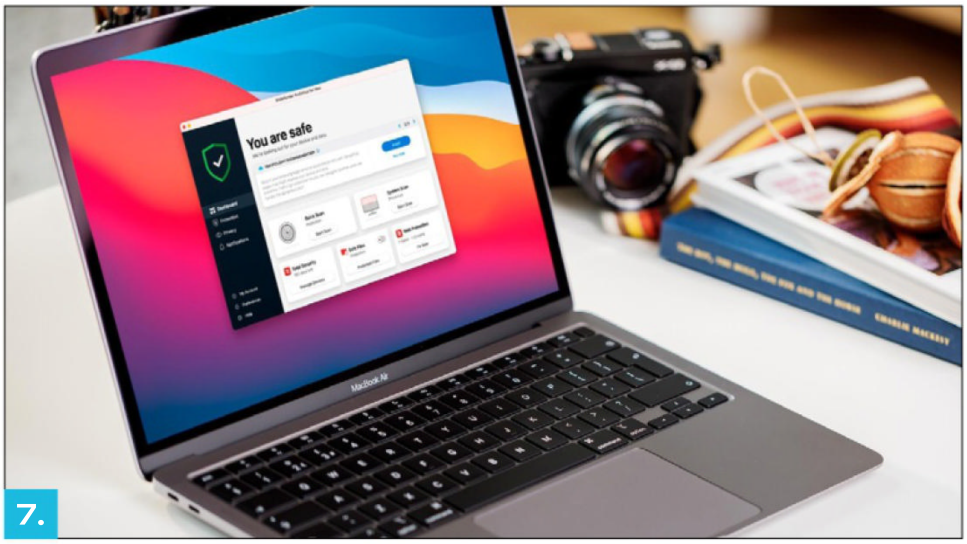
It is very effective at all these things, although we found that customising its behaviour can be a little fiddly.

7. BITDEFENDER TOTAL SECURITY 2021

Price: £34.99 per year from fave.co/3yeHuL3

Bitdefender Total Security is a very effective tool for keeping your Mac safe, and it will also protect Windows PC, an iOS and Android devices. The bundled VPN is very basic and gives you only 200MB of data per day, but the rest of the suite of tools is effective and easy to manage.

But when you compare what the Mac version offers compared to the Windows version, you'll feel quite hard done by. There's no password manager, no social network protection, no webcam or microphone protection, no Wi-Fi security advisor and plenty of other features that Windows users get for the same price.



7.

Bitdefender is also lagging behind its rivals with no identity protection. If your goal is simply to keep your Mac protected from malware, then Bitdefender does a great job. But you can find better value elsewhere.

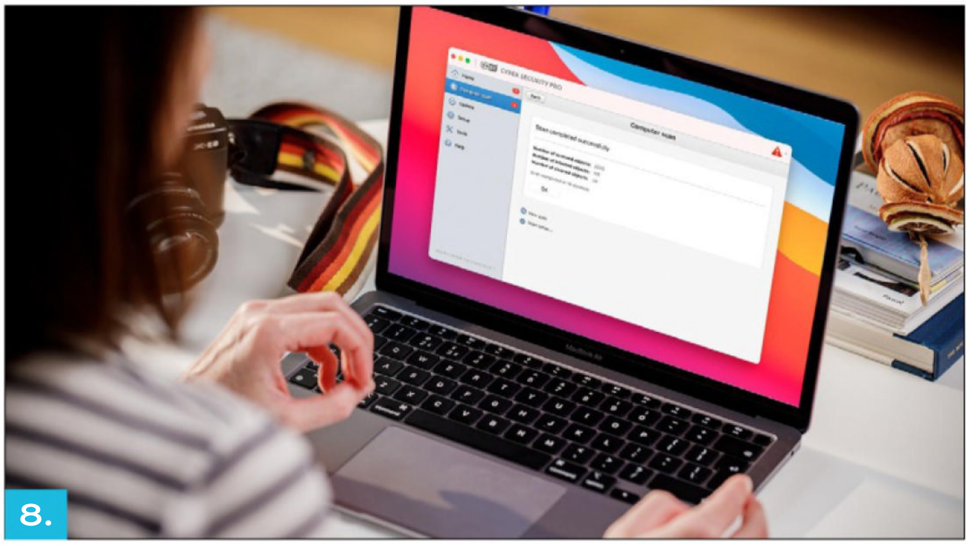
8. ESET CYBER SECURITY PRO

Price: £39.90 per year from fave.co/3xTrwWk

Eset Cyber Security Pro is a useful security tool that protects your Mac – and your Windows PC, Linux box and even Android phones, although not your iPhone – against unauthorized software behaviour, network intrusions, search engine hijack scripts and worse.

It stands out from its competition through its comprehensive range of preferences controls that can fine-tune many aspects of its behaviour, and its relatively low price.

It isn't the most unobtrusive in



8.

terms of background performance impact, although most of the time this was minor enough to be not really noticeable.

As well as real-time and on-demand monitoring it also provides a useful firewall, dedicated tools for spotting web-based threats including spyware, and protection against phishing attempts to trick users into divulging private data. It also offers parental controls with three user categories and detailed control over what kinds of sites each user is allowed to visit.

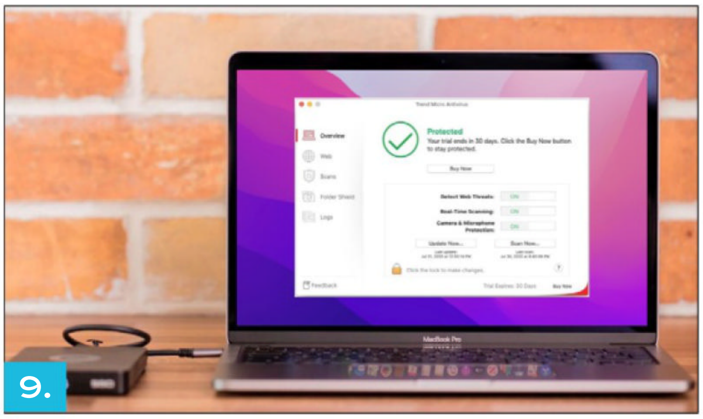
9. TREND MICRO ANTIVIRUS FOR MAC

Price: £19.95 per year from fave.co/3Z6CPX7

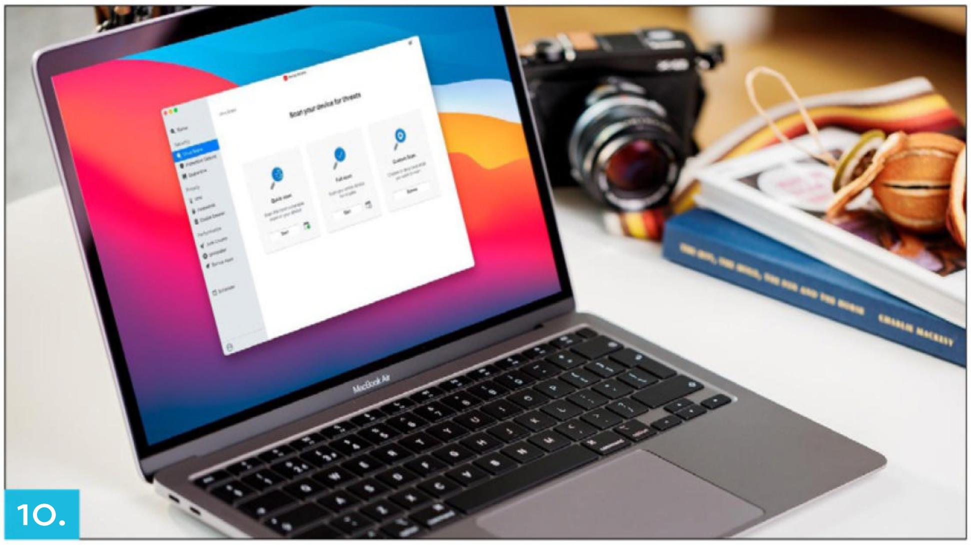
Trend Micro Antivirus is a good program with well rated antivirus protection, and a simple, straightforward interface that users will appreciate. Anyone looking for additional features will be disappointed with this suite, but it offers good protection at a fair price.

In March 2022 AV-Test gave Trend Micro Antivirus for Mac a 99 percent protection score against 200 samples. Our own spot checks produced similarly good results. Lining up against the Objective See malware library Trend Micro had no trouble detecting most threats. However in a few cases it didn't detect all the malware contained in a folder until a scan had been run.

Trend Micro is an excellent choice for those looking for something that's



9.



10.

simple and easy to use. There are options with better protection, but Trend Micro's protection is still good and pricing is fair.

10. AVIRA PRIME

Price: £51.99 per year from fave.co/3KG3lSH

Avira Prime is a security utility designed to keep your Mac safe from potentially unwanted programs; which covers everything from simple scripts designed to compromise and redirect your browser searches through to actual malware.

A single large window presents the various features, from scans to app management and clean-up, although a couple of its features use a separate panel for a web-based console. In our tests it detected all our compromised files and installers.

It doesn't look inside zip archives or disk images, but it pounces as soon as items are extracted from these. Most importantly, even while Avira Prime is actively scanning for trouble it has such a small impact on the general performance of our Mac that we wouldn't notice it without comparing timings. You can get the basics of the security features with Avira Free Security but Prime's annual subscription provides useful additional capabilities, if you can stomach the high cost.

Credit: Getty Images/Sakorn Sukkasemsakorn

Best password manager

Password managers are an essential tool for using the Internet. Here are our top picks. **Martyn Casserly** reports

You probably have a lots of online accounts, and in order to remember your login details you are quite likely to reuse those same few passwords over and over again. It's perfectly understandable, but definitely not safe.

We know that it's important to use an original password for each account and update them on a regular basis, but it can be a Herculean task trying to retain that information in our heads. This is made even more challenging with different sites requiring specific mixtures of characters: this one demands at least two symbols and no capitals, while that one requires a mixture of cases and a minimum length.

That's where password manager apps come in. They allow users to create one master password, after which the app takes care of logging into all other accounts. Having only a single login to remember? That sounds good to us.

HOW PASSWORD MANAGERS WORK

The idea of password managers is to simplify the way you access your various accounts. Instead of having to memorize multiple complex passwords for each of the services you use you need only recall one password and then the password manager will automatically fill in the required details for you.

The managers also offer various other features. For example, they can generate random, highly secure passwords for your accounts, they can warn you if your password has been compromised, and some can advise you about existing insecure passwords and support your efforts to update them.

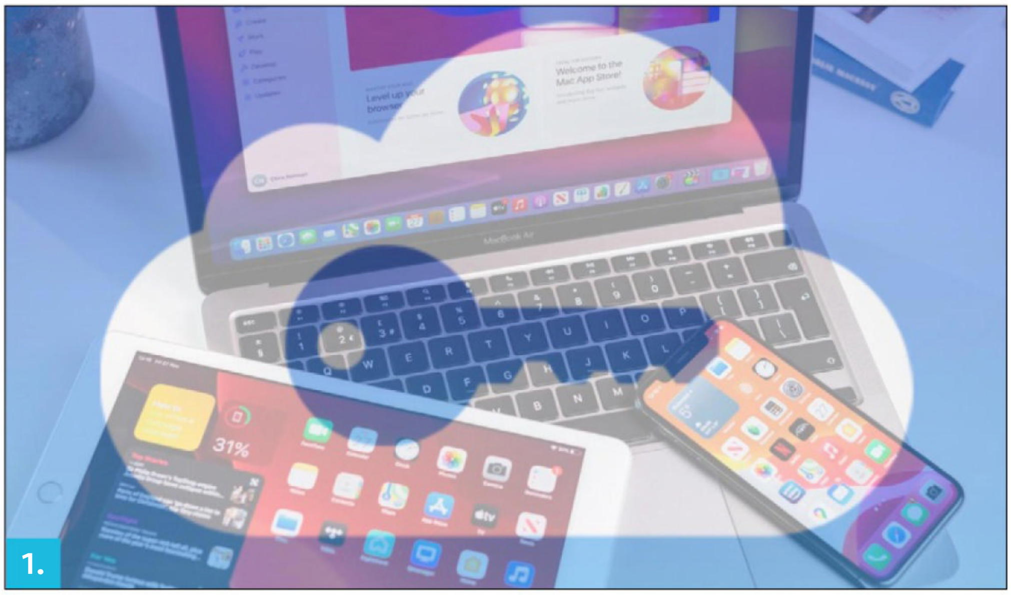
Obviously, security is a high priority – as the manager apps have the virtual keys to your kingdom – which is why all of the options listed below use high-grade encryption to protect your details.

Many also feature digital wallets so your bank details can be safely stored and then used to make purchases online without having to root around in your pocket or bag for the card number and expiry date.

These services don't usually come for free, but many offer trials so you can see if it's the solution for you. After that you'll need to pay a small monthly fee, but we think that's a price worth paying for only having to keep one password in your brain.

Of course, Apple does have a password manager in macOS (and iOS and iPadOS) in the form of iCloud Keychain. It will even generate secure passwords and enter them for you automatically, all while storing them securely away from hackers and generally naughty people. iCloud Keychain is incredibly useful, but it's a bit basic and lacks some of the features offered by other password managers.

So, if you want to stay safe without having to recall hundreds of passwords, but want more control and features than you get from Apple's free offering, here are some of the best alternatives available on the Mac.


1.

1. iCLOUD KEYCHAIN

Price: Free from fave.co/3Zku6Rv

There are lots of password managers available, but you may be wondering if you really need one, as Apple already includes a free one with your Mac.

iCloud Keychain is Apple's own password management system and it is built into macOS and iOS. It helps you to create secure passwords by generating them on your behalf, warns you if you reuse one or if a password is not secure, and, crucially, auto-fills your passwords when needed. It's all tied to your Apple ID login and password and the Apple devices you have registered for two-factor authentication, plus everything is encrypted, so it should be secure.

It doesn't just fill in passwords for you though: it also enters your logins, emails, credit card numbers and address details. So you can effortlessly go to sites, choose the item you want to buy, then complete the transaction in seconds and without needing to dredge your memory or fill in loads of text boxes first.

However, one of the main disadvantages is that iCloud Keychain only works on Apple devices. If you have an Android phone or use a Windows PC, iCloud Keychain is redundant and you will need to find your password information up and enter it manually. Even if you are using Apple devices, iCloud Keychain is only available through the Safari browser, so if you prefer to use Chrome, FireFox, or any other browser, you'll have to painstakingly look up your Netflix password.

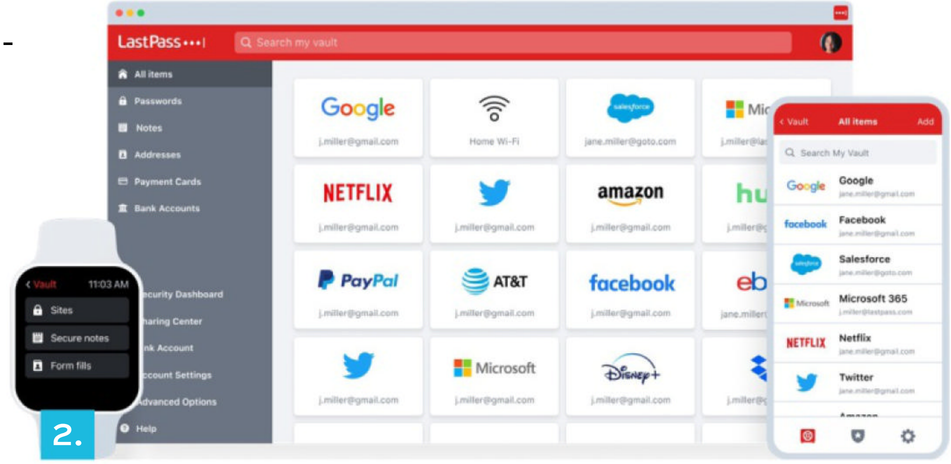
There are a few other areas where iCloud Keychain lacks flexibility, such as not helping you update passwords or telling you when they've been exposed in any security breaches. So, it's pretty much a manual solution for those who only use Apple devices and software. Luckily there are alternatives if you want a little more room to move.

2. LASTPASS

Price: £31.20 per year from fave.co/3m7LslG

LastPass is probably the best-known password manager, thanks to it being one of the original pioneers in the field. The company places a strong emphasis on security, trumpeting the use of 'AES 256-bit encryption with PBKDF2 SHA-256 and salted hashes to ensure complete security in the cloud'.

The app does all of its encryption locally, so LastPass never knows your master password, and the Premium tier also supports a form of two-factor authentication for another layer of security. This is called MFA (Multi-Factor Authentication) and not only allows confirmation text messages to be sent, but also works with biometrics (Face ID & Touch ID) and even voice commands (although some of these methods are reserved for the Business plan).



2.

You can either use LastPass locally on your device via dedicated apps (macOS, iOS and iPadOS), or via the web with plug-ins and extensions available for Safari, Firefox, Chrome, Opera, and Microsoft Edge all of which allow you to automatically access login details for sites and accounts or have LastPass autofill the login fields on your behalf.

Just like with other managers you have access to a vault where all of your passwords are stored, and these can be changed to more complex alternatives at the touch of a button. LastPass will also advise you on how secure your passwords are for your existing accounts. Getting set up is easy too, as you can import existing passwords from web browsers, email, and other password managers.

The app offers a digital wallet to store your card details, plus another area for official ID such as passports and driving licenses. The Note section is a place where you can keep Wi-Fi passwords, insurance details and any other important documents that you need to access. It's also possible to securely share account details and logins with friends and family, even if they don't have LastPass.

There is a free tier, although this is limited to one device, so if you want to sync across your Mac and iPhone you'll need to move up to the Premium tier. At the time of writing, this will cost £31.20 per year. Those wanting more scope can opt for the family plan which includes six user accounts and only costs £40.80 per year on the LastPass website.

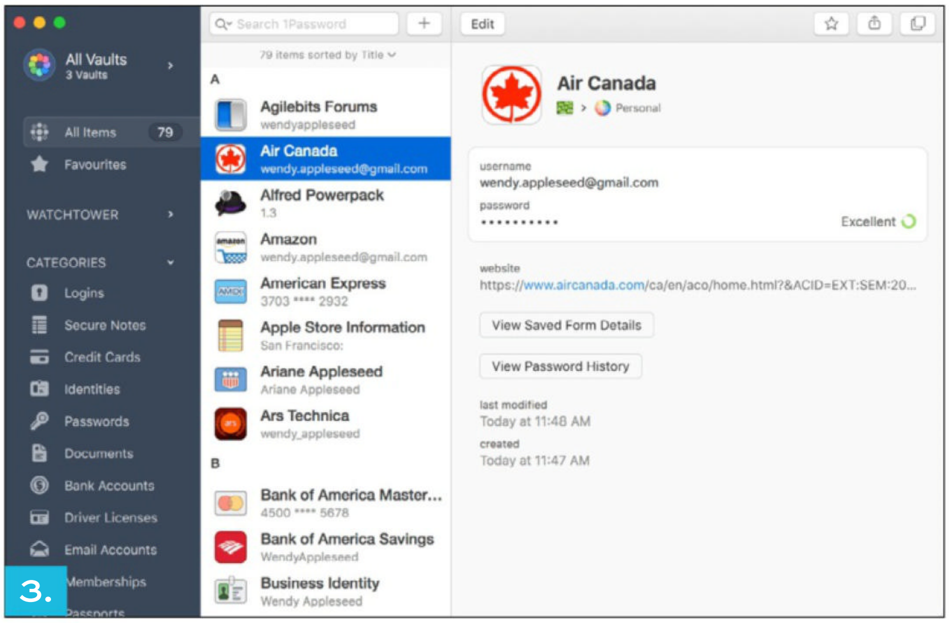
One of the advantages of a paid plan is an Emergency backup which means that, should you suffer an accident or even pass away, your family will be given access to your account.

3. 1PASSWORD

Price: £32.99 per year from fave.co/3xWN04M

Another long-standing favourite is 1Password. Much like the other offerings on this list the app comes with the standard vault that you access via a master password, and in which you can see and update your various account login details.

A free 30-day trial is available, but after that you'll need to move onto a paid subscription that currently costs £32.99 per year. For this you'll be able to use the software on as many devices as you like, including macOS, Windows, ChromeOS and



A
Agilebits Forums
wendyappleseed
Air Canada
wendy.appleseed@gmail.com
Alfred Powerpack
1.3
Amazon
wendy.appleseed@gmail.com
American Express
3703 **** 2932
Apple Store Information
San Francisco:
Ariane Appleseed
Ariane Appleseed
Ars Technica
wendy_appleseed
B
Bank of America Master...
4500 **** 5678
Bank of America Savings
WendyAppleseed
Business Identity
Wendy Appleseed

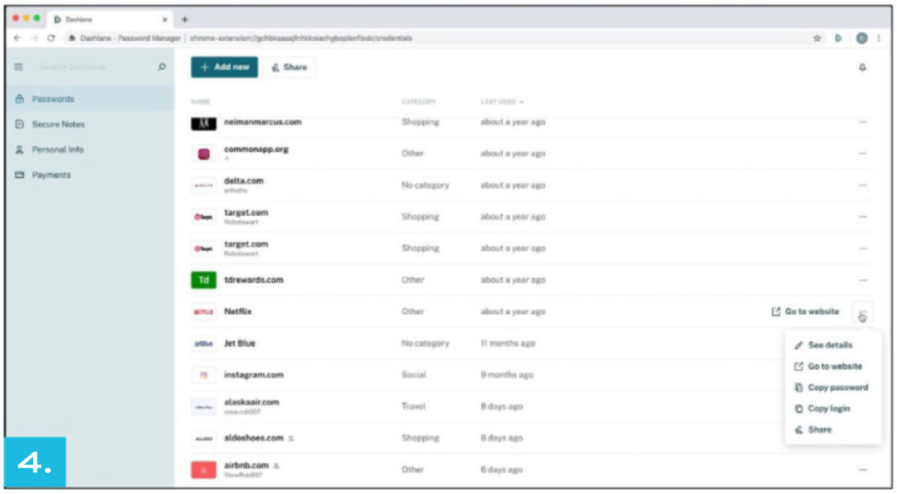
Air Canada
Personal

username
wendy.appleseed@gmail.com
password
••••••••••• Excellent

website
https://www.aircanada.com/ca/en/aco/home.html?&ACID=EXT:SEM:20...

last modified
Today at 11:48 AM
created
Today at 11:47 AM

3.


4.

NAME	CATEGORY	LAST USED
neimanmarcus.com	Shopping	about a year ago
commonapp.org	Other	about a year ago
delta.com	No category	about a year ago
target.com	Shopping	about a year ago
target.com	Shopping	about a year ago
tdrewards.com	Other	about a year ago
Netflix	Other	about a year ago
Jet Blue	No category	11 months ago
instagram.com	Social	9 months ago
alaskaair.com	Travel	8 days ago
aldoshoes.com	Shopping	8 days ago
airbnb.com	Other	6 days ago

Linux, plus the accompanying iPhone and Android apps.

The Family tier costs £54.99 per year and includes five premium accounts and 1GB of secure storage. This does make it appear a little more expensive than some of the other services on this list, most of which have six accounts in the Family package.

Security is again front and centre, with 1Password boasting end-to-end encryption so only you will hold the key to your account. AES 256-bit is the order of the day, and 1Password monitors the activity on your account so it can send you warnings if any odd behaviour is spotted.

One interesting new feature is Travel mode. This allows you to completely remove certain information from your device when going abroad. In these strange times, this could prove very useful if you're passing through some of the rather aggressive customs checkpoints that now demand access to your devices. The best part is when you get home again everything can be restored by flicking a switch in the settings.

1Password has won numerous awards, and is always an easy service to recommend.

4. DASHLANE

Price: Free (paid upgrades available) from fave.co/3Z32rEs

Dashlane is a popular password manager, with a comprehensive suite of tools to make your life a lot easier. Once set up, Dashlane can pull any stored account details you might have in your browsers, making them available in the dashboard area where they can be viewed and managed.

The app analyses your current passwords to see how secure they are, and gives you an overall rating based on how often you reuse login details for multiple sites. There's also a feature to auto-replace passwords instantly with ones generated by Dashlane.

The app now works primarily on the web, with extensions available for Safari, Chrome, Firefox and Microsoft Edge. You still access a fully featured app, where you can see the password health monitor and upload your secure notes and IDs, but it's online. The extensions are much smaller tools there simply to auto-fill your passwords and payment details on websites.

Credit card and PayPal details can be stored in the Payments section of the app, Plus there's a section for digital versions of your passport and other IDs. There's also a section for any secure notes you wish to keep safe.

One of the newer features included is a VPN that you can use to keep your online activities even more secure, especially when using public Wi-Fi services.

The clean, clear interface for Dashlane means it's easy to set-up and use. The fact that it also features AES 256-bit encryption makes it a very good option if you're new to password managers.

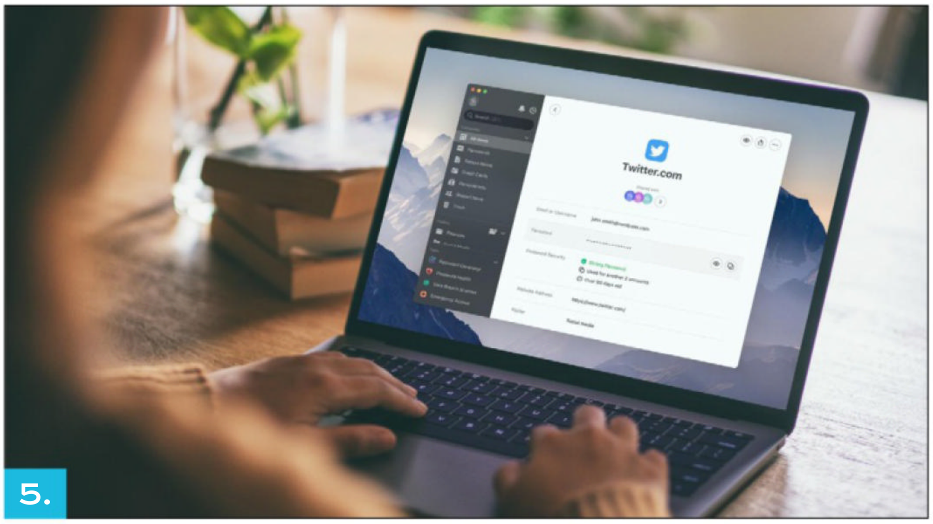
The free tier allows the service to be used on one device and a maximum of 50 passwords, but if you want to sync your passwords to your phone and tablet too then the Premium tier will set you back £29.99 per year. If you want to cover your entire household, then the Family tier includes six premium accounts all for £49.99 per year.

5. NORDPASS

Price: £20.28 per year from fave.co/3KCkxss

One of the newest additions to the password manager arena is NordPass, which is made by the same fine fellows at NordVPN. The latter is one of our favourite VPNs, as you'll see from our Best VPN for Mac round-up (see page 44).

NordPass has grown quickly over


5.

the past couple of years, and now offers full desktop apps for macOS, Windows, and Linux, plus the standard iOS and Android offerings. You can also use NordPass through browser extensions for Chrome, Firefox, Opera, Brave, Microsoft Edge and Safari.

NordPass has all the features you'd expect from a modern password managers, with quick importing of existing passwords from other services, zero-knowledge architecture, local encryption, 2-factor authentication, password generation, secure storage for credit details and notes, autofill for logging into accounts, folders to store passwords for work, home or other classifications, security monitoring for password hacks, support for biometrics, plus a neat interface to manage all of your various data.

Prices are very reasonable, at £22.68 per year for the Premium plan, and the five-account Family plan for £44.28 per year. There is a free tier, which supports unlimited passwords, stores credit card details and secure notes, plus has the ability to sync across all your devices. The main drawback is that you can only be logged into one device at a time. But if you can work with that it's a service you should definitely investigate.

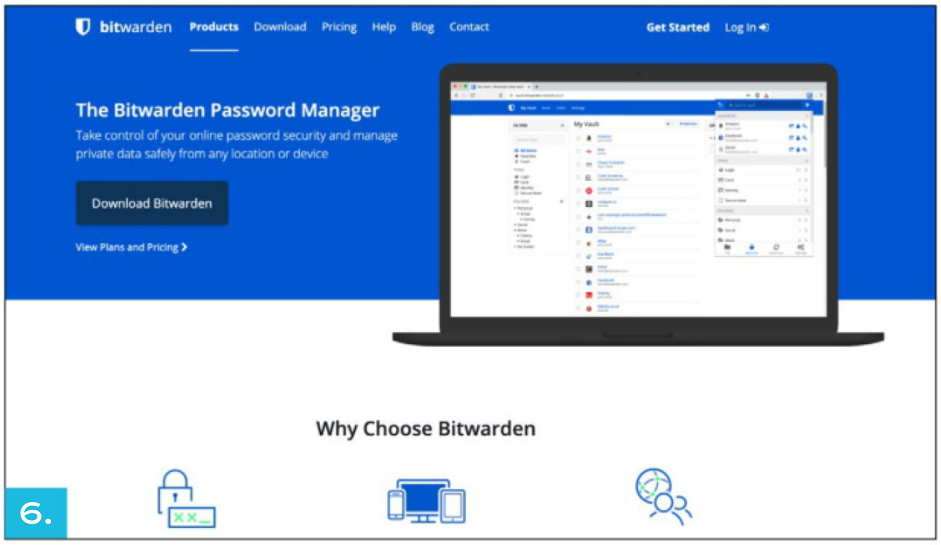
6. BITWARDEN

Price: Free (paid upgrades available) from fave.co/3KY2rl1

When it comes to technology, we often say that you get what you pay for, but in the case of Bitwarden this isn't quite true. The service offers a really impressive range of capabilities on it's free tier, so with this app you get what you don't pay for.

Without signing up to a premium account you get unlimited storage for passwords, credit cards, notes and online account IDs, secure text messaging with individuals, a secure password generator, two factor authentication, plus the ability to either have your data stored on the Bitwarden servers or one you host yourself. Oh, and you can sync all your devices, rather than the single one offered by most other free tiers.

Should you want to expand the features, then the Premium tier costs £8 per year and adds secure files sharing, 1GB of encrypted file attachments, additional two-factor authentication options, password safety analysis, and access to your account by family if you die or become sick. The Family plan offers



The Bitwarden Password Manager

Take control of your online password security and manage private data safely from any location or device

Why Choose Bitwarden

6.

all of this for six Premium accounts and costs £30 per year, making it cheaper than several of the individual plans currently available.

Encryption is high-grade stuff, with Bitwarden deploying end-to-end AES-256 bit encryption, salted hashing, and PBKDF2 SHA-256, all of which is down locally on your machine.

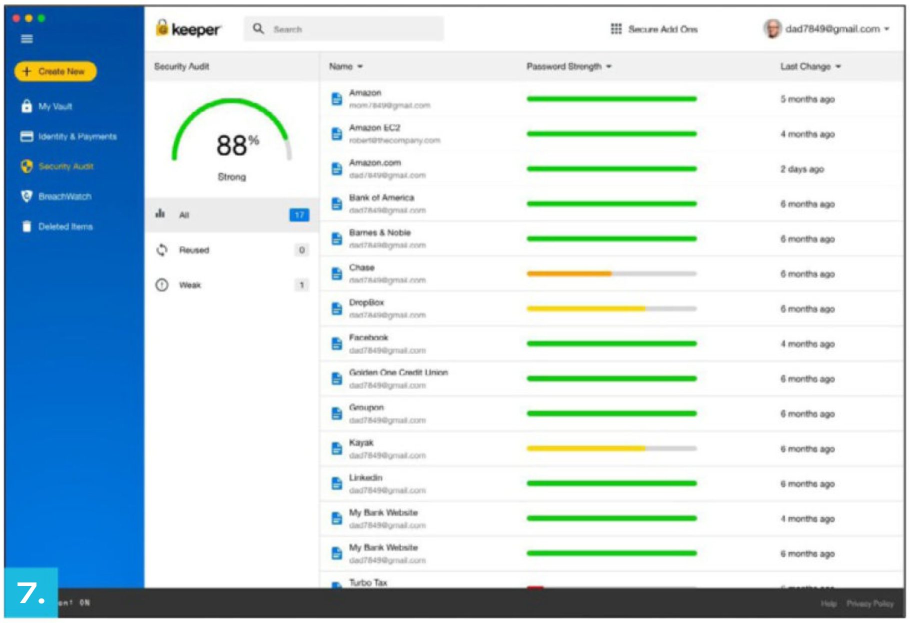
Apps are available on a wide range of platforms, including macOS, Windows, Linux, pretty much every browser you can think of, Android, iOS, and there's even a secure web version if you find yourself without your device.

If you're looking for the value when it comes to Password Managers, it's very hard to look past Bitwarden.

7. KEEPER

Price: £30 per year from fave.co/3xS8WoS

Keeper provides its services to millions of customers around the world. This doesn't come as a surprise when you see the feature list and general polish that the app contains. You can store unlimited passwords, have Keeper auto-generate strong new ones, and sync passwords across multiple devices, all while holding credit card details and other important payment



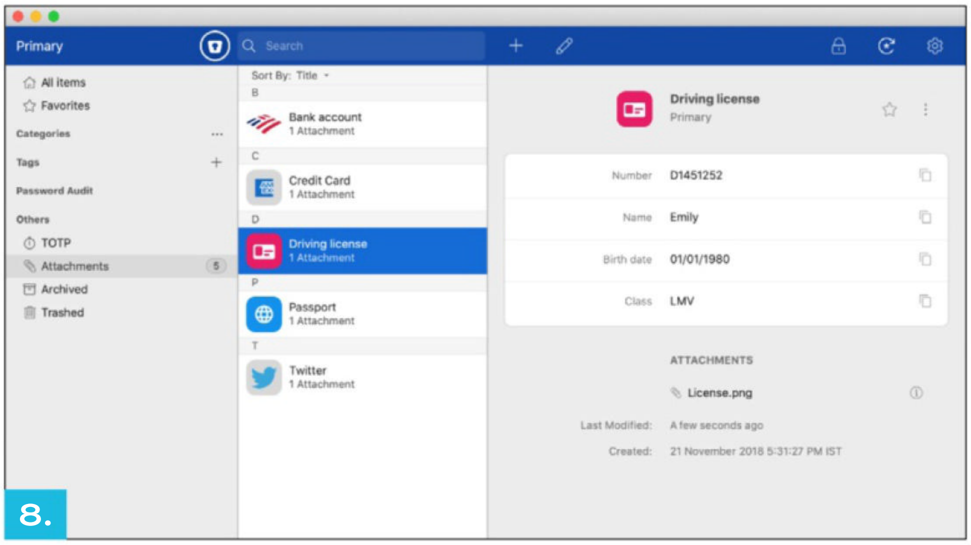
Security Audit

88% Strong

All	17
Reused	0
Weak	1

Name	Password Strength	Last Change
Amazon mom7849@gmail.com	🟩	5 months ago
Amazon EC2 robert@thecompany.com	🟩	4 months ago
Amazon.com dad7849@gmail.com	🟩	2 days ago
Bank of America dad7849@gmail.com	🟩	6 months ago
Barnes & Noble dad7849@gmail.com	🟩	6 months ago
Chase dad7849@gmail.com	🟧	6 months ago
DropBox dad7849@gmail.com	🟨	6 months ago
Facebook dad7849@gmail.com	🟩	4 months ago
Golden One Credit Union dad7849@gmail.com	🟩	6 months ago
Groupon dad7849@gmail.com	🟩	6 months ago
Kayak dad7849@gmail.com	🟨	6 months ago
LinkedIn dad7849@gmail.com	🟩	6 months ago
My Bank Website dad7849@gmail.com	🟩	4 months ago
My Bank Website dad7849@gmail.com	🟩	6 months ago
Turbo Tax	🟥	6 months ago

7.



Bank account
1 Attachment

Credit Card
1 Attachment

Driving license
1 Attachment

Passport
1 Attachment

Twitter
1 Attachment

Driving license
Primary

Number D1451252
Name Emily
Birth date 01/01/1980
Class LMV

ATTACHMENTS
License.png

Last Modified: A few seconds ago
Created: 21 November 2018 5:31:27 PM IST

8.

details in its secure vault.

AES 256-bit encryption is all performed locally, so Keeper can never know your details, but there is the option to securely share folders and passwords with friends and family if they need to access any of your accounts. The included secure messaging service is also useful for communicating these requests

There's also support for Touch ID on the Mac and iPhone, with the latter also working with Face ID, plus Apple Watch compatibility and the option of using two-step authentication.

Keeper Unlimited Password Manager is available for £29.88 per year from fave.co/3KY2VYn, but there's also the Family tier that includes five premium accounts, plus 10GB of secure storage for £72 per year. If you want even more protection with the Breachwatch service that monitors password hacks and dark web activity, then there's the Keeper Plus Bundle that will set you back £50.72 for a single account or £95.88 for the Family plan from fave.co/3ZrrCQy.

8. ERPASS

Price: Free (paid upgrades available) from fave.co/3IWP8Q1

Those looking for a simple, secure solution that doesn't break the bank would do well to consider Enpass.

The macOS client is completely free, but if you want to add the same features to your iPhone or Android device then you'll need to move to the Enpass Premium tier that costs £19.49 per year from fave.co/3IxhS0E. There's also a Family tier that offers six Premium accounts (fave.co/3IxhS0E) for an introductory price of £29.24 for 12 months, then increases the price to £38.99 per year. If you prefer to buy a lifetime licence for yourself, you can pick one up for £82.99.

Enpass doesn't store any of your information on its servers. Instead, everything is encrypted and kept on your personal device so you never lose control of your data. Details can be synced securely via iCloud, Dropbox, OneDrive, Google Drive, Box or ownCloud/WebDAV, to keep all of your devices in step.

You still have the classic features of other password managers, such as auto-fill forms, security analysis of your passwords and generating complex replacements easily, secure storage for sensitive information and AES 256-bit encryption, plus support for iOS, Android, and Apple Watch devices.

There's plenty of fine tuning options for those who are a little bit more hands-on, but we like the no-nonsense approach and the fact that your data never leaves your device.

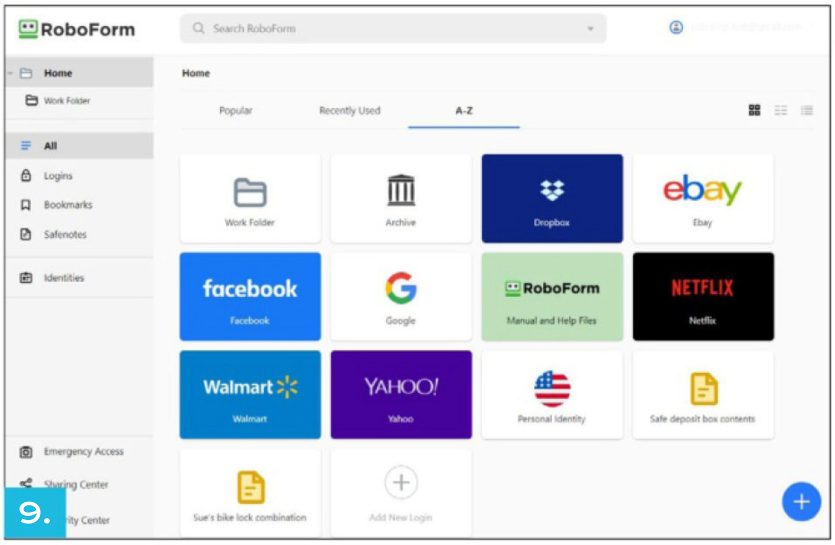
9. ROBOFORM

Price: £14.20 per year from fave.co/3Y1evEJ

Another long-standing favourite is Roboform. Like its rivals in this list, the service offers a wide range of features that make life easier for you when interacting with sites online. There's end-to-end encryption, auto-filling of account details, new password generation, a security suite to monitor and advise you of the current health of your passwords, cloud syncing to keep all your devices up to date, multi-factor authentication, secure sharing, folders and search features to organize your passwords, plus emergency access which allows family members to access your account if you should fall ill or pass away. There's secure storage for your credit cards and IDs, not to mention notes, contacts, and even your browser bookmarks, which is something we haven't seen on other services.

Roboform is available for macOS, Windows, Linux, iOS and Android, or you can use the browser extensions provided for Chrome, Safari, Firefox and Microsoft Edge.

Prices are very affordable, with the free tier actually being quite decent as it provides unlimited password storage, auto-fill, secure sharing and other basic features, albeit for a single device. To take advantage of all the capabilities Roboform has to offer you'll want the Everywhere tier that costs a very reasonable £14.20 per year and works across


9.

all your desktop and mobile devices. It's worth considering the three-year deal which is £42.60 which works out not that much more than many of the 1-year subscriptions offered by other companies.

There's also a family package that gives you five Everywhere accounts for £28.40 for a year or you can opt to pay £85.20 to have the service for three years – see fave.co/3Y7p753.

If you're looking for the best bargain, then Roboform is certainly in the running.

Credit: Getty Images/Prykhodov

Best VPN for Mac

Protect your privacy online. **Anyron Copeman** reports

A VPN (virtual private network) is an essential tool nowadays, regardless of which device you use. With the increased popularity of VPNs has come an increased number of VPN providers vying for your business. That makes finding the best one to suit your needs difficult. To help you sort out the right provider for you, we've committed to extensive research and testing of VPN services that cater to Mac owners in our guide to the top VPN services for Mac.

With the Internet abuzz with privacy concerns and the potential changes coming to net neutrality, you've likely heard about VPNs before. When used correctly, a VPN can greatly strengthen your online privacy, assist in keeping your personal information secure, and even spoof your location in the world – allowing you to access websites or services that would otherwise be off limits due to region-locking.

Indeed, one of the most popular reasons to use a VPN outside the US is to get access to blocked online content, such as foreign Netflix libraries. With a VPN you can watch BBC iPlayer while outside of the UK, or access US Netflix from the UK, for example.

While Macs are generally considered to be more secure than PCs, VPNs are still useful for Mac users because it affects the connection between your Mac and the Internet, rather than the computer itself.

If you subscribe to Apple's iCloud+ you may be thinking you don't need a VPN to hide your location and identity. Apple's update for iCloud subscribers includes iCloud Private Relay, which sounds a bit like a VPN because it encrypts your web-browsing traffic and sends it through a relay to hide your location, IP, and any information about what you were browsing.

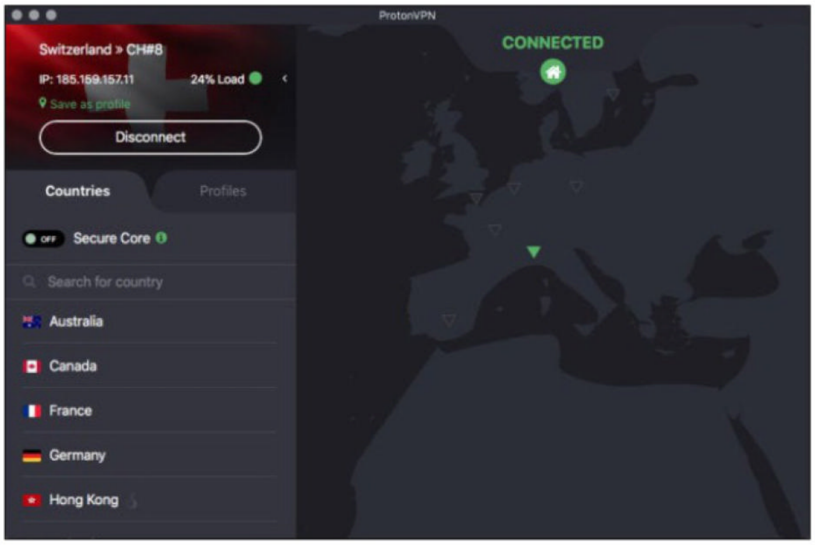
However, iCloud Private Relay is not a VPN because you aren't able to choose an IP address or a region, and you won't be able to make it look like you're coming from another location. So you can't watch geographically locked Netflix content, for example. For more information on iCloud+ Private Relay, see page 57.

Our current favourite service is Surfshark, which is a well-priced all-rounder. But below you will find the top VPN services for Mac.

HOW WE TESTED VPNS

For each VPN service we review, we conduct tests at three different times of the day: morning, afternoon, and evening, using Ookla Speedtest (fave.co/3lZO84I). We start by measuring the speed of our unprotected Internet connection before testing the upload/download speeds of the VPN service. These tests are conducted to servers located in North America, the UK, Europe, Oceana and Asia over an Ethernet connection with a service provision of 100Mb/s.

To test upload and download speeds, we close down all background Internet processes on the Mac, using TripMode. The only traffic on the system able to upload or download any data is Ookla. We use this set-up to ensure that the numbers that Ookla produced were



A good VPN should allow for server connections around the globe.

not stymied by anything else that the computer may have been doing at the time. The speeds Ookla captured were then averaged, providing us with a final numeric score.

We then use those scores to calculate a percentage of difference in speeds, which is what you'll see in our reviews. Since Internet speeds change constantly based on server load, how fast your connection is, and a gazillion other factors, we feel this provides a better picture of what you can expect from a service, on the whole, than merely quoting the exact upload/download speeds we encountered during testing.

Speed isn't the only quantifiable metric that we look at. The number of countries that a VPN offers servers in, total number of servers worldwide, and how much it'll cost you to connect to those servers on a monthly or annual basis are also taken into consideration when recommending a VPN service to you.

Additionally, we conduct hours of research into the VPN providers to find out who owns them, where they're based, what they do with subscriber information, and whether the provider has a track record of questionable business practices.

WHAT'S A VPN?

VPN stands for virtual private network. If you're not using a VPN, when your computer connects to the Internet, it does so through the local gateway provided by your Internet service provider (ISP). Doing this allows you to connect to all of the online services you use everyday.

However, connecting this way also allows an ISP to know your physical location based on where you access the Internet – be it at home, at work, in a cafe, or at a public Wi-Fi hotspot. This information is often sold to marketers and other parties interested in getting to know more about you and your browsing habits.

Worse still, if you connect to the Internet through an access point with weak security, such as at an airport, mall, or local library, hackers connected to the same network could intercept personal information like your social media passwords or banking credentials through what's called a man-in-the-middle attack. A VPN service can help prevent all of that.

A VPN creates an encrypted digital tunnel between your computer and the server of the VPN service you choose to use. Once this tunnel has been established, your web searches, the sites you access, and the information you submit online will be hidden from prying eyes. This means that your ISP can't log or sell your information and hackers using the same network as you will find it difficult to initiate an attack on you. Almost no one will have any idea of what information you're accessing.

WHAT A VPN CAN'T DO

A VPN can't protect you from viruses, malware, or ransomware attacks if you choose to download an infected file, or a visit site designed to inject your computer with malignant code. It won't keep spoofed sites from stealing your personal information, if you happen to visit one. So, you'll want to bone up on online security best practices.

You should know that while using a VPN will allow you to anonymously engage in peer-to-peer file-sharing/torrenting, some service providers may cancel your VPN subscription or turn over your information to the authorities if they catch you trading copyrighted material with others.

WHAT TO LOOK FOR

A clear privacy policy. A good VPN should offer an easy-to-understand privacy policy that outlines what, if any, information the company collects from its users. It's important that this policy details what they do with this information. Some VPN providers, especially those that offer their services for free, sell their user information to advertisers and other interested parties, just like an ISP does. Choose a provider that offers a level of privacy that suits you.

Know where the provider is based. Many countries have no laws demanding that VPN providers maintain logs of their users' activity. This makes maintaining your privacy more assurable than it would be if you use a VPN located in a country that requires that user-activity records be maintained. Some companies, in an effort to make their network of servers look bigger or more varied than it actually is, spoof the locations of their servers.

The more servers, the merrier. Choosing a VPN provider with a ton of servers around the world is important for a couple of reasons. First, having a multitude of servers to choose from means that you won't be forced to connect to an overpopulated server where the data flows like mud. Second, having a wealth of servers to choose from both at home and internationally means more opportunities for spoofing your location, allowing you to hide where you are or access region-locked content with ease.

Multiple payment options. It's a vicious circle. Paying for a VPN with a credit card online before you have access to a VPN could allow your financial information to fall into the wrong hands. Look for providers that offer alternative payment options such as PayPal, Bitcoin, AliPay, or via the Mac App Store.

An easy-to-use interface. It takes a lot of digital wizardry to connect to a VPN. Some people want to see how their VPN operates, behind the scenes. Using an open source VPN client like Tunnelblick is great for this. Most people, however, just want their VPN to work with minimal frustration. Look for a VPN service that offers a client with an easy-to-use interface.

Protection for all of your devices. A good VPN service will offer licenses for multiple devices to protect your loved ones' computers as well as your personal smartphone and tablet. To this end, before investing in a VPN subscription, make sure that it provides software clients for all of the devices you own.

1. SURFSHARK

Price: £1.92 per month from fave.co/41w9JC

- 3,200+ RAM-based servers.
- Multi-Hop connections.
- Unlimited simultaneous connections.
- 24/7 customer service.
- Two-factor authentication.
- GPS spoofing (Android only).

Surfshark is a great-value VPN that

1.

offers a lot more than you'd expect for a small monthly price. Its apps are easy to use and it reliably unblocks streaming services such as Netflix and BBC iPlayer. It's missing the specialty servers offered by rivals such as NordVPN, though.

Connection speeds are very impressive, and that's thanks to the use of the WireGuard protocol. You really won't notice any slowdown in your Internet speed when Surfshark is running, so long as you have WireGuard selected and aren't using servers the other side of the globe.

The company has upgraded all its servers so they run entirely in RAM, just like NordVPN and ExpressVPN. It's also a member of the VPN Trust Initiative, while two-factor authentication (2FA) is a feature few VPN services offer.

The other reason to consider Surfshark is because it undercuts almost all of its rivals on price, yet doesn't place any limit on the number of devices you can use simultaneously. So you can install and use it across many devices including your Mac, PC, Android and iOS devices, as well as browsers.

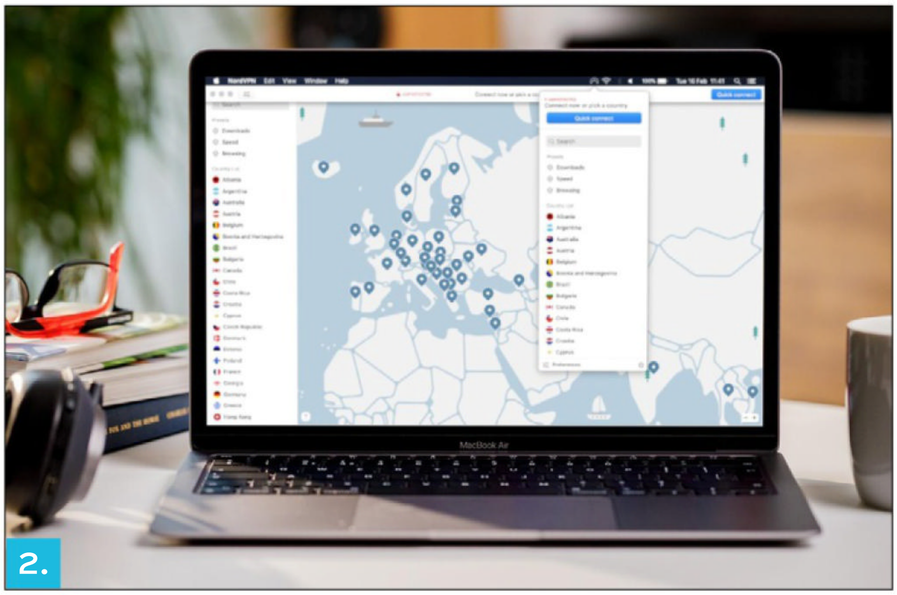
There's a kill switch, a strict no-logs policy and a Multi-Hop feature which routes your connection via two VPN servers for an extra layer of protection. However, there's no split tunnelling or GPS spoofing on the Mac.

2. NORDVPN

Price: £2.99 per month from fave.co/3IBKXHZ

- 6 simultaneous connections.
- 24/7 tech support.
- Kill Switch.
- Works with Netflix and other streaming services.

NordVPN is one of the biggest and best-known VPN services. It sat firmly at the top of this list for



2.

years until Surfshark pipped it to the post. NordVPN is easier to use than Surfshark and has a more up-to-date independent audit. It also has speciality servers for specific purposes. But Surfshark is cheaper, offers unlimited connections and has more in-depth double VPN features.

There are more than 5,000 servers available across 59 countries. You won't have to figure out which one to choose thanks to the handy 'Quick connect' feature that picks the server best suited to your needs. Connections are fast and reliable, and NordVPN unblocks popular streaming services around the world including Netflix and BBC iPlayer. You can connect up to six devices simultaneously.

Recently Nord has added support for the faster WireGuard protocol, making it one of the fastest VPN services out there. However, it's only available on the 'IKE' version of the app, which only offers a permanently enabled kill switch. To have more control, you'll need to download the 'OpenVPN' version, albeit with slightly slower speeds.

You can get 68 percent off the usual monthly price if you take advantage of the two-year plan. However, there's no split tunnelling on the Mac version.

3. EXPRESSVPN

Price: £5.75 per month from fave.co/41wKWha

- Kill switch (Network Lock).
- 5 simultaneous connections.
- 24/7 customer service.
- Works with Netflix and other streaming services.

ExpressVPN is one of the most accomplished VPN services you can buy. Everything you'd expect from a modern VPN is here, including

3.

an effective kill switch, impressive device support and split tunnelling for app-by-app protection. Although the latter doesn't yet work on macOS Big Sur, it is extremely easy to set up, with quick access via the menu bar one of the highlights.

ExpressVPN has often led the way when it comes to security, but other providers are quickly catching up. It's no longer the only one with RAM-based servers, while solid device and tech support are the norm whichever service you use.

The new Lightway protocol looks set to deliver big increases to the speeds ExpressVPN is capable of, but as open-source technology many similar services will be able to make use of it. Many of these are significantly more affordable.

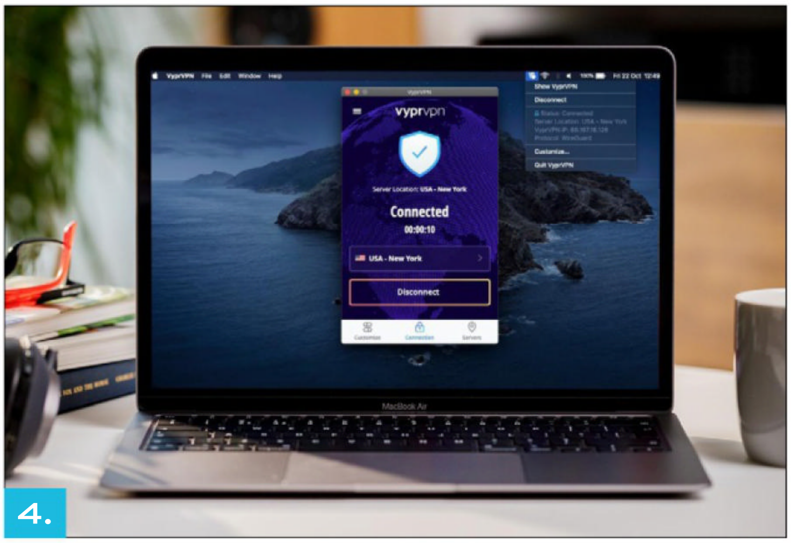
With the introduction of Apple Silicon, there's no doubt that ExpressVPN is more than capable of serving the next generation of Mac. It's just not the only one.

4. VYPRVPN

Price: £9 per month from fave.co/3IUpdbV

- Kill switch and split tunnelling.
- WireGuard protocol means fast speeds.
- 30 simultaneous connections.
- Works with Netflix and other streaming services.

VyprVPN offers everything most people are looking for in a VPN, without needing to spend much money. You get fast WireGuard speeds, alongside separate protocols focused on reliability, anti-censorship and ease of use. It's also excellent at unblocking geo-restricted content, whether that's local versions of Netflix or



BBC iPlayer & ITV Hub from outside the UK. Premium features such as split tunnelling and a kill switch are here too, even if the latter can't be customised.

VyprVPN's no-logs policy has been independently audited, and the service adheres to a strict Privacy Policy from parent company Golden Frog. More than 700 servers in over 70 countries should be plenty for most people, although there's often only one per country. It's also not clear which of these are physical and virtual.

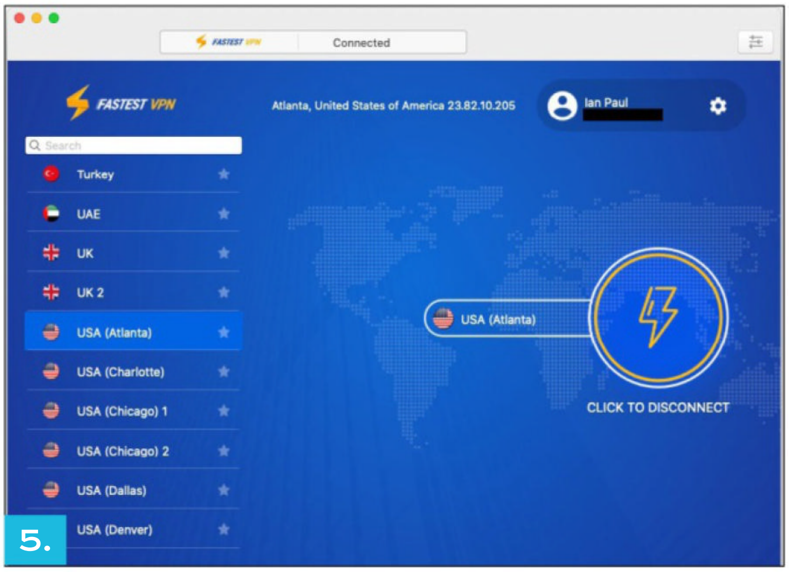
Nonetheless, it's still speedy, reliable and affordable – especially if you don't mind subscribing for a year. That 12-month plan will set you back £4.50 per month, representing excellent value for money.

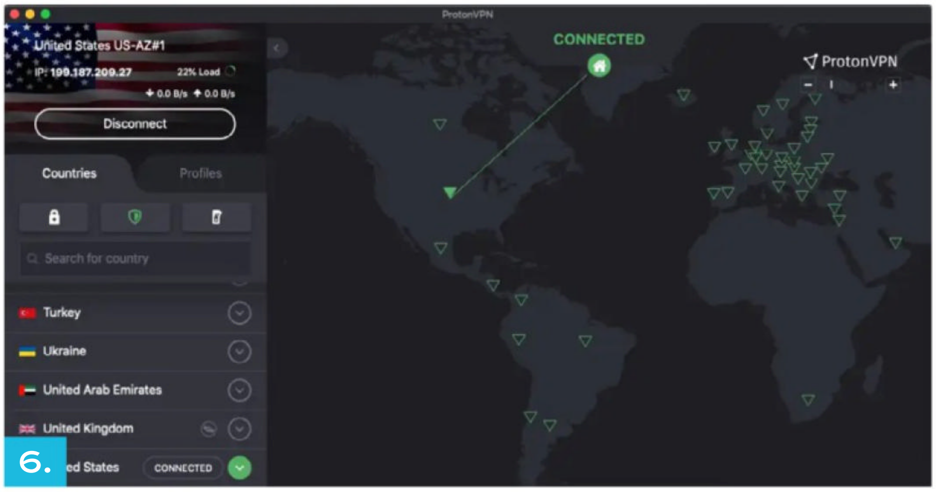
5. FASTESTVPN

Price: $40 (around £33) lifetime licence from fave.co/3yeXtc1

- Supports 10 simultaneous connections.
- 32 country connections with more than 250 servers.
- Internet kill switch blocks all online traffic if VPN connection drops.

This easy-to-use, attractive, and uncomplicated app is a great option for VPN newbies. In addition to its straightforward and uncluttered design, FastestVPN also offers good speeds and a sufficiently expansive network. It's icing on the cake that its





6.

privacy policy is easy to understand and makes all the right promises.

In our tests, FastestVPN maintained about 30 percent of the base speed across five locations on multiple test days, although there were some weak spots in Asia and Australia.

Despite it's name it's not the fastest VPN, but FastestVPN does make the right privacy promises in a way that's easy to understand.

6. PROTONVPN

Price: €9.99 per month (around £8.60) per month from fave.co/3kq5jMB

- 55 country options.
- Includes NetShield malware and tracker blocker.
- Internet kill switch option.
- Works with Netflix and other streaming services.
- One of the fastest VPN we've tested on macOS.

ProtonVPN is an impressive VPN. It starts with a free tier with very limited features, is easy to understand, offers a collection of interesting features and great speeds.

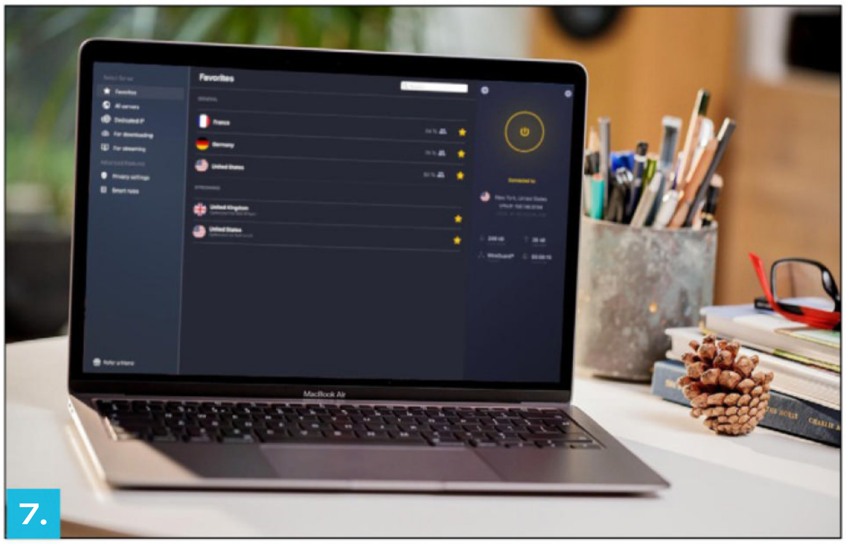
ProtonVPN is a ProtonVPN starts with a free tier with very limited features is an excellent service with fast speeds, the right privacy promises, a good amount of features including support for streaming services, and fair pricing. It's well worth a look.

7. CYBERGHOST

Price: £1.92 per month from fave.co/3KF2CkQ

- 6,700+ servers.
- 7 simultaneous connections.
- 24/7 customer service.
- Kill switch.

CyberGhost is one of the biggest names in the VPN industry. It's affordable and user friendly, so is



7.

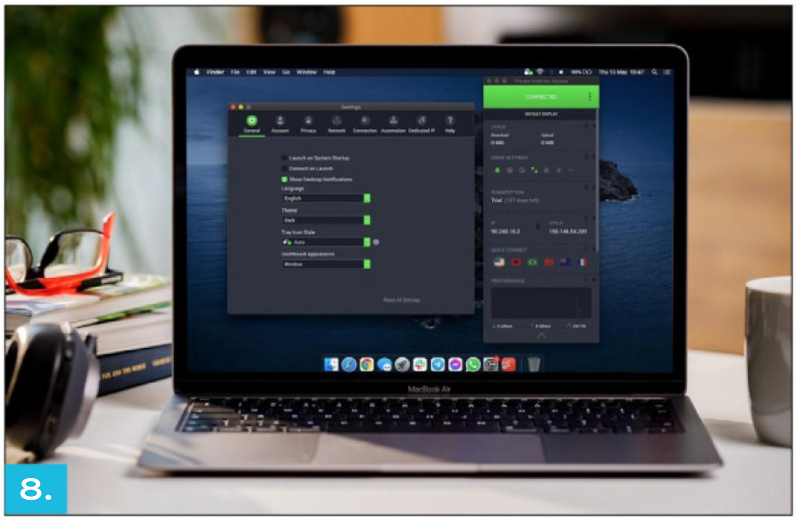
perfect for anyone using a VPN on their Mac for the first time.

Like certain rivals, it is constantly adding new servers and the current tally of over 6700 in 88 countries means you should always be able to get a fast connection. And in our tests, we've always seen great speeds from CyberGhost, especially following the introduction of the WireGuard protocol.

It works with phones, tablets, browsers and of course your Mac.

It's not perfect, though – there's no split tunnelling on the Mac, no evidence of a recent independent audit of security credentials and a user experience that's slightly rough around the edges. It also didn't unblock BBC iPlayer in our testing.

Still, at £1.92 per month for 3-year deal (which currently gives you three months' extra free), it still represents very good value for money.



8.

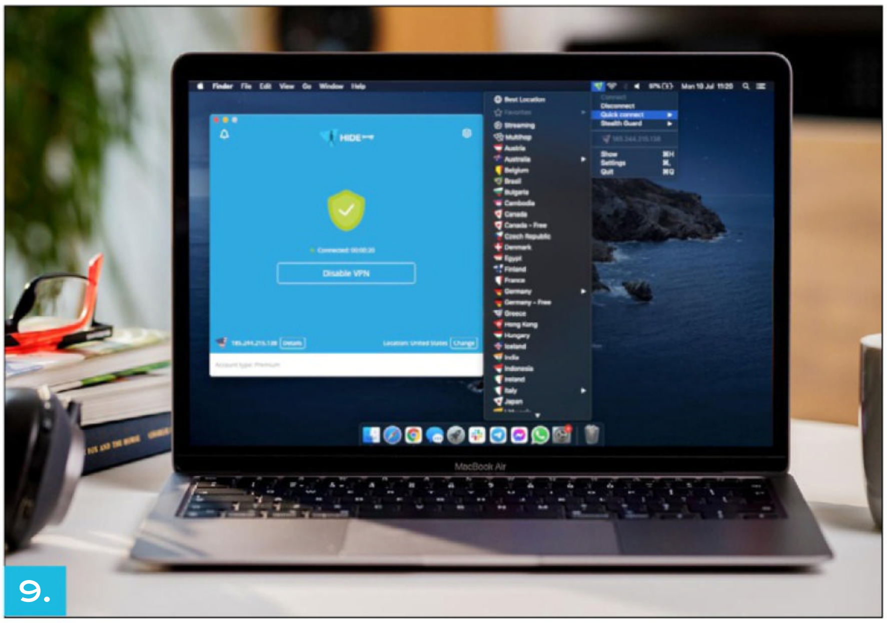
8. PRIVATE INTERNET ACCESS

Price: £1.69 per month from fave.co/3Zrn7Wb

- 33,000+ servers.
- 10 simultaneous connections.
- 24/7 customer service.
- Kill switch and split tunnelling.

Private Internet Access (PIA) is a compelling VPN at a relatively affordable price, making it a great option for the Mac. It has an incredible 33,665 servers across 73 countries – that's far higher than almost any consumer VPN service. These include all the most popular locations, with the option for up to 10 simultaneous connections.

Speeds are excellent, thanks to the recent introduction of the WireGuard protocol. PIA also benefits from a kill switch and split tunnelling, features that are sometimes left out of Mac VPN services. It allows you to access international versions of Netflix, as well as BBC iPlayer while outside the UK. The service doesn't log any of your details or activity, so even though it is based in the US, there's no data to hand over should the authorities order PIA to do so.



9.

However, it's not perfect. There's no evidence of an independent audit and the Mac app is clunky in comparison to some rivals.

Nonetheless, PIA is a solid VPN service at an affordable price.

9. HIDE.ME

Price: £9.99 per month from fave.co/3y2nRp3

- 1,900+ servers in 47 countries.
- Kill switch.
- Split tunnelling.
- 24/7 live chat.
- 10 simultaneous connections.
- Free version.

Hide.me is another VPN service which has improved considerably in recent years. As well as offering a completely free version (which none of its rivals here do), it has also added WireGuard, which is considerably faster than other encryption protocols.

Other key features include a customisable kill switch and split tunnelling, as well as a Stealth Guard which stops selected apps from running without the security of a VPN connection.

It can unblock Netflix and allows you to access BBC iPlayer from outside the UK. There's also solid device support, with up to 10 simultaneous connections permitted.

However, the user interface on Mac is a bit clunky, and we're still waiting for an update to the 2015 no-logs policy certification.

10. MALWAREBYTES PRIVACY VPN (MAC)

Price: £2.50 per month from fave.co/3SuCWtf

- Offers 32 country locations.
- More than 245 servers.

Malwarebytes, probably best known for antivirus software and advice, also offers a standalone VPN service called Malwarebytes Privacy. It's an easy to use app with the right kind of privacy promises – as you'd expect from a respected name in security based in the US.

In our tests Malwarebytes was a mid-tier performer in terms of speeds, but it should be good enough for most casual users.

Malwarebytes Privacy VPN does a good job and, starting at £2.50 a month for one device, the price is right.

10.

FAQ: iCloud+ Private Relay

Apple's new privacy component is in beta, but you can still try it out. **Jason Cross** reports

If you've downloaded iOS 15, you might have noticed something different about your iCloud account. Apple is upgrading all paid iCloud accounts to something it calls iCloud+. It includes several interesting new features on top of the existing iCloud storage, sync, and cloud features, but the most interesting might be something Apple calls iCloud Private Relay. At first, it sounds like a VPN: your web-browsing traffic is encrypted and sent through a relay to hide your exact location, IP, or the contents of your browsing traffic.

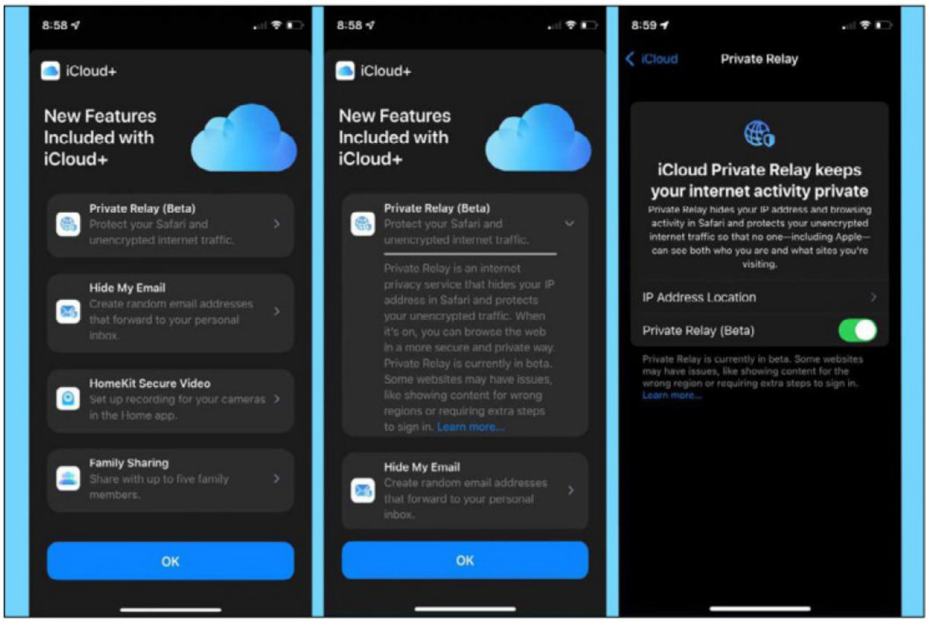
It's not a VPN, though. Not quite. There are important differences, which we'll describe here. But iCloud Private Relay may be enough for most people, giving the most obvious benefits of a VPN to millions of users who would never consider signing up for one. Here's what this Private Relay feature is, how it works, and how it's different from a traditional VPN.

HOW TO YOU TURN ON iCLOUD PRIVATE RELAY

iCloud Private Relay is a free upgrade in iOS 15 for anyone who pays for iCloud storage either separately or as part of an Apple One bundle. To turn it on, head to the Settings app, then tap your Apple ID name at the top. Then tap iCloud and Private Relay (Beta) and flip the toggle green to turn it on. You can also choose between two IP address locations: General 'so that websites can provide local content in Safari' or broader country and time zone for more anonymity.

When Private Relay is enabled, all of your browsing activity in Safari will be routed through two Internet 'hops', or relays. Your data is encrypted and then sent to Apple, so your ISP can't see any of your web browsing requests. Once at Apple's proxy server, the DNS request (the thing that points a domain name like "macworld.com" to a specific server IP address) and your iPhone, iPad, or Mac's IP address are separated. Your IP address is retained by Apple, while your DNS request is passed on, encrypted, to a 'trusted partner' that has the decryption key, along with a fake intermediary IP address that is based on your approximate location. Apple didn't name its partners, but some web sleuths have figured out that they are major Internet backbone companies such as Akami, Cloudfare, and Fastly.

This means that Apple knows your IP address but not the name of the sites you're visiting, and the trusted partner knows the site you're visiting but not your IP (and therefore



Protect your Safari and unencrypted internet traffic.

Create random email addresses that forward to your personal inbox.

Set up recording for your cameras in the Home app.

Share with up to five family members.

Private Relay is an internet privacy service that hides your IP address in Safari and protects your unencrypted traffic. When it's on, you can browse the web in a more secure and private way. Private Relay is currently in beta. Some websites may have issues, like showing content for wrong regions or requiring extra steps to sign in.

iCloud Private Relay keeps your internet activity private

Private Relay hides your IP address and browsing activity in Safari and protects your unencrypted internet traffic so that no one—including Apple—can see both who you are and what sites you're visiting.

Private Relay is currently in beta. Some websites may have issues, like showing content for the wrong region or requiring extra steps to sign in.

iCloud Private Relay.

not who or where you are). Neither party can piece together a complete picture of both who you are and where you're going.

The website you're visiting typically gets your exact IP address and DNS request, so it can easily build a pretty detailed profile of exactly who you are, where you are, and where you're going online. Combine that with a few cookies, even innocuous-seeming ones, and it's pretty simple to have your entire online activity profiled, tracked, traced, and sold to advertisers (and others). What iCloud Private Relay does is make the websites you're visiting totally ignorant of this information, so the sites can't build profiles of your activity.

The IP addresses Apple uses in place of your real one are still roughly approximate to your general area; it's not enough to identify you personally, but it will allow sites that use your IP address to deliver local news, weather, sports, or other information to keep working fine. There's an option to use an even broader IP address, but it might make some of those sites work incorrectly.

Note that Apple does not allow you to choose an IP address or even a region, and won't ever make it seem like you're coming from a totally different place. In other words, if you want to use it to access geographically locked content in Netflix or other online services, you're out of luck.

WHY iCLOUD PRIVATE RELAY IS DIFFERENT FROM A VPN

As cool as this Private Relay feature is, it's definitely not a VPN. It will do a great job of preventing profiling of your web activity based on your basic connection data. But it has a lot of shortcomings compared to a real VPN. Some of these include:

- It only works with Safari, not any of the other apps or web browsers you use. Technically, some other DNS info and a small subset of app-related web traffic will use it, but it's best to think of it as a Safari-only thing.

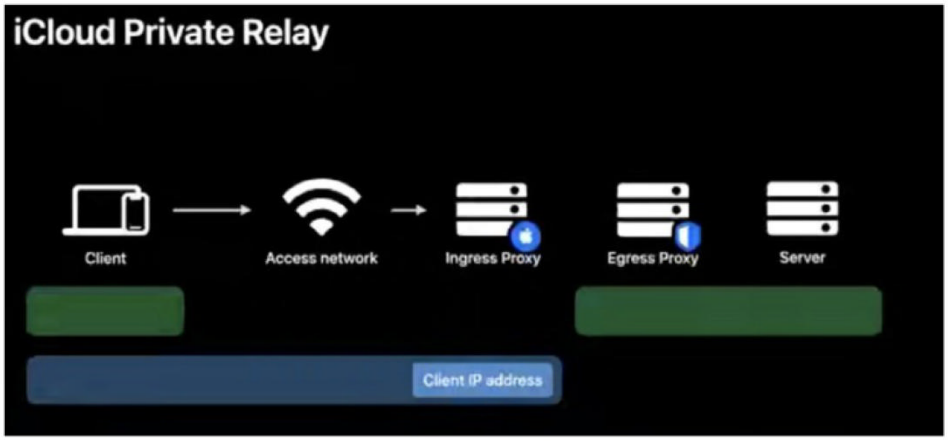
- It's easily identifiable as a 'proxy server', which many large networks like those at schools or businesses will not work with. Most good VPNs disguise themselves to look like regular non-proxy traffic.

- As mentioned, it can't hide the region you're connecting from, only your specific IP location, so you can't access content locked out of your region or experience websites as if you're connecting from another country.

If all you really want to do is stop websites from building a profile of you and selling it around to advertisers and data brokers, then using iCloud Private Relay on your iPhone, iPad or Mac is a great option. It's fast, easy, and if you already pay for any amount of iCloud storage, you'll get it for free.

You should know that, as of iOS 15.1 and watchOS 8.1, iCloud Private Relay and Mail Privacy Protection do not work on Apple Watch. If you use the Mail app on your Apple Watch or open a web link (say, sent to you via Messages), the watch will use your real IP address.

If you want real privacy and security for everything you do on the Internet, or want to access content that's available in countries other than your own, you'll still need a VPN. Fortunately, we have some VPN recommendations for you.



Apple's two-proxy system makes it very difficult for any one company to build a profile of your web activity.

CAN A CARRIER BLOCK iCLOUD PRIVATE RELAY?

Yes, your cellular provider can disable the feature. In iOS 15.3, Apple has tweaked the wording in Settings in iOS 15.3 to let people know what's going on:

Private Relay is turned off for your cellular plan. Private Relay is either not supported by your cellular plan or has been turned off in Cellular Settings. With Private Relay turned off, this network can monitor your Internet activity and your IP address is not hidden from known trackers or websites.

A few carriers in Europe have disabled the feature for some users. This is not always malicious, or merely about collecting and selling user data. Some carriers provide content filtering features like parental controls, and iCloud Private Relay prevents them from working. In order to ensure compatibility with these features, iCloud Private Relay must be disabled.

The more elegant solution, of course, would be to allow users to enable iCloud Private Relay and simply warn them that such features may not work on that device, rather than taking the choice out of their hands entirely.

Credit: Getty Images/BlackJack3D

How to protect your Mac from malware and theft

While virus outbreaks on Macs are rare you could still be targeted. Here's what you should do to stay safe. **Karen Haslam** reports

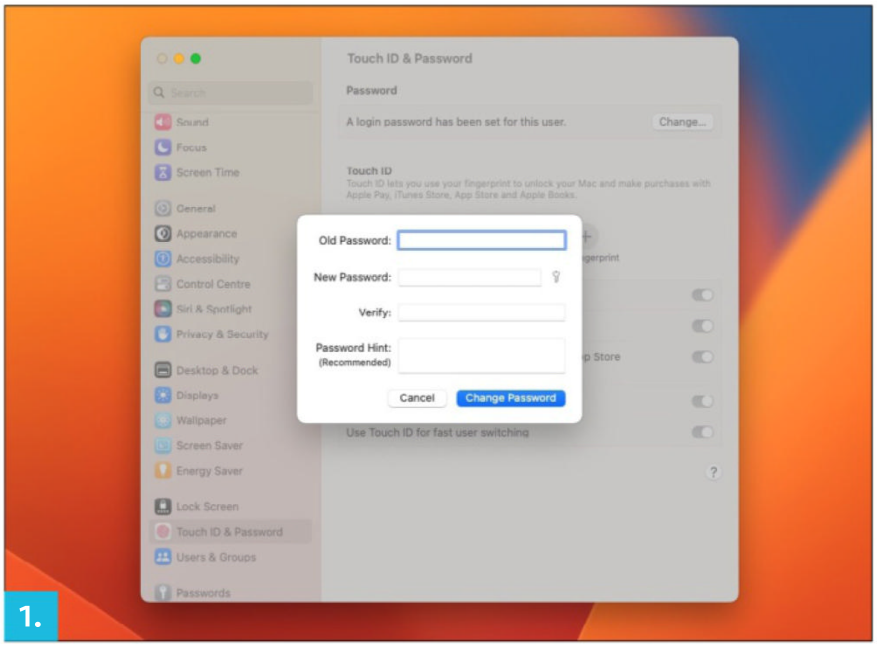
One of the best things about owning a Mac is the fact that you are less likely to be a victim of malware than with a Windows PC. However, macOS isn't foolproof and you shouldn't be too lax about protecting your investment. Here are our tips for keeping your Mac safe from day one:

1. CHOOSE A STRONG LOGIN PASSWORD

The first thing you should do with your Mac is set up a good password. You might think that there is no need to password-protect your Mac if you're only going to be using it at home, but there are various reasons why you need this layer of protection.

For one thing, without a password

on your Mac, nothing on your Mac is secure and someone could gain access to your email, photos, and more. macOS has a number of security features that keeps your data safe, but if someone gets past your login screen, they can still gain access to sensitive information.



1.

Touch ID & Password

Password

A login password has been set for this user.

Touch ID

Touch ID lets you use your fingerprint to unlock your Mac and make purchases with Apple Pay, iTunes Store, App Store and Apple Books.

Old Password:

New Password:

Verify:

Password Hint: (Recommended)

Use Touch ID for fast user switching

You can choose your password during set-up, but if you haven't – or just want to change the one you made – here's how:

macOS Ventura

1. Open System Settings.
2. Select Touch ID & Password.
3. You can now set up a password or change your existing password to something safer.
4. If your Mac has Touch ID, you can also enter multiple fingerprints and select that can be used for Apple Pay and other purchase, and auto-filling passwords.

macOS Monterey or earlier

1. Open System Preferences.
2. Select Security & Privacy.
3. Click General.
4. You can now set up a password or change your existing password.

Make sure you choose a sensible password that won't be easily guessed as your Mac can also be used as part of Apple's two-factor authentication for iCloud.

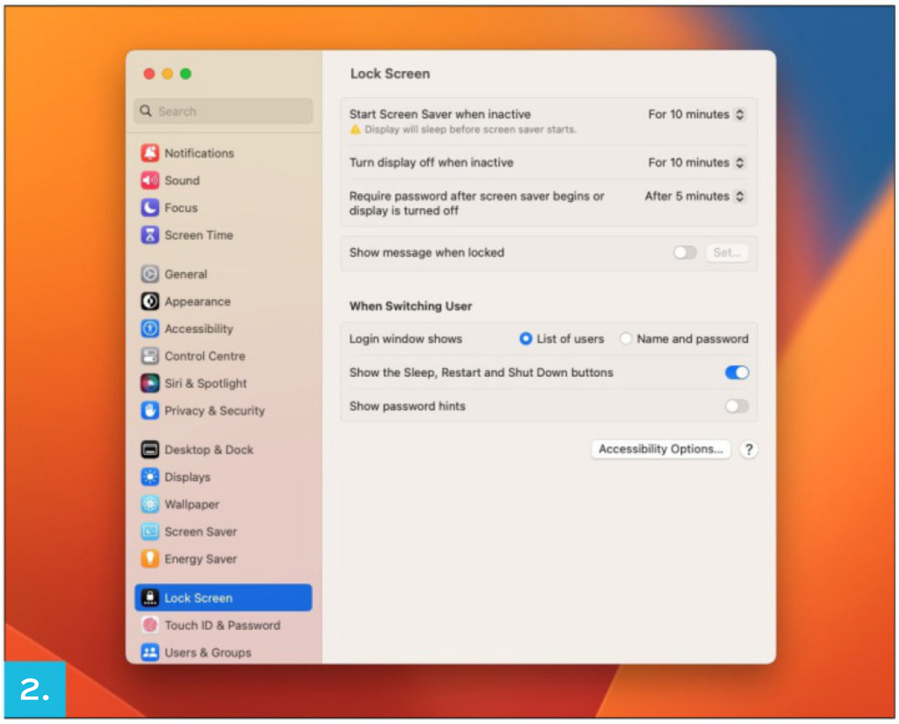
2. CHANGE YOUR LOCK SCREEN SETTINGS

You can set your Mac display to turn off when inactive after a period of time, which will

When you select the amount of time you are happy to leave your Mac unprotected keep in mind that if the screensaver doesn't start for half an hour and then your Mac waits another 15 minutes before requiring a password, your Mac will be unprotected for 45 minutes. To choose the length of time you are willing to let pass before having to enter the password after the screensaver starts or the screen turns off, follow these steps:

macOS Ventura

1. Open System Settings.
2. Click on Lock Screen.
3. Select 'Start screensaver when inactive' and choose 10 minutes.
4. Select 'Turn display off when inactive' we recommend you choose 10 minutes.
5. Select 'Require password after the screensaver begins or display is turned off' and choose 5 minutes.



Lock Screen

Start Screen Saver when inactive: For 10 minutes
⚠ Display will sleep before screen saver starts.

Turn display off when inactive: For 10 minutes

Require password after screen saver begins or display is turned off: After 5 minutes

Show message when locked

When Switching User

Login window shows: ● List of users ○ Name and password

Show the Sleep, Restart and Shut Down buttons

Show password hints

2.

macOS Monterey or earlier

1. Open System Preferences.
2. Click on Battery (MacBook) or Energy Saver (desktop).
3. On a MacBook, click Battery and select 10 minutes using the 'Turn the display off after' slider.
4. On a desktop, click on Power Adapter and select 10 minutes using the 'Turn the display off after' slider.
5. Go to Security & Privacy and beside 'Require password after sleep or screensaver begins,' choose five minutes.

In both cases, this will mean your Mac is locked down after 15 minutes of inactivity. If you'd like that time to be less then adjust the settings accordingly.

3. USE APPLE'S PASSWORD MANAGER

We all know the importance of a secure password, but remembering them all can be frustrating. That's why Apple offers a way to secure all your passwords so you only have to remember one. Apple's iCloud

Keychain is a built-in password manager that works with all your Apple devices and will log you into all your software and services.

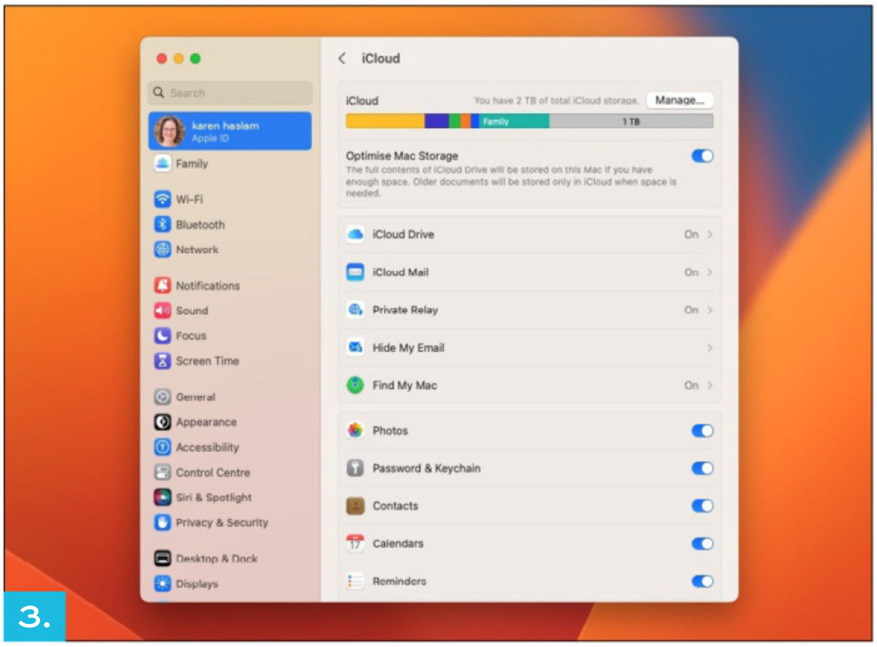
You just need to make sure you have set up iCloud Keychain:

1. Open System Settings in macOS Ventura or System Preferences on older versions of macOS

2. Click on the Apple ID information section at the top.

3. Click on iCloud.

4. Click the Password & Keychain toggle to turn it on.



3.

iCloud

iCloud — You have 2 TB of total iCloud storage. Manage...

Optimise Mac Storage: On
The full contents of iCloud Drive will be stored on this Mac if you have enough space. Older documents will be stored only in iCloud when space is needed.

iCloud Drive: On
iCloud Mail: On
Private Relay: On
Hide My Email
Find My Mac: On
Photos: On
Password & Keychain: On
Contacts: On
Calendars: On
Reminders: On

Now when you need to enter a password, your Mac will offer to autofill the fields after Touch ID or password authentication.

4. TURN ON FIND MY MAC

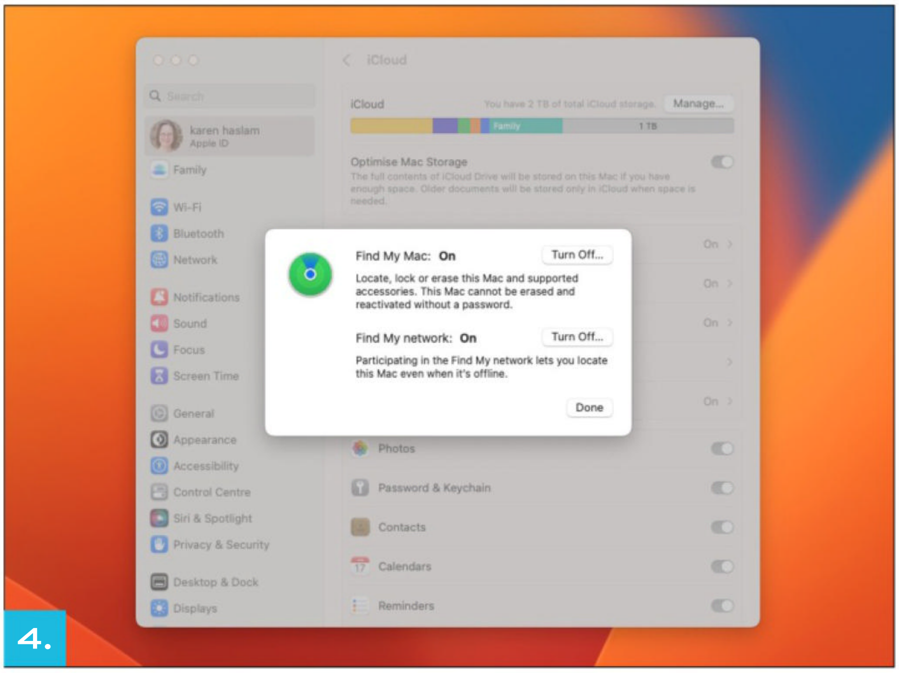
Find My is an Apple app that can help you locate a lost Mac or erase it remotely if it's been stolen. Here's how to set it up:

1. Open System Settings/System Preferences.

2. Click on your Apple ID.

3. Click on iCloud.

4. Scroll through the options until you find Find My Mac and turn it on.



4.

Find My Mac: **On** — Turn Off...
Locate, lock or erase this Mac and supported accessories. This Mac cannot be erased and reactivated without a password.

Find My network: **On** — Turn Off...
Participating in the Find My network lets you locate this Mac even when it's offline.

Done

5. Click Allow on the pop-up box when asked to 'Allow Find My to use the location of this Mac'.
6. Enter your Mac password.
7. If Location Services is turned off you will need to turn it on, so go to Security & Privacy and click on I.

Now, you'll be able to track your MacBook if it's lost and completely wipe away your data if it's stolen. Find My is an invaluable tool that we hope you never have to use – but you'll be glad you set it up if you do.

5. SET UP MULTIPLE USERS

If other people will be using your Mac, it's a good idea to set them up as their own users, so they can't access your data. Additionally, if someone needs access to your Mac you can set up a temporary Guest User.

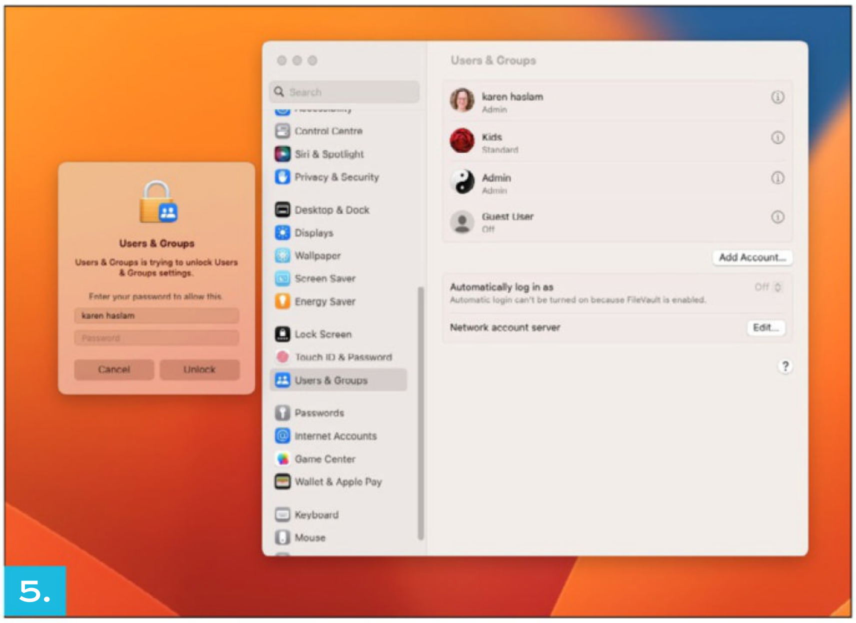
macOS Ventura

1. Open System Settings.
2. Choose Users & Groups.
3. Click on Add Account...
4. Enter your password to unlock.
5. Enter the full name and account name of the user.
6. Create a password.
7. Click on Create User.

macOS Monterey or earlier

1. Open System Preferences.
2. Choose Users & Groups.
3. Click the lock icon and enter your password.
4. Click on the plus symbol.
5. In the 'New Account' section, choose Standard (not Administrator).
6. Give them a name, account name, and password.

If you want to set up a Guest User, select the option in the list of names and choose 'Allow guests to log into this computer'. You won't need to set a password as they can't



Users & Groups

Users & Groups is trying to unlock Users & Groups settings.

Enter your password to allow this.

karen haslam

Password

karen haslam Admin
Kids Standard
Admin Admin
Guest User Off

Automatically log in as Off
Automatic login can't be turned on because FileVault is enabled.

Network account server

5.

change user or computer settings and all saved files are deleted once they log out.

6. LOCK DOWN YOUR MAIL

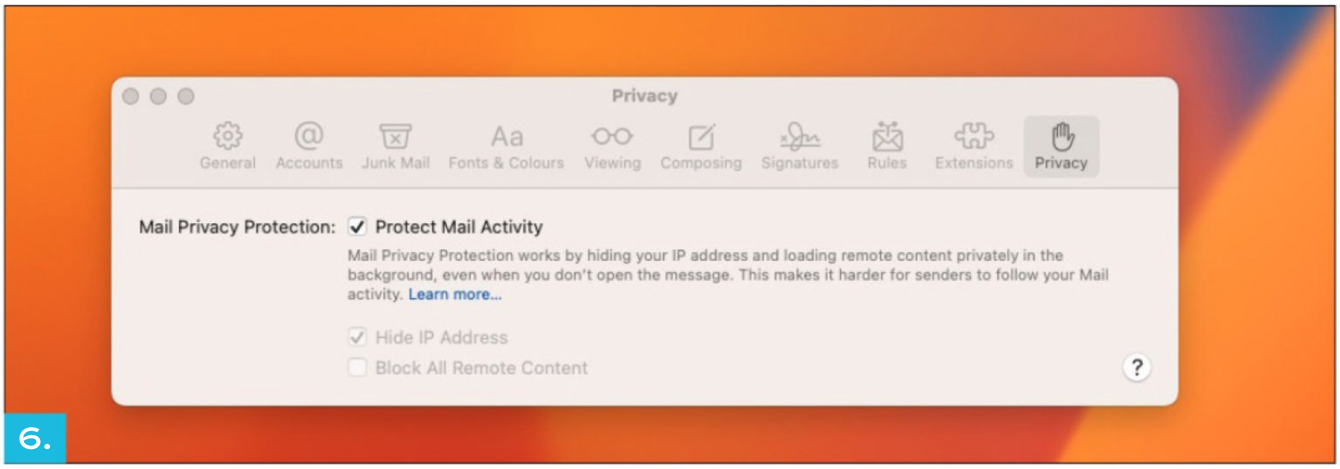
Your email is as much of a risk as Safari or Chrome, so locking it down is just as important. One thing you can do to protect yourself is to stop scammers from being able to use tracking pixels hidden in images to tell them you have opened the email to confirm that the email address is in use. You can also turn on Mail protection right on your Mac to protect your address:

1. Open Mail.
2. Click Mail > Settings (Preferences in Monterey or earlier).
3. Click Privacy.
4. Make sure that Protect Mail Activity is selected. This will hide your IP address and load remote content privately so that senders can't see your activity.

Another thing you can do is hover over links and email addresses in the message to see the URL so you can see if they are really what they appear to be.

7. LIMIT YOUR APP DOWNLOADS

One of the most powerful security features on your Mac is Gatekeeper. Designed to keep you safe by stopping you from installing anything that hasn't been verified by Apple, it'll warn you any time your try to install an application from the web and block installation of some apps. The safest way to install apps on your Mac is to only download from the Mac App Store, but if you venture outside the store, your Mac can warn you before installing the app.



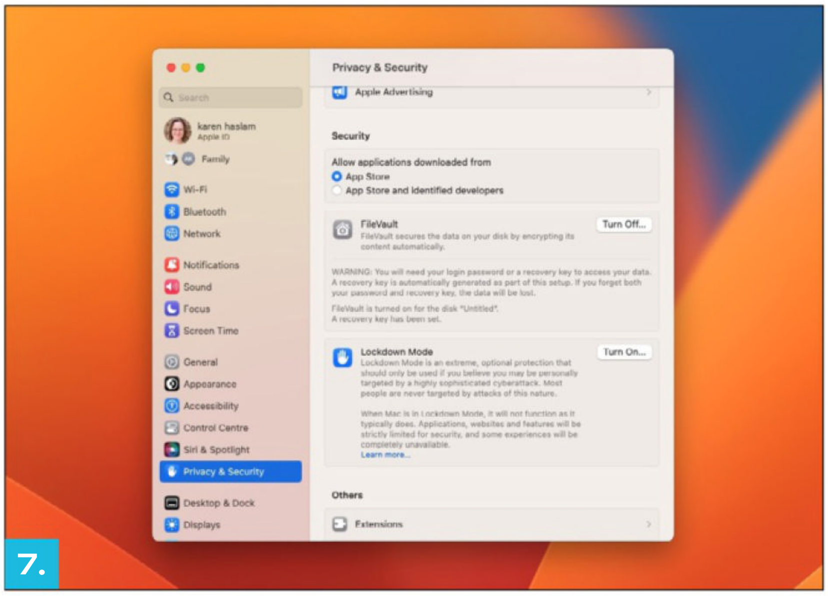
Mail Privacy Protection: ☑ Protect Mail Activity

Mail Privacy Protection works by hiding your IP address and loading remote content privately in the background, even when you don't open the message. This makes it harder for senders to follow your Mail activity. Learn more...

☑ Hide IP Address

□ Block All Remote Content

6.



Privacy & Security

Security

Allow applications downloaded from
● App Store
○ App Store and identified developers

FileVault
FileVault secures the data on your disk by encrypting its content automatically.

WARNING: You will need your login password or a recovery key to access your data. A recovery key is automatically generated as part of this setup. If you forget both your password and recovery key, the data will be lost.

FileVault is turned on for the disk "Untitled".
A recovery key has been set.

Lockdown Mode
Lockdown Mode is an extreme, optional protection that should only be used if you believe you may be personally targeted by a highly sophisticated cyberattack. Most people are never targeted by attacks of this nature.

When Mac is in Lockdown Mode, it will not function as it typically does. Applications, websites and features will be strictly limited for security, and some experiences will be completely unavailable.

Others

7.

1. Open System Settings/System Preferences.
2. Click on Privacy & Security.
3. Select App Store under the 'Allow applications downloaded from' section.

This won't prevent you from downloading apps outside the App Store, but it will require a couple of extra steps before it installs.

8. KEEP YOUR SOFTWARE UP TO DATE

All of Apple's protections will be no good to you if you don't update your software when updates are issued so be sure to always update your Mac if Apple issues an update – many of which has a security component.

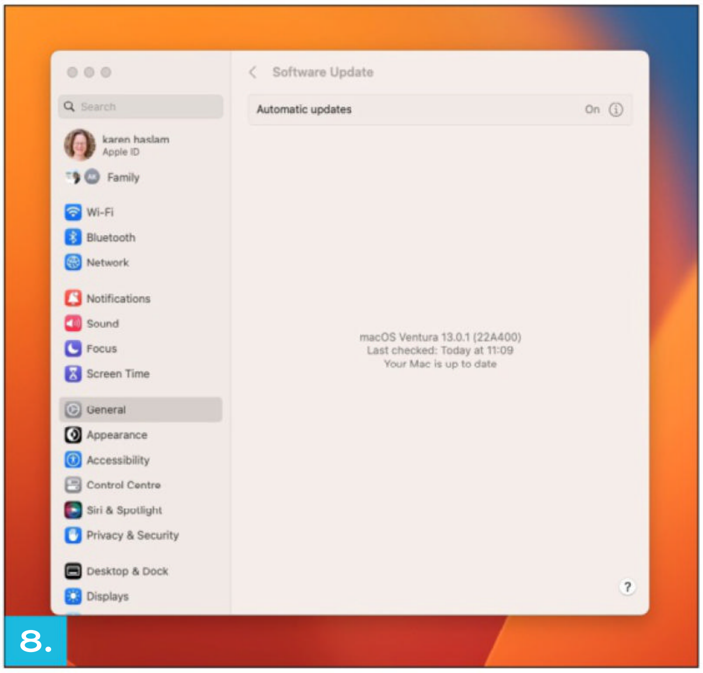
To update your Mac follow these steps:

macOS Ventura

1. Open System Settings.
2. Click on General.
3. Click on Software Update.
4. Your computer will check for updates.
5. If one is available, click Download and Install.

macOS Monterey or earlier

1. Open System Preferences.
2. Click on Software Update.
3. Your computer will check for updates.
4. If one is available, click Download and Install.



Software Update

Automatic updates On

macOS Ventura 13.0.1 (22A400)
Last checked: Today at 11:09
Your Mac is up to date

8.

To automatically install updates overnight, turn on Automatic Updates on Ventura or check the box beside ‘Automatically keep my Mac up to date’ on Monterey or older.

9. AUGMENT APPLE’S XPROTECT ANTIVIRUS

If malware or a bad app gets past Gatekeeper, macOS includes its own antivirus software called XProtect, which blocks and removes any malware detected on your Mac. XProtect is on by default and is updated by Apple regularly, but it’s not foolproof, so you might want to check out a Mac antivirus app to give yourself another layer of protection.

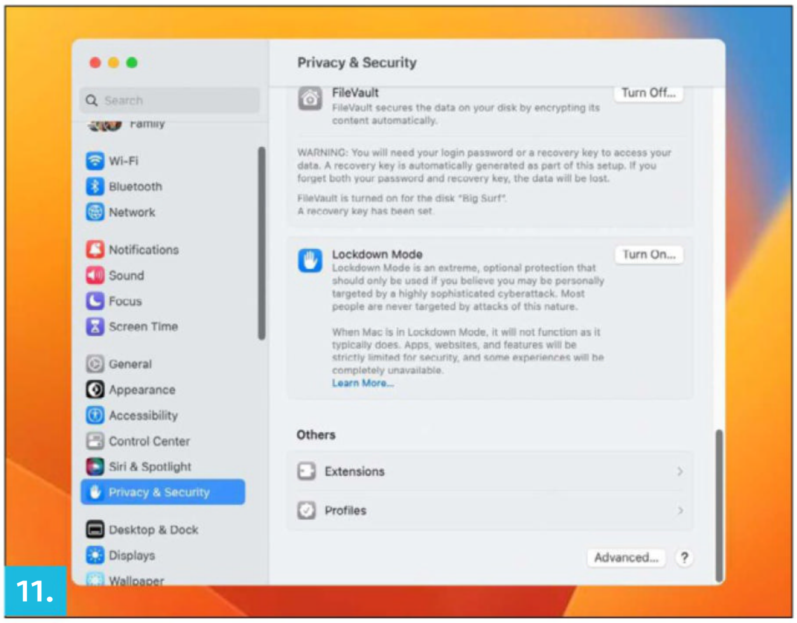
10. USE A VPN

You can add another layer of protection by using a VPN on your Mac. A VPN will encrypt all your data and route it to an endpoint operated by the folks who run the VPN service keeping your data completely private.

Apple offers its own pseudo-VPN called iCloud Private Relay for anyone who pays for iCloud+ that encrypts your web traffic but doesn’t hide your region and only works with Safari. So if you want a VPN that works with other browsers (and one that allows you to access region-locked content), you’ll need a dedicated VPN.

11. TURN ON LOCKDOWN MODE

Lockdown Mode isn’t a setting most people will need to use. Apple says the extreme security measures are for “the very few users who, because of who they are or what they do, may be personally targeted by some of the most sophisticated digital threats, such as those from NSO Group and other private companies developing state-sponsored mercenary spyware”. When activated, it will block most attachments in Messages, disable



Privacy & Security

FileVault

FileVault secures the data on your disk by encrypting its content automatically.

WARNING: You will need your login password or a recovery key to access your data. A recovery key is automatically generated as part of this setup. If you forget both your password and recovery key, the data will be lost.

FileVault is turned on for the disk “Big Surf”.
A recovery key has been set.

Lockdown Mode

Lockdown Mode is an extreme, optional protection that should only be used if you believe you may be personally targeted by a highly sophisticated cyberattack. Most people are never targeted by attacks of this nature.

When Mac is in Lockdown Mode, it will not function as it typically does. Apps, websites, and features will be strictly limited for security, and some experiences will be completely unavailable.
Learn More...

Others

Extensions

Profiles

11.

complex web technologies', and block incoming FaceTime calls, among other high-level security measures.

To turn it on, you'll need macOS Ventura. Head over to System Settings, then Privacy & Security, and click 'Turn' on next to Lockdown Mode.

Credit: Getty Images/solarseven

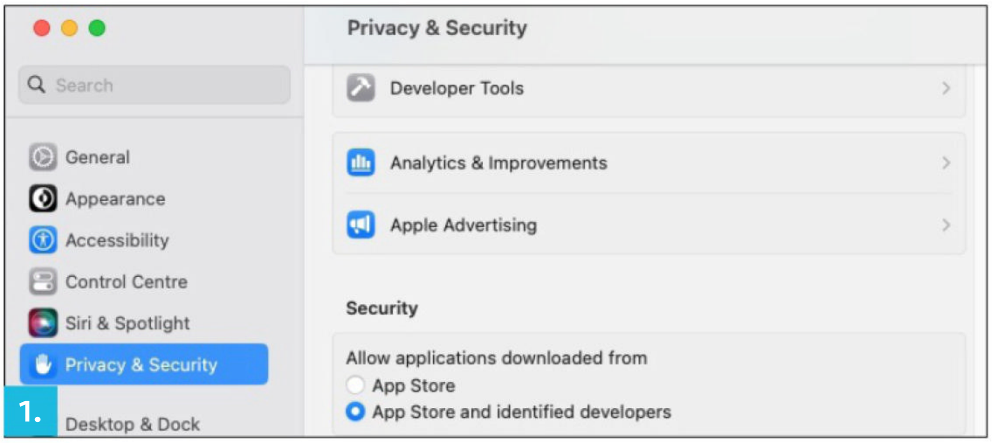
How to check your Mac for viruses

macOS does a good job of stopping malware from attacking your Mac. But there's more you can do. **Karen Haslam** reports

You may have been led to believe that you don't have to worry about computer viruses on your Mac. And, to some extent, there's truth to that. While your Mac can definitely be infected with malware, Apple's built-in malware detection and file quarantine capabilities should make it less likely that you'll download and run malicious software.

Apple introduced malware detection to the macOS back in 2009 with Snow Leopard (Mac OS 10.6).

This system consists of the quarantine of any app downloaded from the Internet, the use of Code Signing certificates to verify that an app is coming from a legit source, and regular security updates that include databases of known malware targeting the macOS.



Security

Allow applications downloaded from

○ App Store

● App Store and identified developers

1.

HOW APPLE SCANS YOUR MAC FOR VIRUSES AND MALWARE

Apple includes antivirus software in macOS that monitors your Mac for malware, blocks malware and removes it if necessary. There are three elements to this: XProtect, Gatekeeper and Notarization.

1. Apps are checked before they can be installed

Apple makes it hard to install an app that might not be safe on a Mac. Mac users can choose to only install apps from the Mac App Store, which is the safest option as it mean that the app has been thoroughly checked by Apple before being distributed.

Alternatively there is an option to install apps from the Mac App Store and from identified developers. An identified developer is one whose software has been scanned by Apple to ensure it is safe. As long as the app has passed Apple's tests it will have a Notarization ticket, which Gatekeeper looks for before telling macOS that it is safe to open.

If you only install apps from the Mac App Store, or notarized apps from identified developers, you should be safe, but sticking to the Mac App Store is the safest option as apps on the Mac App Store can't be tampered with. If you want to make sure your Mac can only install apps from the Mac App Store these are the steps to follow:

macOS Ventura

1. Open System Settings.
2. Click on Privacy & Security.
3. Scroll down to Security and select

App Store below Allow applications downloaded from.

macOS Monterey or earlier

1. Open System Preferences.
2. Click on Security & Privacy.
3. Click on General.
4. Under Allow applications downloaded from select App Store.

If you prefer to allow installations from outside the Mac App Store follow the same steps but choose App Store and identified developers from the options.

If you choose to allow installations from identified developers then Apple will look for evidence that the app is notarized and it will also verify that the app hasn't been tampered with and no malware is present. Unfortunately in the past there have been apps that slipped through this process because a certificate was present, such as the case of the Shlayer malware, but Apple has ramped up security since and changes to notarized apps are pushed out as required.

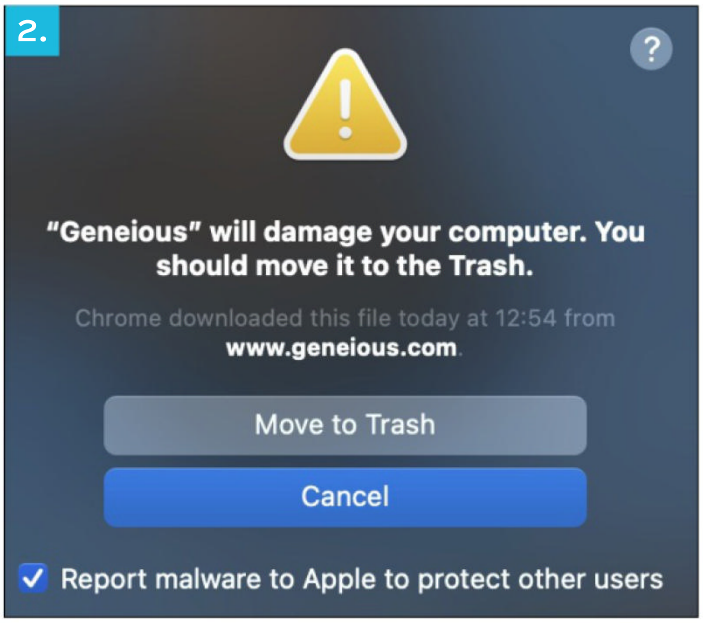
If Gatekeeper detects that the app has no notorization to prove the developer is certified by Apple, a message saying the app can't be opened because of your settings will be displayed. If you know that the software is from a legitimate developer you can override this and open the app. However, you should be aware that even legitimate software has been known to conceal malware.

2. XProtect blocks malware from running

Even if the developer is recognised by Apple, the software will still be checked against a list of known malware in XProtect. XProtect will scan an app the first time it launches and it will scan the app every time there is an update issued for it.

Updates to XProtect are pushed out frequently and macOS automatically checks for updates daily – a Mac user doesn't even need

2.



"Geneious" will damage your computer. You should move it to the Trash.

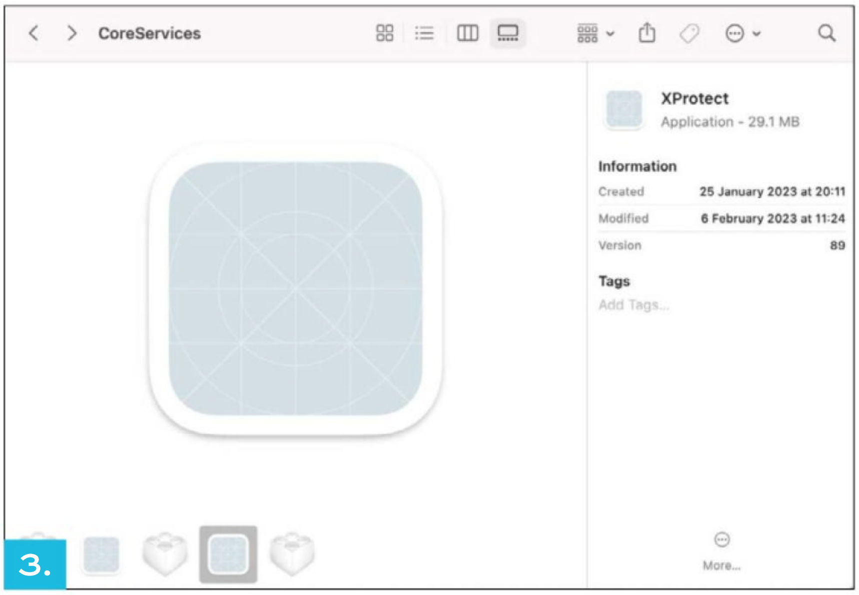
Chrome downloaded this file today at 12:54 from **www.geneious.com**.

☑ Report malware to Apple to protect other users to do anything as these updates are separate to macOS updates. This means that even the newest malware should be identified by XProtect, although Apple isn't always as fast at getting this information updated as other antivirus solutions are. If malware is identified the app will be blocked and a message will appear giving the option to delete the software.

To take full advantage of XProtect you need to be running macOS Catalina (10.15) or later, but we would advise that, because Apple only supports the last three versions of macOS, you will be safest if you are running Big Sur, Monterey and Ventura. You should make sure your Mac is set to receive these updates automatically by following these steps:

macOS Ventura

1. Open System Settings.
2. Go to General > Software Update.
3. Click on the i beside Automatic updates and check that Install Security Responses and System Files is selected.



3.

CoreServices

XProtect
Application - 29.1 MB

Information
Created 25 January 2023 at 20:11
Modified 6 February 2023 at 11:24
Version 89

Tags
Add Tags...

More...

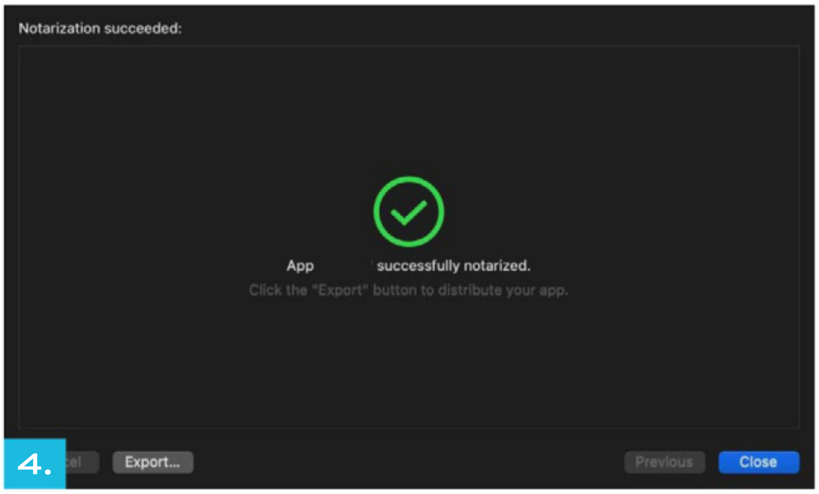
macOS Monterey or earlier

1. Open System Preferences.
2. Click on Software Update.
3. Click on Advanced.
4. Make sure the box beside Install system data files and security updates is selected.

3. Malware is removed by XProtect Remediator

When malware is identified on a Mac the user sees an alert suggesting that the move the affected app to the trash. The user is also asked to alert others to the malware, which they can do automatically. This doesn't mean it is entirely down to the user to delete the app and remove the malware though.

The removal used to involve a separate Malware Removal Tool


4.

Notarization succeeded:

App successfully notarized.

Click the "Export" button to distribute your app.

(MRT) found in /Library/System, but is wasn't an app users could run. However, since macOS Monterey MRT was replaced by an XProtect Remediator that scans for and removes malware.

XProtect Remediator will scan your Mac at least once a day or more, and is updated much more frequently than MRT was – since MRT is no longer updated it is a good reason to make sure you are running macOS Catalina or later.

XProtect Remediator will attempt to remedy or remove malware.

4. Developer loses certificate and app loses notarization

If an app had been notorized by Apple but malware is identified that developer will lose the certificate that allows them to distribute apps and the app will lose its notarization.

This change to the notarization is then pushed to other Mac users so that Gatekeeper knows not to allow that app to be opened.

macOS checks for XProtect updates daily, but Notarization updates are issued even more frequently, so if malware is detected, or an app loses its Notarization, Mac users should quickly be protected.

5. Is Apple's protection enough?

If Mac users rely solely on XProtect and Apple's other protections there are limitations in comparison to other anti-malware solutions, which are updated more regularly and have teams of specialists working on identifying malware. The protection offered by XProtect is also more basic than that of third-party anti-malware apps that can also protect you from phishing, social networking scams, and they can protect your Windows using friends.

XProtect is updated more frequently than it was – which was one of the main criticisms – but other malware apps check for malware constantly. XProtect only checks for malware when an app is downloaded for the first time, if the app is updated and if the status of the developer signature or app notarization changes.

Apple's protections should keep your Mac free from most malicious software, but they do not make it impossible for malicious software to be installed on your Mac. If new malware is released today and you download and run it today you will have done so before Apple's databases could have been updated. So it's always best to be wise when downloading software from unknown sources.

HOW TO SCAN FOR VIRUSES ON A MAC

macOS will automatically scan your Mac for any malware definitions that features in XProtect, you can't force it to do this. If you wish to enhance the protection to include other kinds of malware, and scan for Windows viruses so there is no danger of passing them on, then you would be wise to install a third party anti-malware app.

There are lots of third party apps that can to scan your Mac for viruses, including some free options and many that offer a free trial period.

Before you can scan your Mac for viruses you may need to visit the Privacy & Security in System Settings or Security & Privacy in System Preferences to allow access. For example, in the case of Avira we had to click on Allow to let it scan our system. You will also need to allow Full Disk Access, which can also be done in Privacy & Security.

Initiating a virus scan is an easy process that usually begins with the user clicking a Scan or Smart Scan button. Expect the scan to take a while. We had about an hour wait while our Mac was scanned by Sophos while a scan with the free Avira took about half an hour.

Credit: Getty Images/Arkadiusz Warguła

How to remove a virus from a Mac

Mac malware is rare, but it does exist. Here's how to get rid of Mac viruses for free. **Karen Haslam** reports

If you are worried you have some kind of malware or virus on your Mac, we are here to help you figure out what's going on and, if necessary, clean up the damage – all for free. A lot of the websites offering advice on Mac malware removal are companies trying to sell your anti-virus solutions, which makes their tips somewhat biased, but here you can expect impartial advice.

We'll cover how to remove malware from your Mac, getting rid of any viruses that might be lurking. We'll also explain why it's probably not a virus thanks to Apple's stringent protections in macOS, but, if it is, we'll let you know about the free and cheap options that can protect your from Mac from malware.

Note that in this article we are going to be mixing and matching the terms malware and virus, but they are actually separate concepts. Malware tends to take the form of apps that pretend to do one thing, but actually do something nefarious, such as steal data. Viruses are small discrete bits of code that get on to your system somehow and are designed to be invisible. There are also other types of threat, such as ransomware and adware, and other phishing attempts, where an attempt is made to extract information that can be used to obtain money from you.

We'll address how to detect and get rid of these types of malware on your Mac in this article.

HOW TO REMOVE MALWARE FROM A MAC FOR FREE

You may be wondering whether you need to wipe your Mac to remove the virus, or indeed if wiping your Mac will completely remove the virus. It's possible that you won't have to go that far – try these steps to clean things up:

1. Update macOS to the latest version

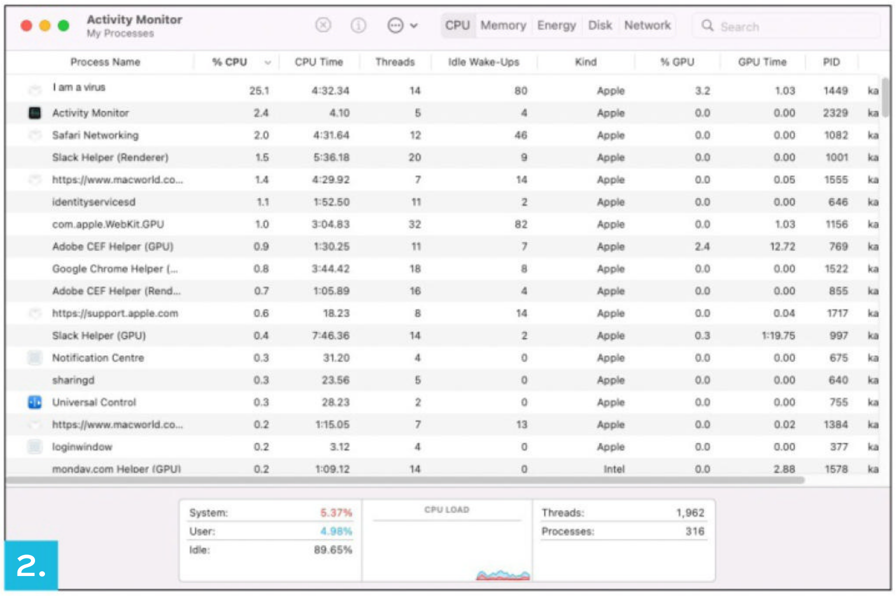
One reason you may not need a Mac antivirus on your Mac is that Apple offers its own protections. For several years now Apple has included invisible background protection against malware and viruses.

One of these protections is Xprotect. Xprotect is Apple's built-in malware protection. Xprotect will scan files you've downloaded and check them for known malware or viruses. If any are found you will be told the file is infected or damaged. The Xprotect system gives a warning when you download malware that it knows about, and tells you exactly what to do.

It has been very effective at halting the spread of Mac malware before it can even get started, and is yet another reason why malware or virus infections on a Mac are rare.

Apple updates Xprotect automatically, so you shouldn't need to manually update macOS yourself to get the latest virus protections. However, if you are running an older version of macOS might not be protected (Apple only supports the past three versions of macOS).

While it's partially true that updating your Mac software could rid you of a virus, you should note that as good as Apple's protections are, they may not be enough. Unfortunately, some times it takes Apple a few days (or longer) to respond to the latest



2.

Activity Monitor
My Processes

Process Name	% CPU	CPU Time	Threads	Idle Wake-Ups	Kind	% GPU	GPU Time	PID	
I am a virus	25.1	4:32.34	14	80	Apple	3.2	1.03	1449	ka
Activity Monitor	2.4	4.10	5	4	Apple	0.0	0.00	2329	ka
Safari Networking	2.0	4:31.64	12	46	Apple	0.0	0.00	1082	ka
Slack Helper (Renderer)	1.5	5:36.18	20	9	Apple	0.0	0.00	1001	ka
https://www.macworld.co...	1.4	4:29.92	7	14	Apple	0.0	0.05	1555	ka
identityservicesd	1.1	1:52.50	11	2	Apple	0.0	0.00	646	ka
com.apple.WebKit.GPU	1.0	3:04.83	32	82	Apple	0.0	1.03	1156	ka
Adobe CEF Helper (GPU)	0.9	1:30.25	11	7	Apple	2.4	12.72	769	ka
Google Chrome Helper (...	0.8	3:44.42	18	8	Apple	0.0	0.00	1522	ka
Adobe CEF Helper (Rend...	0.7	1:05.89	16	4	Apple	0.0	0.00	855	ka
https://support.apple.com	0.6	18.23	8	14	Apple	0.0	0.04	1717	ka
Slack Helper (GPU)	0.4	7:46.36	14	2	Apple	0.3	1:19.75	997	ka
Notification Centre	0.3	31.20	4	0	Apple	0.0	0.00	675	ka
sharingd	0.3	23.56	5	0	Apple	0.0	0.00	640	ka
Universal Control	0.3	28.23	2	0	Apple	0.0	0.00	755	ka
https://www.macworld.co...	0.2	1:15.05	7	13	Apple	0.0	0.02	1384	ka
loginwindow	0.2	3.12	4	0	Apple	0.0	0.00	377	ka
mondav.com Helper (GPU)	0.2	1:09.12	14	0	Intel	0.0	2.88	1578	ka

System:	5.37%
User:	4.98%
Idle:	89.65%

Threads:	1,962
Processes:	316

threat. For that reason it is worth considering an additional antivirus tool to stay safe.

2. Use Activity Monitor to find viruses on a Mac

If you know for sure you've installed some malware – such as a dodgy update or app that pretends to be something else – make a note of its name. You can quit out of that app by tapping Cmd + Q, or clicking Quit in the menu, but note that this won't stop it from starting up again – in fact it may still be working in the background.

If you don't have any idea what is causing the issues you suspect are caused by a virus on your Mac, you can use Activity Monitor to spot if an app or a task is using a lot of resources – this may be the malicious software.

1. Open Activity Monitor, which you'll find within the Utilities folder of the Applications list (or you can search for it in Spotlight by pressing Command + Space and typing **`Activity Monitor`**).

2. If you are suspicious about a particular app, use the search field at the top right to search for that app's name. You might find that the questionable app is still running, despite the fact you quit it.

3. To stop such an app running select it in the Activity Monitor list, click the 'x' icon at the top left of the toolbar and select Force Quit. Note that this won't stop the malware from starting up again – we'll explain how to remove it in the next step.

4. If you don't have a suspicious app name to search for, sort your Activity monitor by CPU so you can see which applications and tasks are using a lot of your Mac's resources. Make sure you note the details and names of these suspicious processes before quitting them by clicking on the 'x'

icon and selecting Force Quit.

5. Next check the Memory tab to see if anything is using a lot of memory.

6. Check the Disk tab to see if anything is standing out in the Bytes Written column.

7. Check the Network tab and pay special attention to the Sent Bytes column.

8. Once you have a selection of names that could relate to what you are looking for search your system for them using Spotlight (Command + Space) and remove them from your Mac

3. Delete the file or app and empty the Download folder

If you believe your Mac was infected after opening a particular file or app and you have a file name to search for, you can attempt to locate that app, delete that file permanently by putting it into the Trash, and then empty the Trash. You should also empty the Downloads folder and delete everything in there: drag the whole lot to the Trash, and then empty the Trash. However, it is rarely this simple: most malware authors will obfuscate their code so that it uses non-obvious names, which makes it almost impossible to uncover this way.

4. Clear your cache

You should also clear your browser's cache. In Safari this can be done by clicking Safari > Clear History, and then selecting All History from the drop-down list. Finally click the Clear History button.

In Google Chrome this can be done by clicking Chrome > Clear Browsing Data, then in the Time Range drop-down box selecting All Time. Then click Clear Data. It's also worth deleting your application cache, although this could cause even more problems for you.

5. Shut down and restore from a backup

If none of the above have worked, which is unfortunately likely, you could try restoring from a backup, such as one made with Time Machine, but not a back up made since you contracted the virus – obviously, this backup should be from a time before you believe your computer became infected.

After restoring the backup, be careful when rebooting not to plug in any removable storage such as USB sticks you had plugged in earlier when your computer was infected, and certainly don't open the same dodgy email, file or app.

6.

6. Wipe your Mac and reinstall macOS

Sometimes the only way to be sure you're clean of an infection is to wipe your Mac to restore it to factory settings and then reinstall macOS and all your apps from scratch. Restoring your Mac to factory settings should remove the virus.

WHAT TO DO IF YOUR MAC HAS A VIRUS

In addition to the above there are a few other things you should do to protect yourself if you think you might have been infected with Mac malware – before and after the virus is removed.

1. Stay offline

While you think you are infected you should stay offline as much as possible. Try and turn off your Internet connection by either clicking the Wi-Fi icon in the menu back and selecting Turn Wi-Fi Off, or disconnecting the Ethernet cable if you're using a wired network.

If possible, keep your Internet connection turned off until you're sure the infection has been cleaned up. This will prevent any more of your data being sent to a malware server. (If you need to download clean-up tools, then this obviously might not be possible.)

2. Use safe mode

Boot your Mac up in Safe mode – this should at least stop the malware from loading at start up.

3. Don't use any passwords – and change them as soon as you can

From the moment you suspect you have a virus you shouldn't type any passwords or login details in case a hidden keylogger is running. This is a very common component with malware. Beware that many keylogger-based malware or viruses also periodically secretly take screenshots, so be careful not to expose any passwords by copying and pasting from a document, for example, or by clicking the Show Password box that sometimes appears within dialog boxes.

Once you are free of the virus you should change all your passwords, and we really do mean all of them – including those for websites, cloud services, apps, and so on.

4. Cancel bank and credit cards

If you handed over money at any point for the malware – such as if you paid for what appeared to be a legitimate antivirus app, for example – then contact your credit card company or bank immediately and explain the situation. This is less about getting a refund, although that might be possible. It's more about ensuring your credit card details aren't used anywhere else.

Even if no money has changed hands you should inform your bank or financial institutions of the infection and seek their advice on how to proceed. Often at the very least they make a note on your account for operatives to be extra vigilant should anybody try to access in future but they may issue you with new details.

The ultimate Mac troubleshooting guide

Tips for when your Mac won't work. **Roman Loyola** reports

The Mac is one of the most reliable PCs you can buy, which is probably why there's a heightened sense of anxiety when you press the power button and nothing happens. But take a deep breath. When your Mac won't start, there are a number of reasons why, and most likely, it's an easy fix. Apple has a support document with advice on what to do when your Mac won't turn on, but we're going to give you a little more detail and a few more things to check. Be sure to bookmark this page for when it inevitably happens again.

Before we start, let this be a lesson to keep a backup. Whether you use a cloud service, store important files on iCloud Drive, or use Time Machine with an external drive, you'll want to make sure your most personal stuff that isn't already in a cloud – local documents, files, movies, music, and so on. That way even if you need to wipe your Mac and start over.

YOUR MAC WON'T POWER UP

Make sure it's not actually on

If you press the power button and nothing happens, it might actually already be on. It sounds silly, but when a MacBook battery dies it goes into hibernation mode and it can be tough to tell if it's actually on or not. Listen for fan noise (though even Macs with fans are pretty quiet when they aren't doing anything), and check for light indicators, such as the backlighting on a MacBook keyboard or the Touch Bar on a MacBook Pro.

Also, look at the display. If it's a deep black, the screen is definitely off, but if the colour is more like an extremely dark grey that's close to black but not quite, it's on. You can tell by checking the contrast on a MacBook or iMac between the black bezel and the display – it should blend seamlessly if it's powered down. If you're using an external display, look for a power indicator LED on the front, and check that the cable connection is secure.

If you've determined that your Mac is actually on and not responding, you can try a restart. If you don't know how to do that, see below.

Check your connections

Beyond asking, "Is it plugged in?" we have a few more obvious issues that can often fix start-up problems.

The power cable to the Mac. This can sometimes get knocked loose, especially if you have a MacBook that you move around a lot. When I use my MacBook Pro on my lap while it is charging, sometimes the Thunderbolt power adapter becomes slightly unplugged and I don't even realize it. If it's been unplugged and the battery is dead, see above.

The power adapter in the wall. If you're not using an extension cable, the weight of the MacBook power adapter could cause it to fall out of a power socket. Also, the power adapter brick can somehow get disconnected from the prong module – that happened to me recently while moving things around for the cable guy. If you have a desktop Mac, it may have become unplugged while moving your desk.

The power strip/UPS. If your Mac is plugged into a power strip or UPS, check to see it hasn't been switched off or unplugged.

The outlet. Seems silly to mention this, but blackouts and blown fuses can happen, and during daylight hours you may not notice. As I write this on an unplugged MacBook Pro, the TV LED light is the only obvious and immediate indication I can find in the room that the power is on, so if the power went out, I won't know until I look at the television. You could check your circuit breaker or fuse box. Also, check the power outlet itself by plugging in something else.

Modules do well to stay on the power adapter, but it is possible for it to slide out of place.

Check the cables and peripherals

If you've determined that power is available and everything is plugged in, let's see if we can isolate the issue.

Try a different power cable or adapter. Cables can get tweaked, and power adapters can be rendered useless if there was a power surge. If you don't have a spare, ask a friend.

Disconnect peripherals. It's possible that something attached to your Mac is disrupting the boot process. Disconnect anything that's not needed to run your Mac: printers, external non-boot storage, cameras, etc. (You can leave your mouse and keyboard connected, as well as the display on desktop Macs.) If you're using a Mac Pro, make sure the internal components are seated properly.

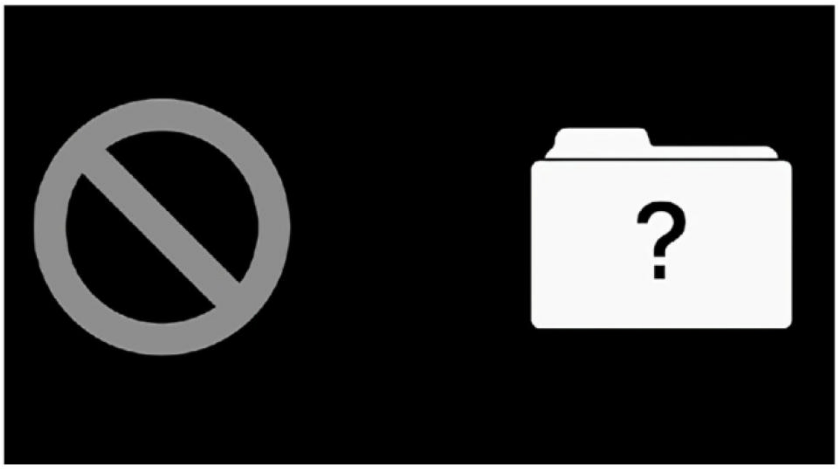
Plug in your MacBook and wait a few minutes. If you're trying to boot a MacBook using battery power, maybe the battery is drained. Let it charge for a few minutes, then try booting again.

Cycle the power

You have power, and all the connections are good. You can try performing a power cycle, which essentially forces your Mac to restart the boot process. Here's how to do a power cycle.

MacBooks: Press and hold down the power button for 10 seconds. The MacBook could make a squeal and then shut down if it's on. Press the power button again to turn it on.

Desktop Mac: Hold down the power button for 10 seconds. Then unplug the Mac for another 10 seconds before plugging it back in. Press the power button to turn it back on.



If the icon on the left appears during Mac start-up, it means the operating system on the start-up device isn't compatible. The icon on the right means that the start-up device has not been detected or the installed system software is no loner working.

YOUR MAC TURNS ON, BUT WON'T BOOT

If a normal start-up is unsuccessful, you need to restart in Safe Mode again and then see if you can check for any macOS and software updates, since there's likely an issue with the OS. If everything's up to date, there are a few more fixes you can try.

Reset the NVRAM/PRAM. This is for Intel Macs only; NVRAM on M-series Macs works differently and doesn't have an easy way for resetting. NVRAM and PRAM is used by the Mac for quick access to system settings. It's possible that a setting here got corrupted, so a reset may help fix things.

To reset the NVRAM/PRAM, turn off your Mac. Then hold down Command + Option + P + R as you turn the Mac on. Keep holding down those keys until you notice that the Mac restarts and the Apple logo appears.

After the Mac completes its start-up, you'll need to go into System Preferences and make some adjustments to the sound volume, screen resolution, and other settings to your liking.

Reset the SMC. This is also for Intel Macs only; M-series Macs do not have a system management controller (SMC). And the way to reset the SMC depends on the type of Intel Mac you have.

- **Intel MacBooks with a T2:** Turn off the laptop. Hold down for seven seconds the Control and Option keys on the left side of the keyboard, and the Shift key on the right side. (The Mac may turn on.) After seven seconds, keep those keys pressed and press and hold the power button for another seven seconds. (The Mac may turn off.) Release the keys and then turn on the Mac is it's off.

- **Intel MacBooks without a T2:** Turn off the laptop. On the left side of the keyboard, hold down the Shift, Control and Option keys, then press and hold down the power button for 10 seconds. Turn on the laptop.

- **Intel desktop Mac with or without a T2:** Turn off the Mac and then unplug the power cable. After 15 seconds, plug the cable in, then wait 5 seconds. Power up the Mac.

Fix the firmware

If you've followed all of the steps here and your Mac still won't start up, the problem could lie within the firmware. If you have another Mac, you can try connecting the two together and performing a revive or restore.

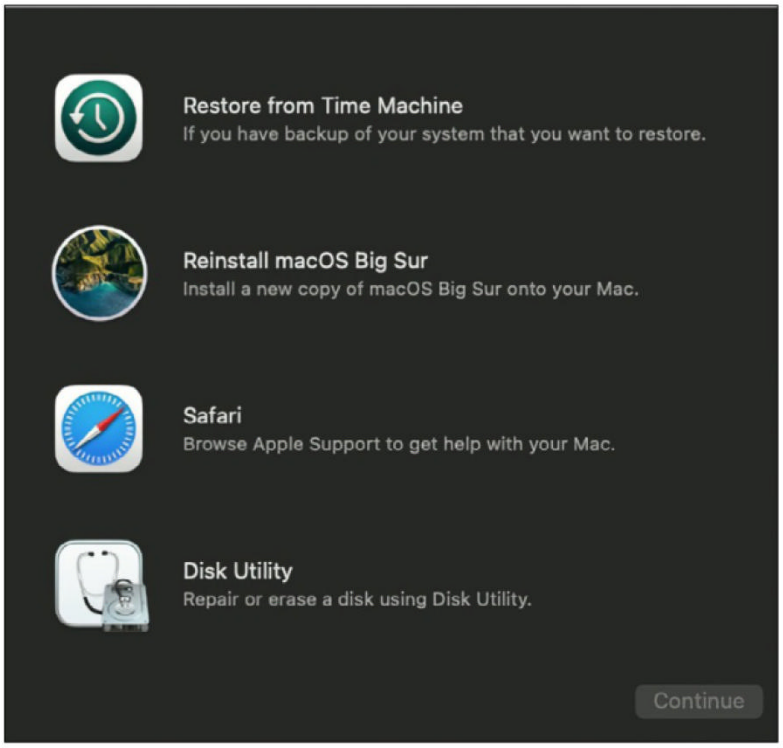
Boot into Safe Mode

You're able to turn on your Mac. Progress. But if your Mac won't start up all the way, you'll still need to do some work to get it working.

Safe Mode is a boot process where the Mac uses only what's necessary to start up – it doesn't load login items, optional system extensions, and non-macOS fonts. It also clears out system caches and checks your start-up disk for problems. The method for activating Safe Mode depends on the Mac you are using:

- **Intel-based Macs:** Turn off the Mac. Then power it on while holding down the Shift key. You can release Shift when the login window appears (you may have to log in twice). At the login window, you should see 'Safe Boot' in the upper right corner of the screen.

- **M-series Macs:** Turn off the Mac. Hold down the power button for 10 seconds when you power it on, and then release the button when the start-up options window appears. Select your start-up disk (usually your storage device on the left), then hold down the Shift key while you click Continue in Safe Mode. You can release the Shift key when the login window appears. Log in to the Mac (you might have to do this twice).



Restore from Time Machine
If you have backup of your system that you want to restore.

Reinstall macOS Big Sur
Install a new copy of macOS Big Sur onto your Mac.

Safari
Browse Apple Support to get help with your Mac.

Disk Utility
Repair or erase a disk using Disk Utility.

These are the main tools you can access when you boot into macOS Recovery.

If the Mac successfully boots into Safe Mode, you can try immediately restarting the Mac again and see if it will start-up normally. If it does, the problem might only be temporarily fixed. We recommend checking your login items, the apps, and services that automatically launch at start-up. To check your software login items, go to System Preferences > Users & Groups > Login Items. You'll need to go through the process of isolating what software is problematic by unchecking items, restarting, checking an item, restarting, repeat.

Boot into macOS Recovery

Disk Utility. If you've reached this step, there's likely a fairly large problem with your Mac, but it's not hopeless yet. When you boot into Recovery mode you can access Disk Utility, among other things. In this situation, Disk Utility is used to repair any issues with your start-up drive. Here are the instructions.

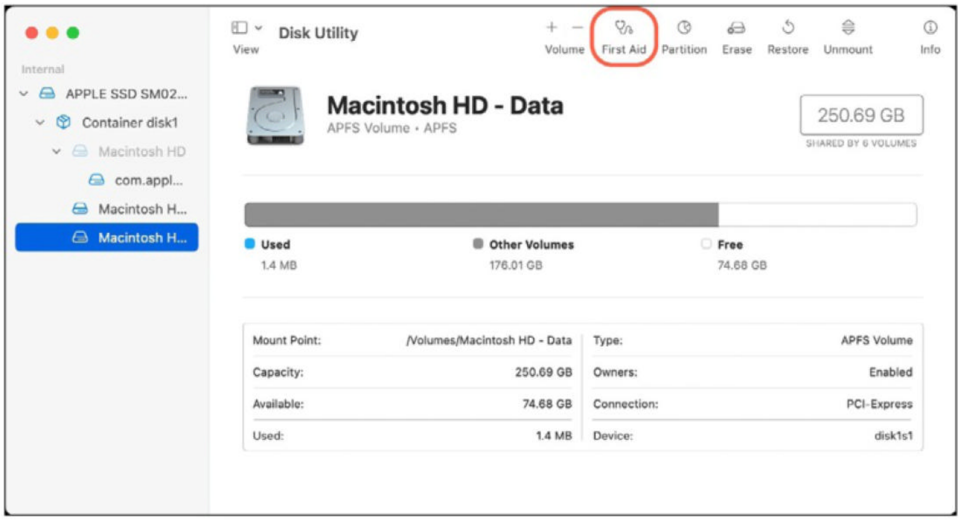
- **Intel Macs:** Turn off the Mac. Hold down Command + R and turn on the Mac, and keep holding down those keys.

- **M-series Macs:** Turn off the Mac. Press and hold down the power button until you see your start-up options, which will be your start-up disk and a gear icon called Options. Click Options.

After performing the boot procedure above, the Mac will ask for a password, and after you enter it, you'll see a window with four options. Click Disk Utility, which will launch the Disk Utility app. Now follow these instructions to repair your start-up disk.

1. Press Command + 2 to Show All Devices. The left column shows all the storage devices connected to your Mac, starting with the start-up device. Underneath each device submenus for each volume the device has.

2. Select the last volume that appears for the start-up device.



Mount Point:	/Volumes/Macintosh HD - Data	Type:	APFS Volume
Capacity:	250.69 GB	Owners:	Enabled
Available:	74.68 GB	Connection:	PCI-Express
Used:	1.4 MB	Device:	disk1s1

The First Aid button in Disk Utility.

Then click the First Aid button at the top. You'll need to confirm the task by clicking Run in the pop-up that appears. You'll also need to enter a password.

3. When the task is done, select the next volume above, and run First Aid again. Keep doing this up the chain until you've done the whole device.

4. Restart your Mac.

Reinstall macOS

You've reached the nuclear option, which is to reinstall macOS. Boot into macOS Recovery (as described above and select Reinstall macOS, which will launch the macOS installer, which will lead you through the process. It'll take about an hour or so, and you should be able to reinstall the Library and important bits without losing any of your data. However, if the system can't read your disk, you may need to erase your disk to install it.

On M-series Macs you'll be using Big Sur, Monterey, or Ventura but Intel Macs might be a little trickier.

Instead of the Command-R keystroke above, you can boot into macOS Recovery over the Internet using two methods. If you haven't updated the OS, use Shift + Option + Command + R during start-up to use the version of macOS that came with your Mac, or the closest version still available. You can also press Option-Command-R during start-up to get the latest macOS that is compatible with your Mac, assuming you've been keeping up with updates.

CALL APPLE SUPPORT

If, after all that, the Mac still won't complete its start-up process, it's time to contact Apple support. Before you do so, note down key points of behaviour the Mac exhibits while trying to start-up, such as when pauses occur, when the start-up stalls, any unusual things that show up on the screen, and so on. This information can help Apple support diagnose your problem. You can either call, chat online, or make an appointment at an Apple retail store.

Credit: Getty Images/Saturn_3

Help Desk

Solutions to all your Mac problems. **Glenn Fleishman** reports

HOW TO REMOVE A PERSONAL SCREEN TIME PASSCODE WHEN YOU'VE FORGOTTEN IT

Screen Time is a somewhat useful feature to help limit time on screens, online, and, particularly, apps. It's used by parents for children, but you can also use it for yourself. With Screen Time enabled, you can choose your own limits.

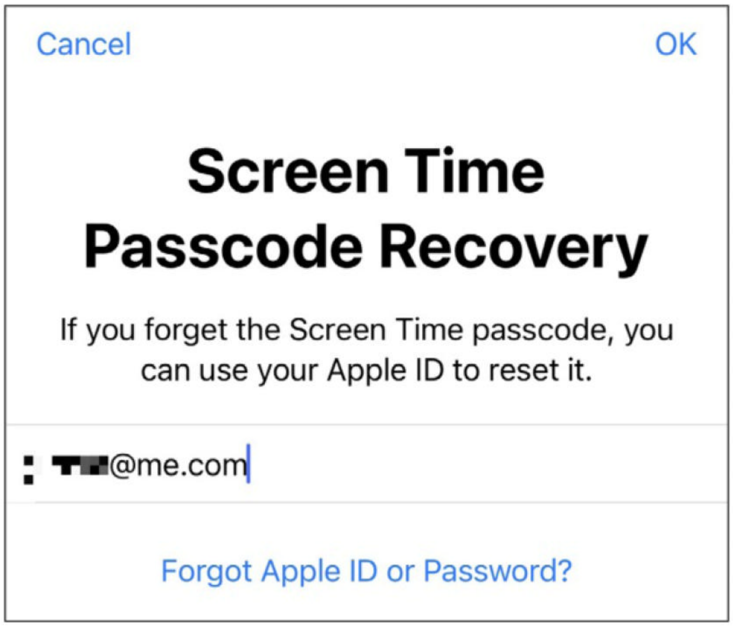
You can go one step further by setting a Screen Time passcode – you might want to have to enter a passcode instead of just tapping when you exceed limits you've set for yourself. (You might even ask someone else to set the code and not tell you if you need some additional, external help.)

When you set up a Screen Time passcode for your iCloud account, Apple prompts you to enter an Apple ID and its password to cache the code. It doesn't have to be the same Apple ID you use with iCloud.

What happens if you forget your Screen Time passcode for your children or yourself? With your kids, both iOS/iPadOS and macOS can typically retrieve the code from the Keychain using Touch ID or Face ID. Failing that and for your own lost passcode, you can use Apple ID-based recovery.

In iOS/iPadOS:

1. Go to Settings > Screen Time.
2. Choose a user if it's not your own passcode.



Screen Time Passcode Recovery

If you forget the Screen Time passcode, you can use your Apple ID to reset it.

[redacted]@me.com

Forgot Apple ID or Password?

Apple requires you enter an Apple ID and its password to make sure you can recover a Screen Time passcode were you to forget it.

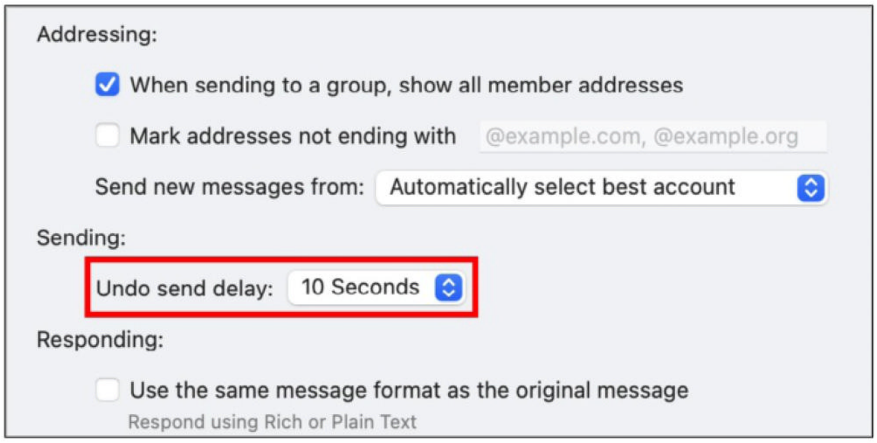
3. Tap Change Screen Time Passcode.
4. Tap Turn Off Screen Time Passcode.
5. Tap Forgot Passcode?
6. Enter the Apple ID username and password you used when setting up your passcode.
7. Tap OK.

In macOS:

1. Go to System Preferences > Screen Time (Monterey or earlier) or System Settings > Screen Time (Ventura).
2. Choose the user if other than you.
3.Click Options if you don't see the Screen Time: On label at the upper-right corner.
4. Uncheck or disable Use Screen Time Passcode.
5. If not prompted to use Touch ID, enter the Apple ID account and password you used when setting it up.
6. Click OK.

HOW TO CHANGE THE DELAY BEFORE APPLE MAIL SENDS YOUR MESSAGES

What happens when you click or tap Send on an email and realize you forgot an attachment,



Addressing:

☑ When sending to a group, show all member addresses

□ Mark addresses not ending with @example.com, @example.org

Send new messages from: Automatically select best account

Sending:

Undo send delay: 10 Seconds

Responding:

□ Use the same message format as the original message
Respond using Rich or Plain Text

As highlighted in red, you can set the delay for when messages are sent, allowing a quick 'unsend'.

absent-mindedly signed a letter to your boss with 'all my love', or suddenly flashed that you typed 'pubic' not 'public'? Apple added an option in iOS 16/iPadOS 16 and macOS Ventura called Undo Send, which is a bit of a misnomer: it's really 'delay until sending'.)

Apple turns this option on by default to 10 seconds. I know, because I never enabled it and both my iPhone and Mac. If you want to disable or change this interval:

- In iOS/iPadOS, go to Settings > Mail and tap Undo Send Delay. You can change it to Off or 10, 20, or 30 seconds.

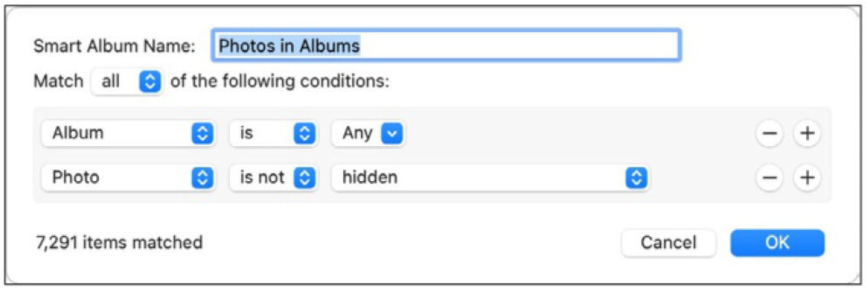
- In macOS in the Mail app, choose Mail > Settings > Composing. You can uncheck "Undo send delay," or check that box and set it to 10, 20 or 30 seconds via a pop-up menu.

Apple thinks 10, 20, or 30 seconds is long enough. For true deliberation, the company should analyze your email and suggest a duration: or some messages, perhaps 30 minutes; others, a lifetime.

HOW TO TAG IMAGES TO FIND OUT WHICH ALBUMS THEY'RE IN WITHIN PHOTOS FOR MACOS

Photos for macOS offers a smart album feature that lets you create a set of search criteria to produce a dynamic album based on characteristics found in and attached to images and videos. It's powerful, as it lets you group and filter media in quite sophisticated ways. But there's an obvious omission that Apple hasn't corrected several years after the introduction of the Photos app: you can't determine in which albums a given photo or movie has been referenced.

This makes some sense. The unit in Photos is a photo or video, not an



Smart Album Name: Photos in Albums

Match all of the following conditions:

Album is Any

Photo is not hidden

7,291 items matched

See all the photos found in any album by adding a single criterion – hidden.

album, which is a collection of those things. However, based on reader questions, it's an ongoing frustration. You can simulate determining what albums media are in through the application of keywords, though it requires ongoing manual effort to maintain.

1. Go to a given album, like one that contains pictures of a trip to Columbus, Ohio.
2. Select all the images in the album (choose Edit > Select All, for instance).
3. Display the Info palette (Window > Info or press Command + I).
4. In the Keyword field, enter a unique descriptor for that album, like columbusoh or columbus-2022.
5. Repeat for every album to which you want to apply this option.

Now you can view any item in an album to see which albums it's in.

There's another trick to finding all your media in any album:

1. Choose File > New Smart Album.
2. Set the first criterion to Album, is, Any; click the + (plus) button at right to add a second; set it to Photo, is not, hidden. (While it says 'Photo', it includes videos.)
3. Name it descriptively, like 'Photos in Albums'.
4. Click OK.

You can view the 'Photos in Albums' smart folder, select an image or video, and view the associated keywords. This will show you to which albums you've added the media. You have to navigate to an album to see all the media it contains, but this provides a clue.

To keep this working, you need to add keywords to photos and movies as you add them to albums.

REVIEWED:
MAC MINI (M2 PRO)

Macworld

MARCH 2023

APPLE'S EPIC NEW LAPTOP

16-INCH MACBOOK PRO (M2 PRO)

NEXT-GEN CHIPS: M2 PRO VS M2 MAX

FOUNDRY

an IDG, Inc. company