

4 simple ways to dramatically increase your MacBook's security

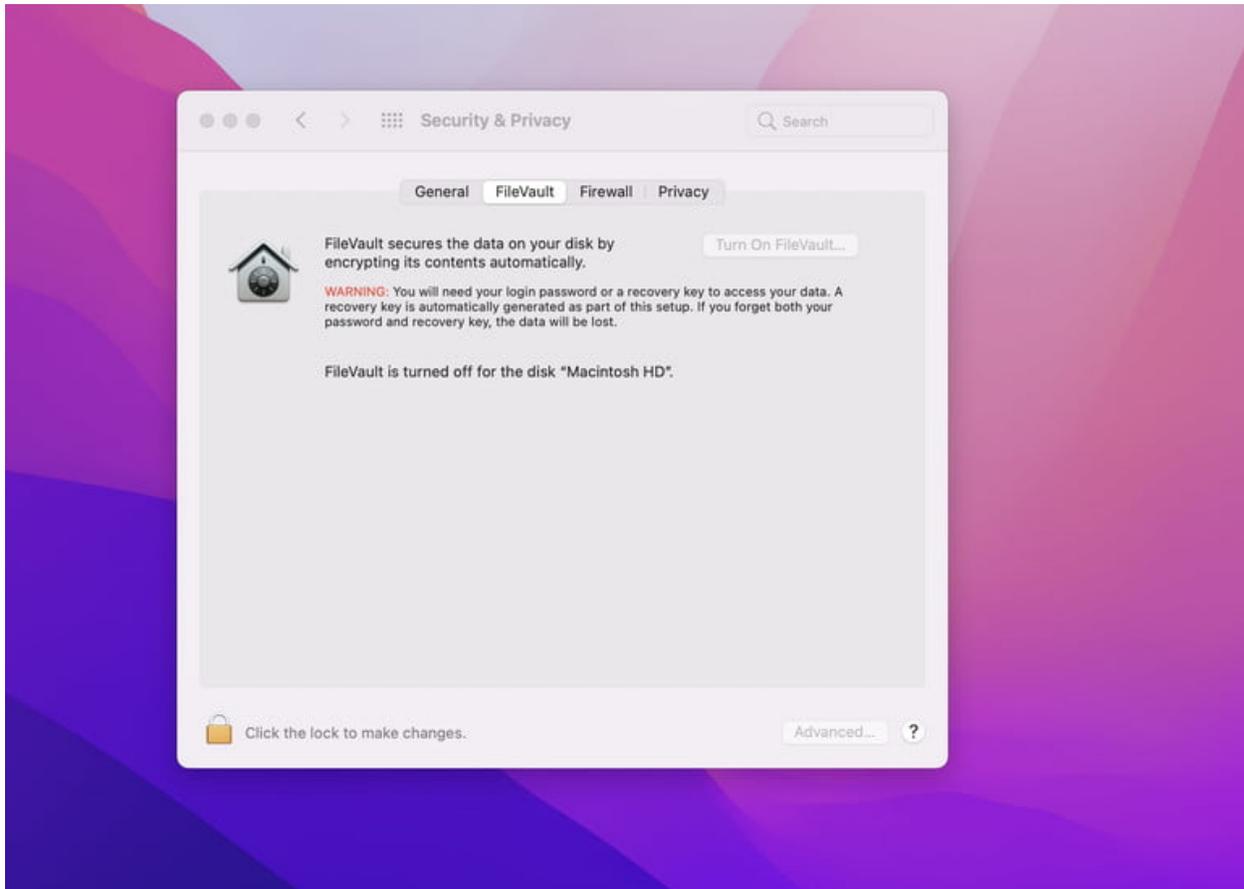
By Arif Bacchus

October 10, 2021 6:00AM - digital trends

Popular perception might lead you to believe that MacBooks and other Mac machines are already safe and immune to viruses and similar security issues. But don't let that fool you. Macs are known to be vulnerable to viruses and even some of the same security flaws that plague PCs.

Sure, [you can use antivirus software](#) on MacOS to protect yourself, but taking a few simple steps can also give you extra piece of mind. Here are four ways you can keep your MacBook safe.

Turn on FileVault



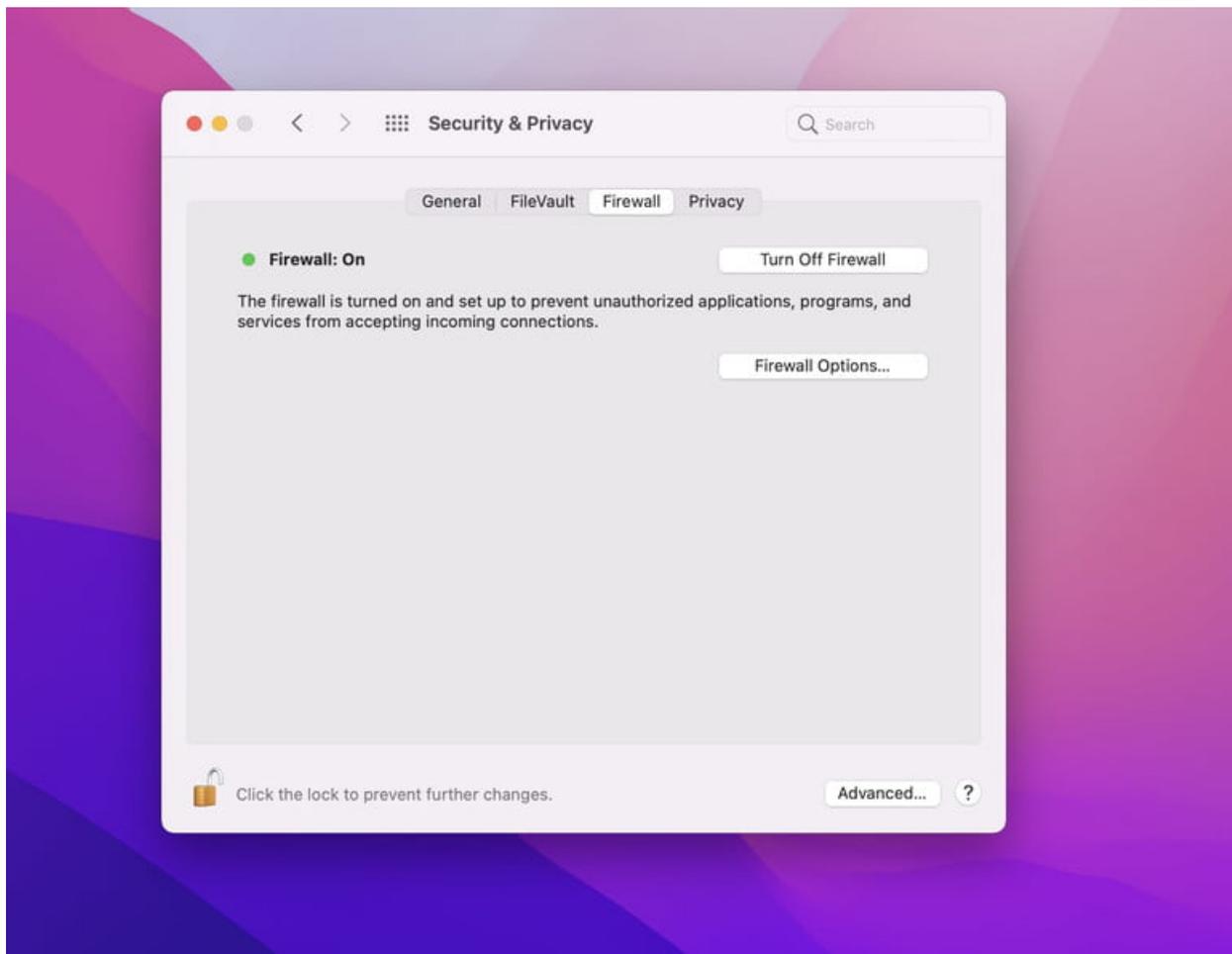
Arif Bacchus/Digital Trends

Our first tip is one that might have slipped under your radar. As part of the security features in your MacBook, you might have noticed something called **FileVault**. This is a setting that can help encrypt all the data on your main MacOS hard drive. With it, your data will be encrypted using the XTS-AESW 128 encryption standard. This makes it harder for someone to access your files if your Mac machine were to be stolen.

FileVault is available on Mac OS X Lion or later. You can get to it by clicking the Apple Menu and choosing System Preferences > Security and Privacy > FileVault tab.

When turned on, you'll always have to log into your MacBook with your account password. If you forget your MacBook password and you want to unlock your data, you can use your Apple ID as an alternative to unlocking. If you lose both your account password and your FileVault recovery key, though, you won't be able to log in to your Mac or access the data on your startup disk. Any encryption you start will happen in the background while you're connected to AC power.

Use a firewall



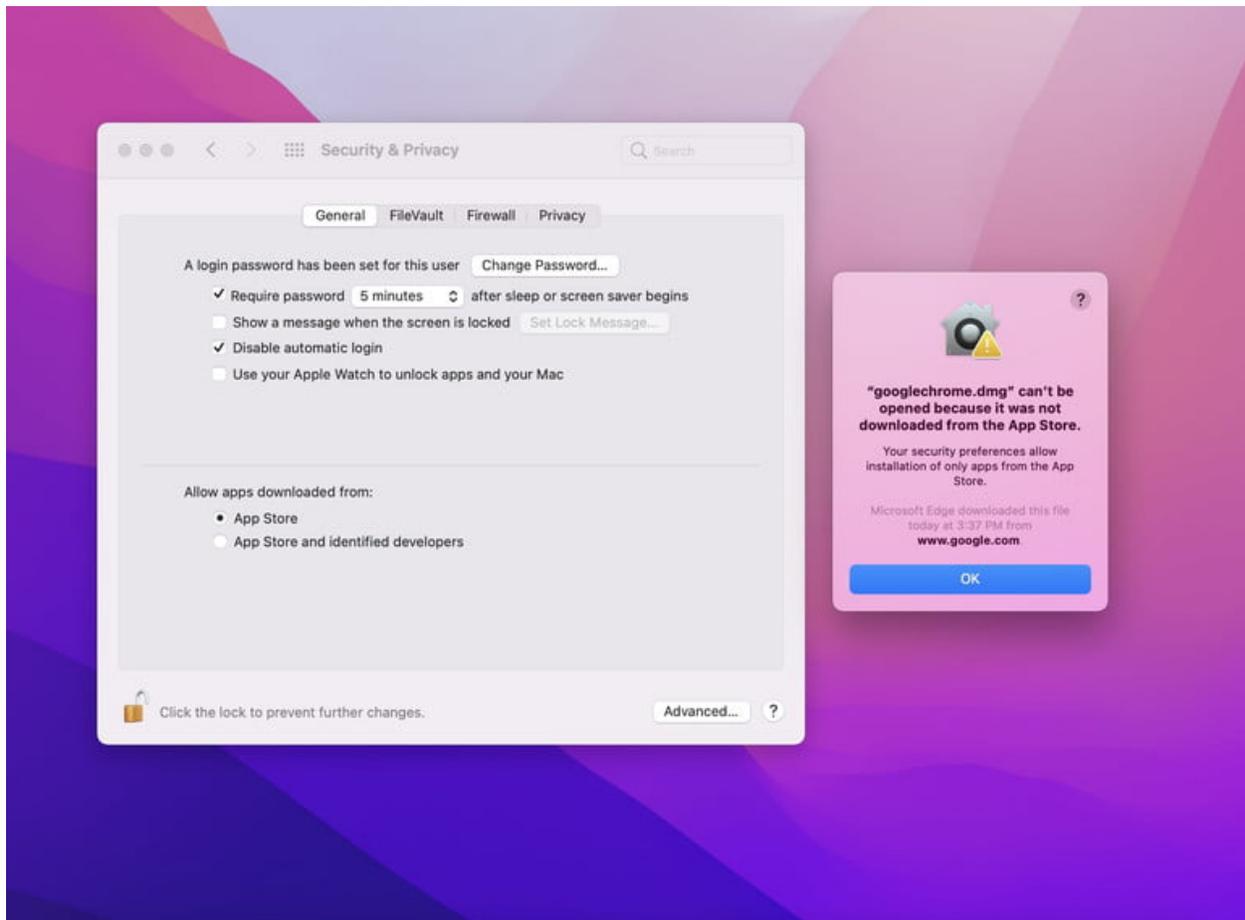
Arif Bacchus/ Digital Trends

Firewalls are something we talked about before for Windows machines. On Macs, though, you can use the in-built one-way Firewall in a similar way to help control connections made to your computer from other computers on your local network. There's a one-way firewall built right in, and it basically can help unauthorized apps from taking control of network ports already open for apps you've approved. Here's how to use it.

Head to the Apple Menu, choose System Preferences > Security and Privacy > Turn on Firewall. After you do this, you can specify certain apps that can connect or block all incoming connections, allow built-in apps to accept connections, or downloaded apps only. You even can choose stealth mode, which will make it more difficult for hackers and malware to find your Mac.

Keep in mind, we're calling the built-in firewall a one-way firewall because it only offers protections on inbound networks. You'll need a paid outbound firewall for true protection from the most sophisticated attacks, as it notifies you about something you downloaded that's connecting to networks without your permission.

Change app security settings



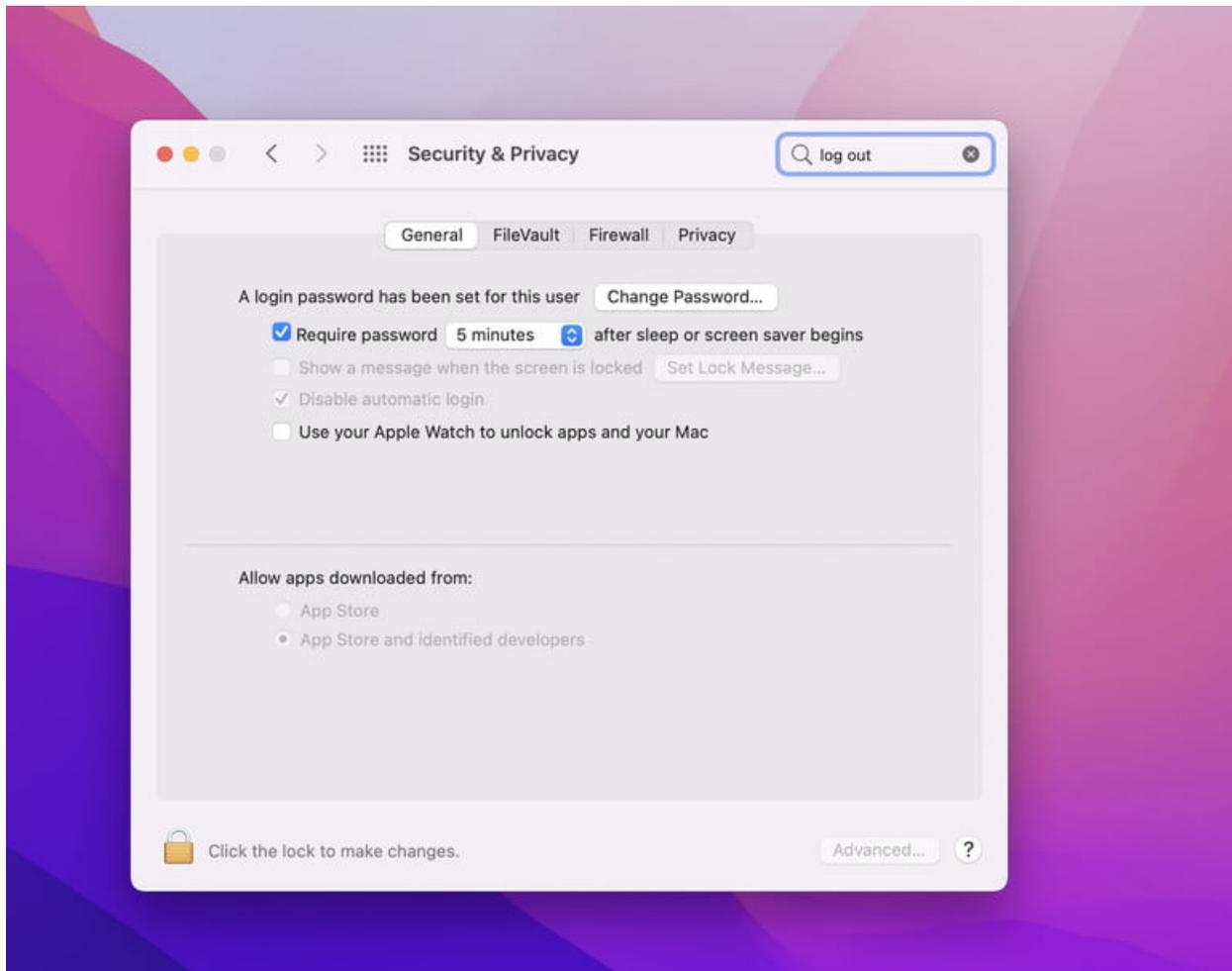
Officially, [Apple notes](#) that the safest place to get apps for your MacBook is from the App Store. All apps listed on the store are reviewed by Apple to ensure that there's no malware, viruses, or other things that can damage your Mac. Of course, there comes a time when you'll need to download extra software from the web that's not on the App Store (like Chrome, or Photoshop,) so Apple has set the Security and Privacy Settings to allow the App Store, as well as Identified Developers, by default.

But if you really want your Mac to be super secure, you can change the setting to App Store only. Once you're at a point

where you're confident you won't need to download extra apps, this ensures that something from your downloads won't sneak onto your system and hijack your Mac without you knowing.

You can change this setting by going to the Apple Menu and choosing System Preferences > Security and Privacy > General, then scrolling down to Allowed apps downloaded from. In this section, you can switch things up so that only apps from the App Store will download. You also can visit this page to grant exceptions to some apps via the Open Anyway button as you see fit.

Always keep your computer locked when you step away



Arif Bacchus/ Digital Trends

Our last tip is one that might seem a bit obvious but is worth mentioning anyway. If you happen to step away from your laptop at any time, we suggest that you always keep it locked. We also suggest that you enable the option to require a password once your Mac comes back from sleep or when the screen saver turns on.

You can set up your Mac to log out when not in use by going to the Apple Menu, then choosing System Preferences, > Security & Privacy. From there, click Advanced, then Log out after... minutes of inactivity. We also suggest going to Security & Privacy, then General , and selecting Require password... after sleep or screen saver begins.

As our final tip, we also suggest using Hot Corners. With Hot Corners, you can mouse over to a corner of the screen to automatically lock your Mac. Visit Desktop & Screen Saver > Mission Control > Hot Corners. You can then choose a modifier key (like command) and one of the corners for Lock Screen.

original article:

https://www.digitaltrends.com/computing/four-ways-increase-security-of-your-macbook/?utm_medium=flipdigest.ad.20211010.carousel&utm_source=email&utm_content=&utm_campaign=campaign