



Safely open apps on your Mac

macOS includes a technology called Gatekeeper, that's designed to ensure that only trusted software runs on your Mac.

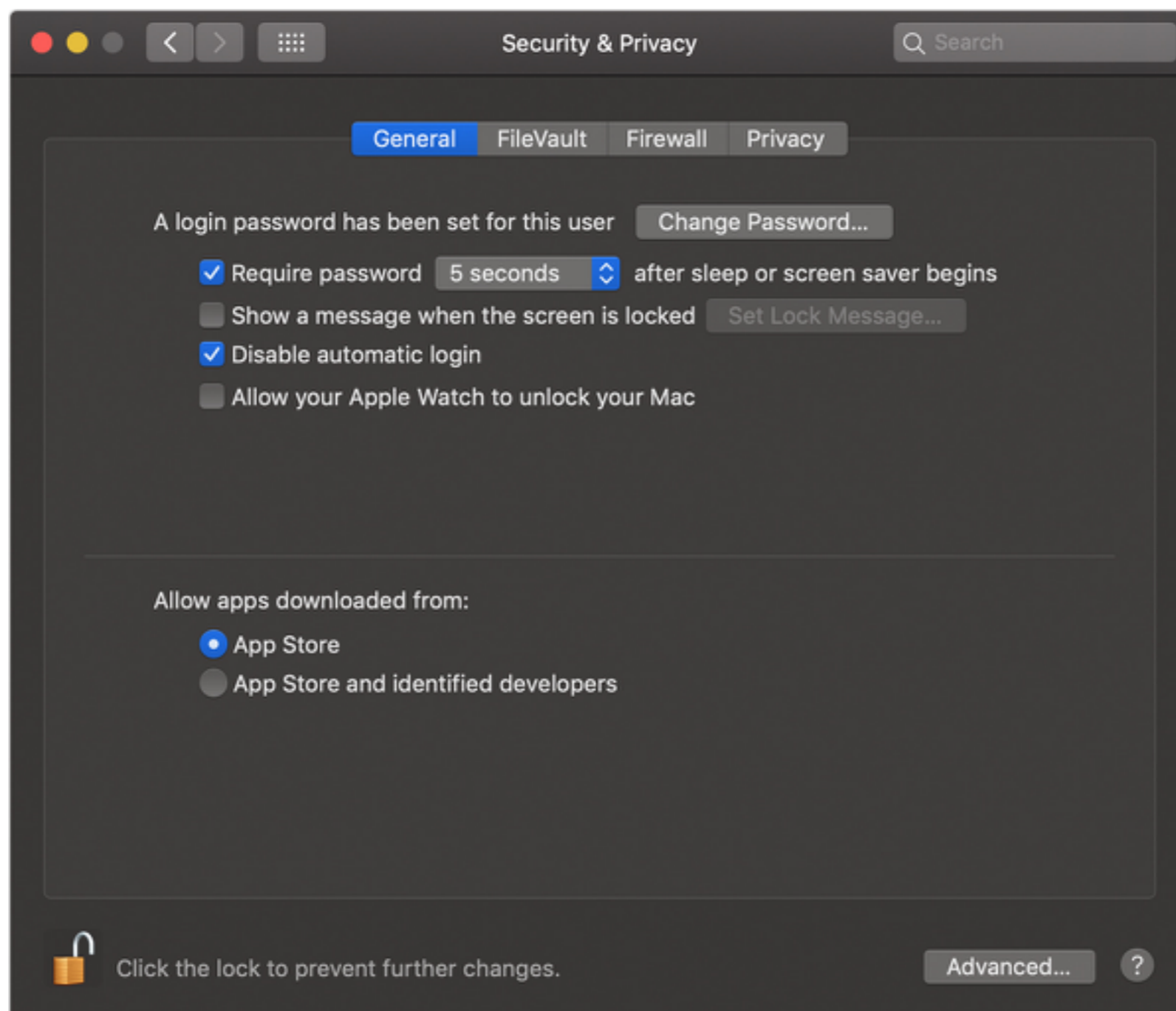
The safest place to get apps for your Mac is the App Store. Apple reviews each app in the App Store before it's accepted and signs it to ensure that it hasn't been tampered with or altered. If there's ever a problem with an app, Apple can quickly remove it from the store.

If you download and install apps from the internet or directly from a developer, macOS continues to protect your Mac. When you install Mac apps, plug-ins, and installer packages from outside the App Store, macOS checks the Developer ID signature and notarization status to verify that the software is from an identified developer and that it has not been altered. With macOS Mojave, developers can also have their app notarized by Apple—an indication that the app was uploaded to Apple and passed a security check before it was distributed.

View the app security settings on your Mac

By default, the security and privacy preferences of your Mac are set to allow apps from the App Store and identified developers. For additional security, you can choose to allow only apps from the App Store.

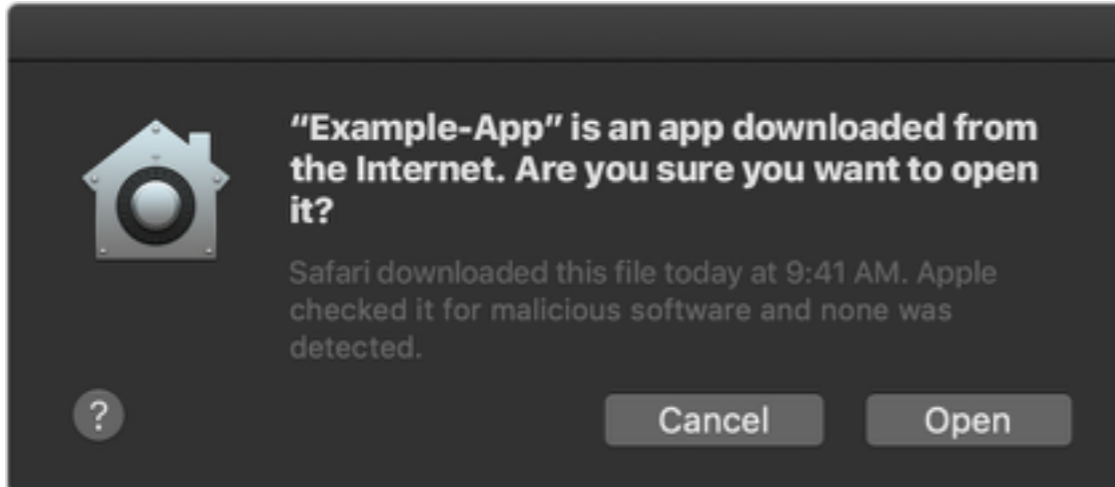
In System Preferences, click Security & Privacy, then click General. Click the lock and enter your password to make changes. Select App Store under the header "Allow apps downloaded from."



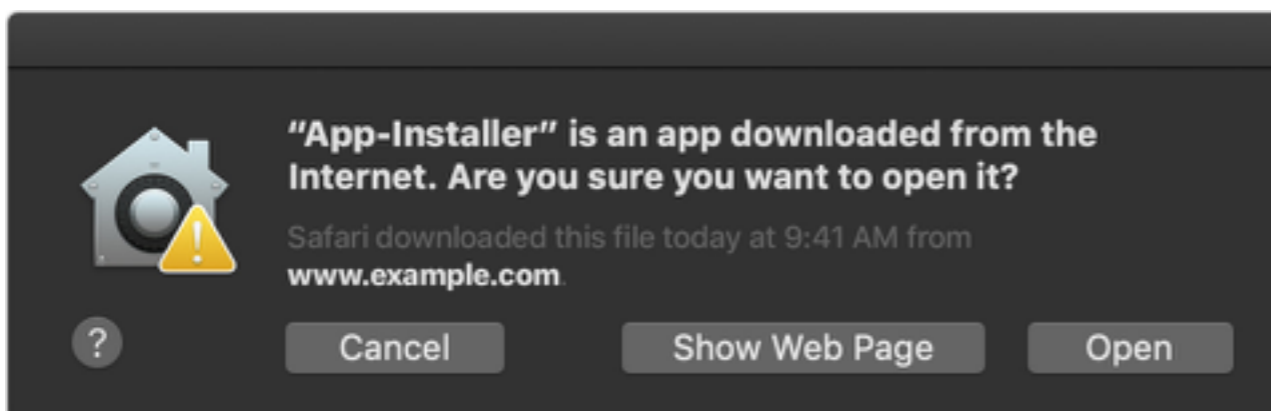
Open a developer-signed or notarized app

If your Mac is set to allow apps from the App Store and identified developers, the first time that you launch an app from an identified developer, your Mac asks if you're sure you want to open it.

An app that has been notarized by Apple indicates that it passed a security check:



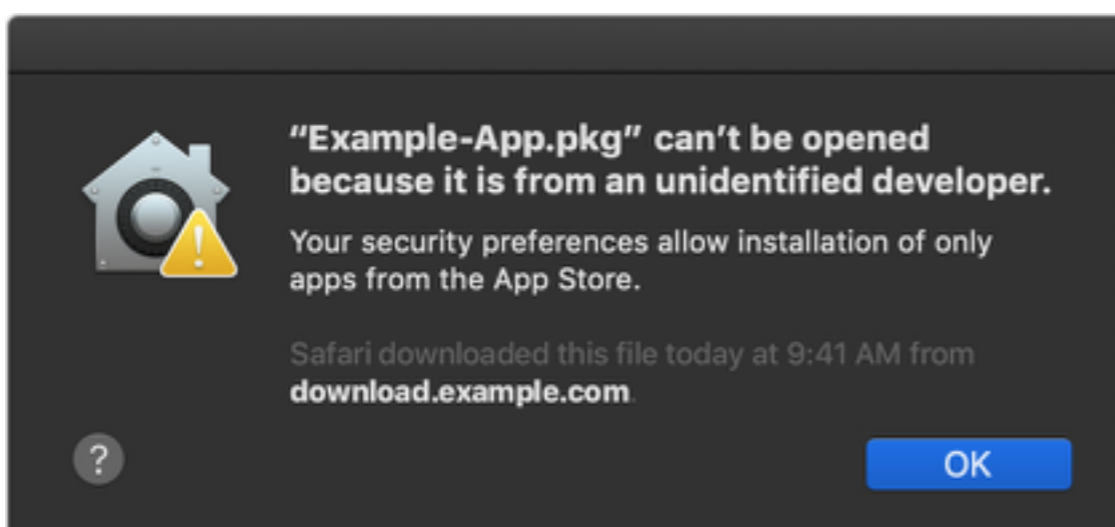
Apps that haven't been notarized show a yellow warning icon:



If you see a warning message and can't install an app

If you have set your Mac to allow apps only from the App Store and you try to install an app from elsewhere, your Mac will say that the app is not from the App Store.

If your Mac is set to allow apps from the App Store and identified developers, and you try to install an app that isn't registered with Apple by an identified developer, you also get a warning.

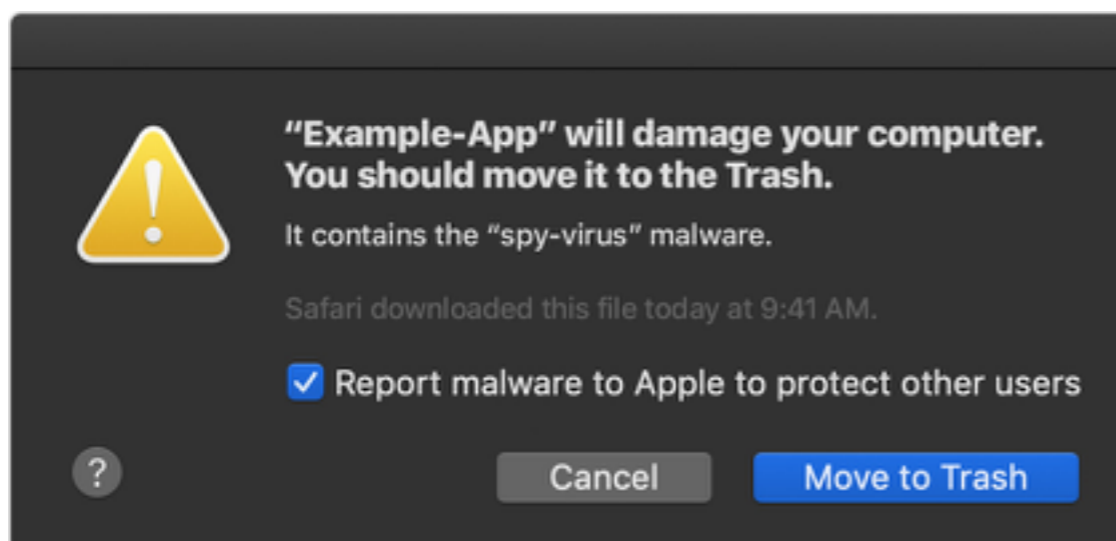


These messages don't necessarily mean that something is wrong with the app. For example, some apps were written before Developer ID registration. If you see a warning, it means that the app has not been signed by the developer, so macOS can't check whether the app has been modified or broken since it was released.

You may want to look for a later version of the app in the App Store or look for an alternative app.

If macOS detects a malicious app

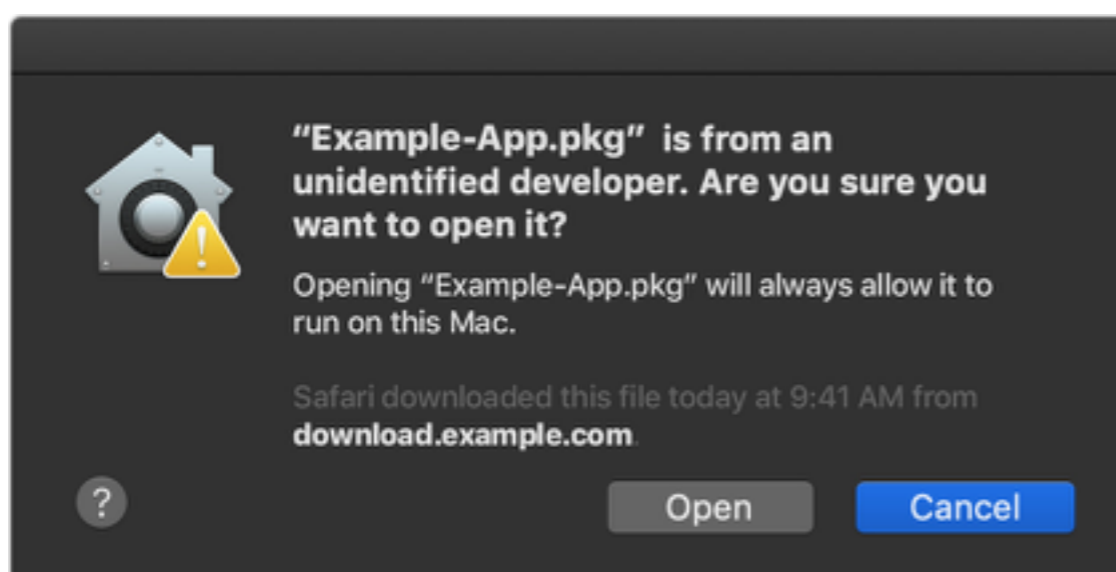
If macOS detects a problem with an app—for example, that it has malicious content or was modified since it was checked—it will notify you when you try to open it and ask you to move it to the Trash.



Install an app from an unidentified developer

If you're certain that an app you want to install is from a trustworthy source and hasn't been tampered with, you can temporarily override your Mac security settings and open it.

In the Finder, Control-click the app, choose Open from the menu, and in the dialog that appears, click Open. Enter your admin name and password when prompted.



The app is now saved as an exception to your security settings, and you can open it in the future by double-clicking it, just as you can any authorized app.

Information about products not manufactured by Apple, or independent websites not controlled or tested by Apple, is provided without recommendation or endorsement. Apple assumes no responsibility with regard to the selection, performance, or use of third-party websites or products. Apple makes no representations regarding third-party website accuracy or reliability. Risks are inherent in the use of the Internet. Contact the vendor for additional information. Other company and product names may be trademarks of their respective owners.

Published Date: September 25, 2018