Safely Open Apps on your Mac

Gatekeeper

Apple, Inc.

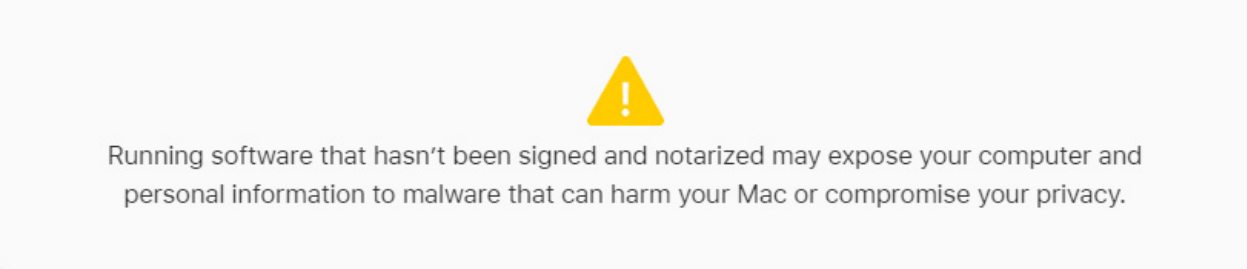
April 30, 2021

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 to verify that the software is from an identified developer and that it has not been altered. By default, macOS Catalina and later also requires software to be notarized, so you can be confident that the software you run on your Mac doesn't contain known malware. Before opening downloaded software for the first time, macOS requests your approval to make sure you aren't misled into running software you didn't expect.

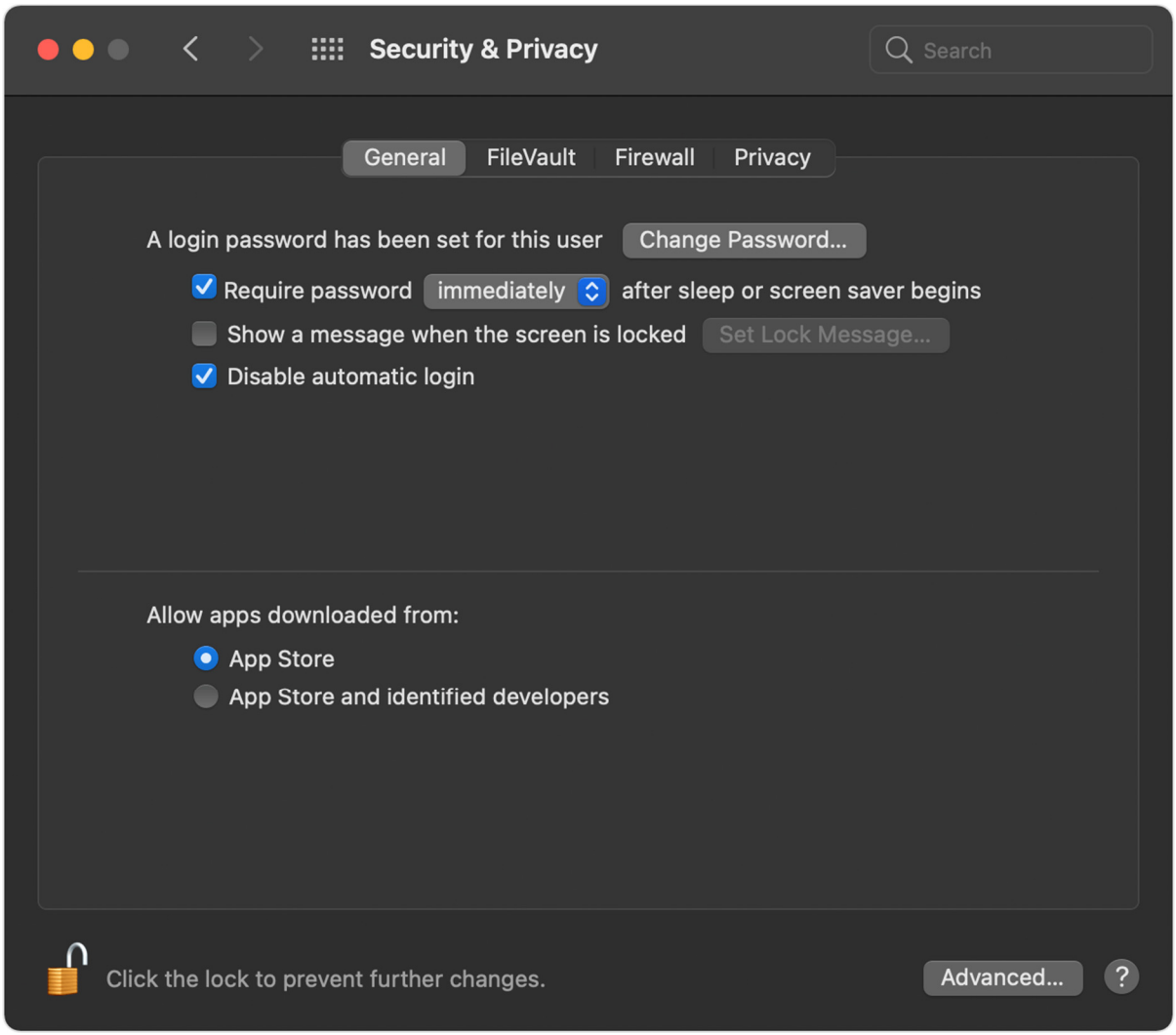


The warning messages displayed below are examples, and it's possible that you could see a similar message that isn't displayed here. Please use caution if you choose to install any software for which your Mac displays an alert.

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 chose to allow only apps from the App Store.

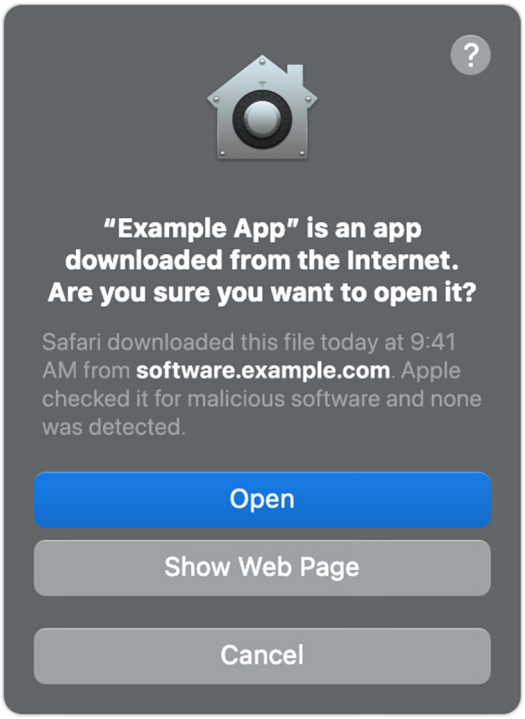
In System Preferences, click Security & Privacy, then click General. Click the lock and enter your password to make changes. Select App Store under the header “Allow apps downloaded from.”



Open a developer-signed or notarized app

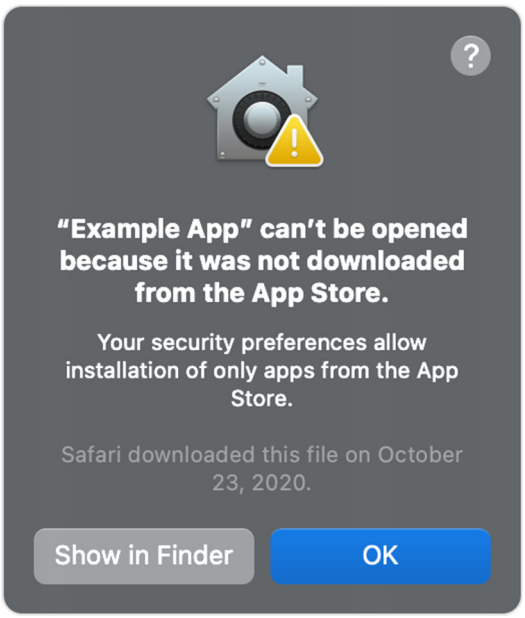
If your Mac is set to allow apps from the App Store and identified developers, the first time that you launch a new app, your Mac asks if you're sure you want to open it.

An app that has been notarized by Apple indicates that Apple checked it for malicious software and none was detected.

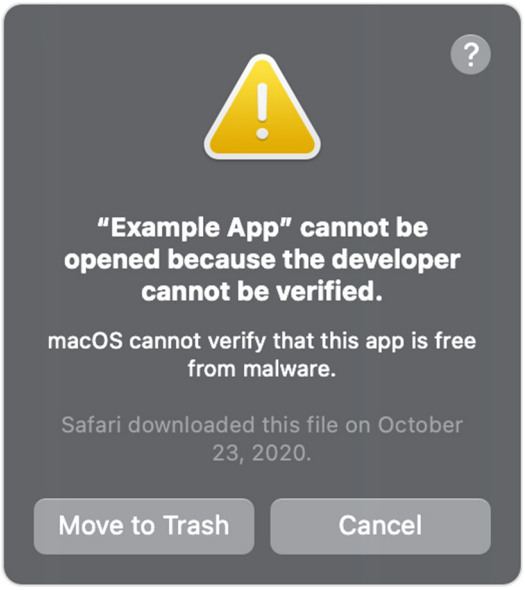


If you see a warning message and can't install an app

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 can't be opened because it was not downloaded 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 signed by an identified developer and—in macOS Catalina and later—notarized by Apple, you also see a warning that the app cannot be opened.



If you see this warning, it means that the app was not notarized, and Apple could not scan the app for known malicious software.

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

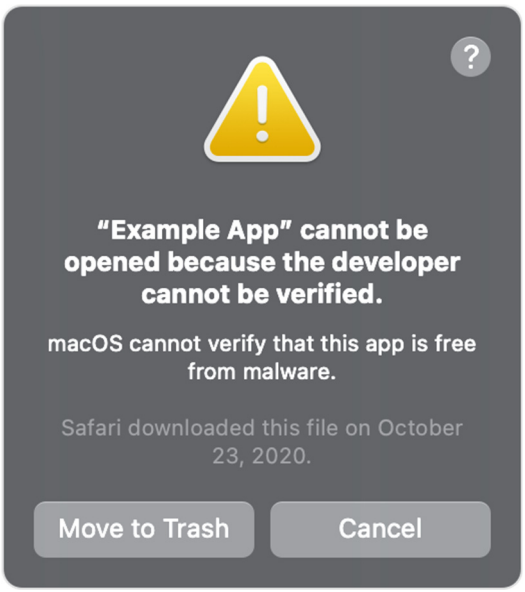
If macOS detects a malicious app

If macOS detects that software has malicious content or its authorization has been revoked for any reason, your Mac will notify you that the app will damage your computer. You should move this app to the Trash and check "Report malware to Apple to protect other users."

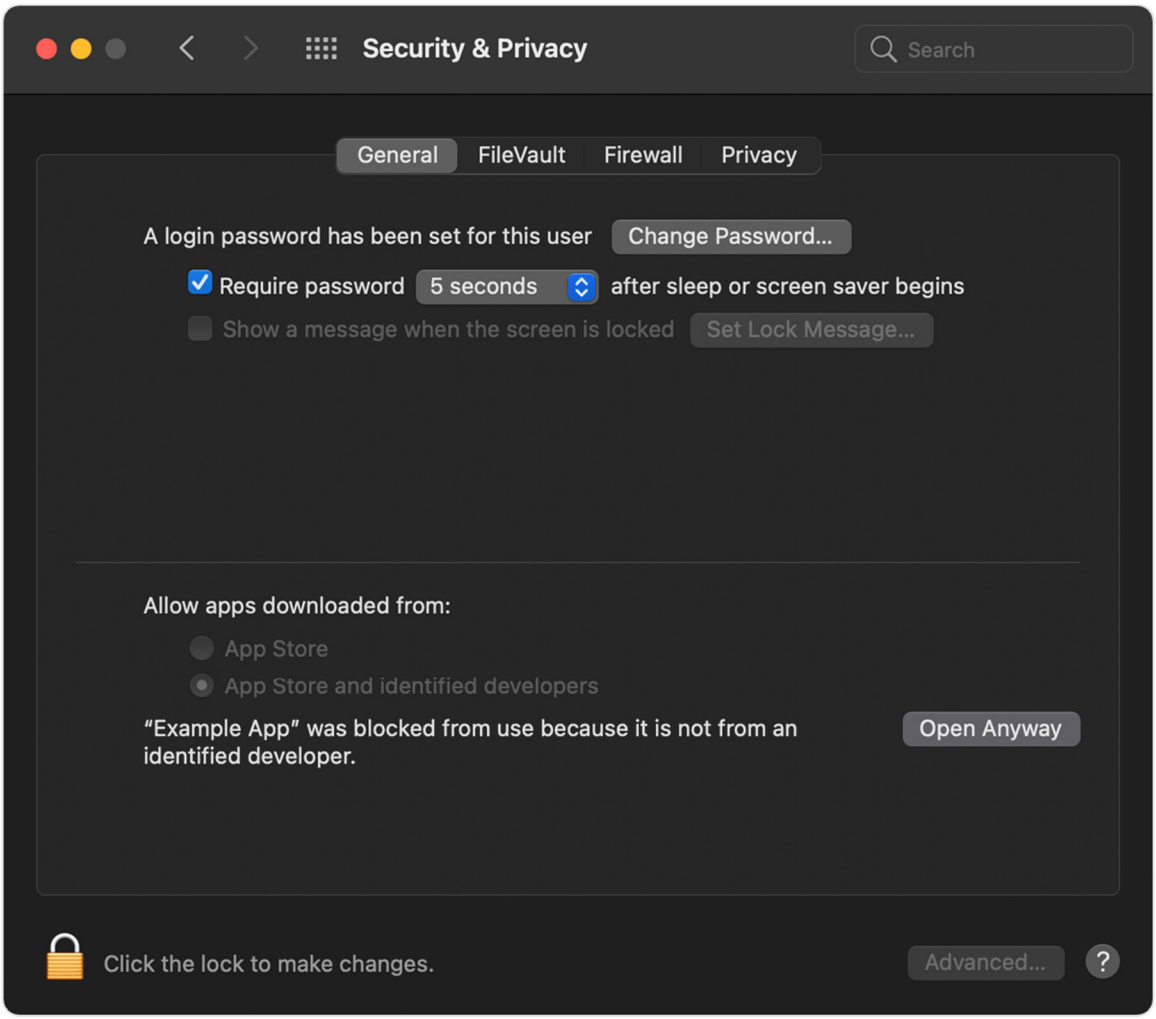
If you want to open an app that hasn't been notarized or is from an unidentified developer

Running software that hasn't been signed and notarized may expose your computer and personal information to malware that can harm your Mac or compromise your privacy. 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 to open it.

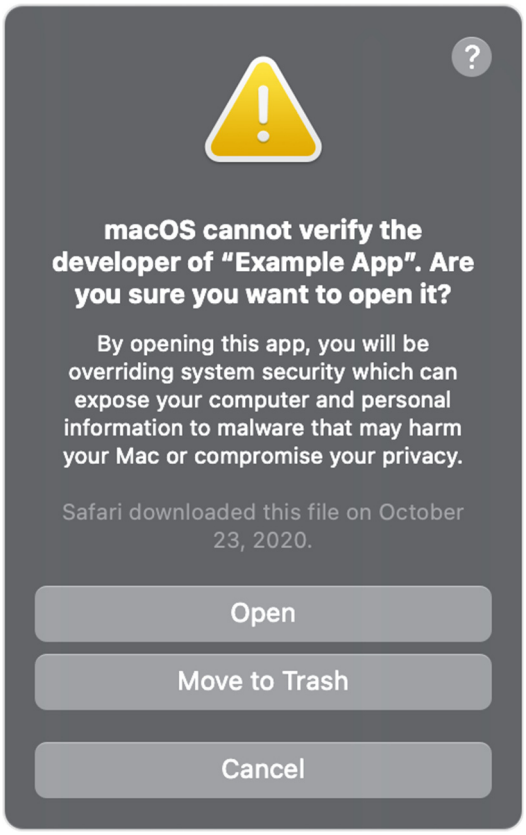
If you still want to open an app for which the developer cannot be verified, open System Preferences.*



Go to Security & Privacy. Click the Open Anyway button in the General pane to confirm your intent to open or install the app.



The warning prompt reappears, and if you're absolutely sure you want to open the app anyway, you can click Open.



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.

Privacy protections

macOS has been designed to keep users and their data safe while respecting their privacy.

Gatekeeper performs online checks to verify if an app contains known malware and whether the developer’s signing certificate is revoked. We have never combined data from these checks with information about Apple users or their devices. We do not use data from these checks to learn what individual users are launching or running on their devices.

Notarization checks if the app contains known malware using an encrypted connection that is resilient to server failures.

These security checks have never included the user's Apple ID or the identity of their device. To further protect privacy, we have stopped logging IP addresses associated with Developer ID certificate checks, and we will ensure that any collected IP addresses are removed from logs.

In addition, over the the next year we will introduce several changes to our security checks:

- A new encrypted protocol for Developer ID certificate revocation checks
- Strong protections against server failure
- A new preference for users to opt out of these security protections

* If you're prompted to open the app in Finder and you're sure you want to open it despite the warning, you can control-click the app, choose Open from the menu, and then click Open in the dialog that appears. Enter your admin name and password to open the app.

Published Date: April 30, 2021