App Is Locked Mac

How to remove YOUR APPLE COMPUTER HAS BEEN LOCKED from Mac?

- Mac Pro Locked Up
- Delete Locked App Mac
- Close Locked App Mac

What is YOUR APPLE COMPUTER HAS BEEN LOCKED?

Managing locked files in OS X. If you can't edit a file in any application, including the Terminal, then it may have a lock flag associated with it. I believe you followed the official guides and you tried to factory reset your Mac and you find yourself in this situation: the disk is locked and you cannot select it for re-installation. You already tried to partition the disk multiple times but it keeps erroring with the Error: -61. In this case you can try.

'YOUR APPLE COMPUTER HAS BEEN LOCKED' is a fake pop-up error message claiming that the system has been infected. This message is displayed by malicious website. Users often visit this website inadvertently - they are redirected by potentially unwanted programs (PUPs) that infiltrate systems without consent. Research shows that as well as causing unwanted redirects, PUPs also deliver intrusive online advertisements and continually monitor Internet browsing activity.

'YOUR APPLE COMPUTER HAS BEEN LOCKED' is unique, since it only targets the Mac OS. This error message states that a system infection has been detected and that personal data (logins/passwords, credit card details, etc.) have been stolen. Therefore, victims must immediately remove the virus by contacting certified technicians via the telephone number ('**1-877-271-8604**') provided. In fact, research shows that this message is a scam. The virus does not exist. The pop-up is designed only to trick victims into calling fake technical support and paying for services that are not required. Therefore, ignore this pop-up and never attempt to contact these people. Be aware that potentially unwanted programs deliver pop-up, coupon, banner, and other similar ads. To achieve this, developers employ a 'virtual layer' - a tool that enables placement of third party graphical content on any site. The displayed ads often conceal underlying content of visited websites, significantly diminishing the Internet browsing experience. In addition, some lead to malicious websites and even accidental clicks can result in high-risk computer infections. Potentially unwanted programs also track Internet browsing activity by gathering IP addresses, search queries, URLs visited, and other similar information that might contain personal details. The data is shared with third parties (potentially, cyber criminals) who generate revenue by misusing personal details. Therefore, the presence of including, for example, Immediately Call Apple Support, Mac Detected TAPSNAKE Infection, and Mac Malware Warning Alert ! All claim that the system is infected or damaged in similar ways and victims are encouraged to contact technical support. In fact, fake error messages are designed to trick victims into paying for services that are not required. Therefore, they should never be trusted. The purpose if PUPs is identical - they are designed only to generate revenue for the developers. Promises to provide so-called 'useful features' are merely attempts to give the impression of legitimacy, whereas PUPs cause unwanted redirects, gather personal information, and deliver intrusive online advertisements.

How did potentially unwanted programs install on my computer?

As mentioned above, PUPs infiltrate systems without users' consent. This is since they are distributed using a deceptive software marketing method called 'bundling' - stealth installation of third party apps with regular software. Developers know that users often rush the download/installation processes and skip most steps. Therefore, bundled programs are hidden within the 'Custom/Advanced' settings. Users who rush and skip this section risk inadvertently installing rogue applications.

How to avoid installation of potentially unwanted applications?

There are two simple steps you should take to prevent this situation. Firstly, never rush when downloading and installing software. Select the 'Custom/Advanced' settings and closely analyze each step. Secondly, decline offers to download/install additional apps and opt-out of those already included.

Text presented within the first YOUR APPLE COMPUTER HAS BEEN LOCKED variant:

YOUR APPLE COMPUTER HAS BEEN LOCKED
Your Computer is infected with an adware or malware causing you to see this popup.
This may happen due to obsolete virus protections.
To fix, please call Apple Support at 1-877-271-8604 immediately. Please ensure you do not restart your computer to prevent data loss.
Possibility of Data & Identity theft, if not fixed immediately.
YOUR APPLE COMPUTER HAS BEEN BLOCKED*
YOUR APPLE COMPUTER HAS BEEN LOCKED !!
System has been infected due to unexpected error!
Please Contact Apple 1-877-271-8604 Immediately!
to unblock your computer.
Suspicious Activity Detected. Your Browser might have been hijacked or hacked.
ANONYMOUS ACTIVITY
Private and Financial Data is at RISK:
. Your credit card details and banking information

. Your e-mail passwords and other account passwords
. Your Facebook, Skype, AIM, ICQ and other chat logs
. Your private & family photos and other sensitive files
. Your webcam could be accessed remotely by stalkers
IMMEDIATELY CALL APPLE SUPPORT AT 1-877-271-8604
MORE ABOUT THIS INFECTION:
Seeing these pop-up's means that you may have a virus installed on your computer which puts the security of your personal data at a serious risk.
It's strongly advised that you call the number above and get your computer inspected before you continue using your internet, especially for Shopping or Banking.
Call immediately for assistance.
Contact Apple Support At (1-877-271-8604)

Another variant of YOUR APPLE COMPUTER HAS BEEN LOCKED scam:

Text presented within the second YOUR APPLE COMPUTER HAS BEEN LOCKED variant:

Your Computer is infected with an adware or malware causing you to see this popup.
This may happen due to obsolete virus protections.
To fix, please call Apple Support at 1-877-271-8604 immediately. Please ensure you do not restart your computer to prevent data loss.
Possibility of Data & Identity theft, if not fixed immediately.

Screenshot of another variant of this scam targeted at **iOS** users (iPhone, iPad, etc), cyber criminals behind this scam are using **+1(844)899-4845** or **+1-866-217-1442** phone numbers. Users who come across this scam **should simply close the tab of the scam website**:

Text presented in this iOS tech support scam:

YOUR APPLE DEVICE HAS BEEN BLOCKED (or *YOUR APPLE DEVICE HAS A VIRUS*)

Apple iOS Alert!!
PEGASUS (SPYWARE) ACTIVATED
System might be infected due to unexpected error! Please Contact Apple Care +1(844)899-4845 Immediately! For assistance regarding how to remove it.
Suspicious Activity Detected. Your Browser has been compromised. Possible network damages if virus not removed immediately. DATA AT RISK:
- Your credit card details and banking information
- Your e-mail passwords and other account passwords
- Your Facebook, Skype, AIM, ICQ and other chat logs
- Your private & family photos and other sensitive files
- Your webcam could be accessed remotely by stalkers.

IMMEDIATELY CALL APPLE CARE AT +1(844)899-4845
MORE ABOUT THIS INFECTION:
Seeing these pop-up's means that your DEVICE which puts the security of your personal data at a serious risk. It's strongly advised that you call the number above and get your DEVICE inspected before your continue using your Internet, especially for Shopping or banking. Call immediately for assistance, Contact Apple Care at +1(844)899-4845

Instant automatic Mac malware removal:Manual threat removal might be a lengthy and complicated process that requires advanced computer skills. Combo Cleaner is a professional automatic malware removal tool that is recommended to get rid of Mac malware. Download it by clicking the button below:
▼ **DOWNLOAD** Combo Cleaner for MacBy downloading any software listed on this website you agree to our Privacy Policy and Terms of Use. To use full-featured product, you have to purchase a license for Combo Cleaner. Limited three days free trial available.

Quick menu:

- STEP 1. Remove adware related files and folders from OSX.
- STEP 2. Remove YOUR APPLE COMPUTER HAS BEEN LOCKED pop-up from Safari.
- STEP 3. Remove YOUR APPLE COMPUTER HAS BEEN LOCKED pop-up from Google Chrome.
- STEP 4. Remove YOUR APPLE COMPUTER HAS BEEN LOCKED pop-up from Mozilla Firefox.

Video showing how to remove adware and browser hijackers from a Mac computer:

Adware removal:

Remove potentially unwanted applications from your '**Applications**' folder:

Click the **Finder icon.** In the Finder window, select "**Applications**". In the applications folder, look for "**MPlayerX**","**NicePlayer**", or other suspicious applications and drag them to the Trash. After removing the potentially unwanted application(s) that cause online ads, scan your Mac for any remaining unwanted components.

Combo Cleaner checks if your computer is infected with malware. To use full-featured product, you have to purchase a license for Combo Cleaner. Limited three days free trial available.

Remove your apple computer has been locked virus related files and folders:

Click the **Finder** icon, from the menu bar. Choose **Go,** and click **Go to Folder...**

Check for adware-generated files in the /Library/LaunchAgents folder:

In the *Go to Folder...* bar, type: **/Library/LaunchAgents**

In the "**LaunchAgents**" folder, look for any recently-added suspicious files and **move them to the Trash**. Examples of files generated by adware - "*installmac.AppRemoval.plist*", "*myppes.download.plist*", "*mykotlerino.ltvbit.plist*", "*kuklorest.update.plist*", etc. Adware commonly installs several files with the same string.

Mac Pro Locked Up

Check for adware generated files in the /Library/Application Support folder:

In the *Go to Folder...* bar, type: **/Library/Application Support**

In the "**Application Support**" folder, look for any recently-added suspicious folders. For example, "**MplayerX**" or "**NicePlayer**", and **move these folders to the Trash**.

Check for adware-generated files in the ~/Library/LaunchAgents folder:

In the Go to Folder bar, type: **~/Library/LaunchAgents**

In the "**LaunchAgents**" folder, look for any recently-added suspicious files and **move them to the Trash**. Examples of files generated by adware - "*installmac.AppRemoval.plist*", "*myppes.download.plist*", "*mykotlerino.ltvbit.plist*", "*kuklorest.update.plist*", etc. Adware commonly installs several files with the same string.

Check for adware-generated files in the /Library/LaunchDaemons folder:

In the *Go to Folder...* bar, type: **/Library/LaunchDaemons**

In the "**LaunchDaemons**" folder, look for recently-added suspicious files. For example "*com.aoudad.net-preferences.plist*", "*com.myppes.net-preferences.plist*", '*com.kuklorest.net-preferences.plist*", "*com.avickUpd.plist*", etc., and **move them to the Trash**.

Scan your Mac with Combo Cleaner:

If you have followed all the steps in the correct order you Mac should be clean of infections. To be sure your system is not infected run a scan with Combo Cleaner Antivirus. Download it HERE. After downloading the file double click *combocleaner.dmg* installer, in the opened window drag and drop Combo Cleaner icon on top of the Applications icon. Now open your launchpad and click on the Combo Cleaner icon. Wait until Combo Cleaner updates it's virus definition database and click **'Start Combo Scan'** button.

Combo Cleaner will scan your Mac for malware infections. If the antivirus scan displays 'no threats found' - this means that you can continue with the removal guide, otherwise it's recommended to remove any found infections before continuing.

After removing files and folders generated by the adware, continue to remove rogue extensions from your Internet browsers.

YOUR APPLE COMPUTER HAS BEEN LOCKED virus removal from Internet browsers:

Remove malicious extensions from Safari:

Remove your apple computer has been locked virus related Safari extensions:

Open Safari browser, from the menu bar, select '**Safari**' and click '**Preferences...**'.

In the preferences window, select '**Extensions**' and look for any recently-installed suspicious extensions. When located, click the '**Uninstall**' button next to it/them. Note that you can safely uninstall all extensions from your Safari browser - none are crucial for normal browser operation.

- If you continue to have problems with browser redirects and unwanted advertisements - Reset Safari.

Remove malicious plug-ins from Mozilla Firefox:

Remove your apple computer has been locked virus related Mozilla Firefox add-ons:

Open your Mozilla Firefox browser. At the top right corner of the screen, click the '**Open Menu**' (three horizontal lines) button. From the opened menu, choose '**Add-ons**'.

Choose the '**Extensions**' tab and look for any recently-installed suspicious add-ons. When located, click the '**Remove**' button next to it/them. Note that you can safely uninstall all extensions from your Mozilla Firefox browser - none are crucial for normal browser operation.

- If you continue to have problems with browser redirects and unwanted advertisements - Reset Mozilla Firefox.

Remove malicious extensions from Google Chrome:

Remove your apple computer has been locked virus related Google Chrome add-ons:

Open Google Chrome and click the '**Chrome menu**' (three horizontal lines) button located in the top-right corner of the browser window. From the drop-down menu, choose '**More Tools**' and select '**Extensions**'.

Delete Locked App Mac

In the '**Extensions**' window, look for any recently-installed suspicious add-ons. When located, click the '**Trash**' button next to it/them. Note that you can safely uninstall all extensions from your Google Chrome browser - none are crucial for normal browser operation.

Close Locked App Mac

- If you continue to have problems with browser redirects and unwanted advertisements - Reset Google Chrome.