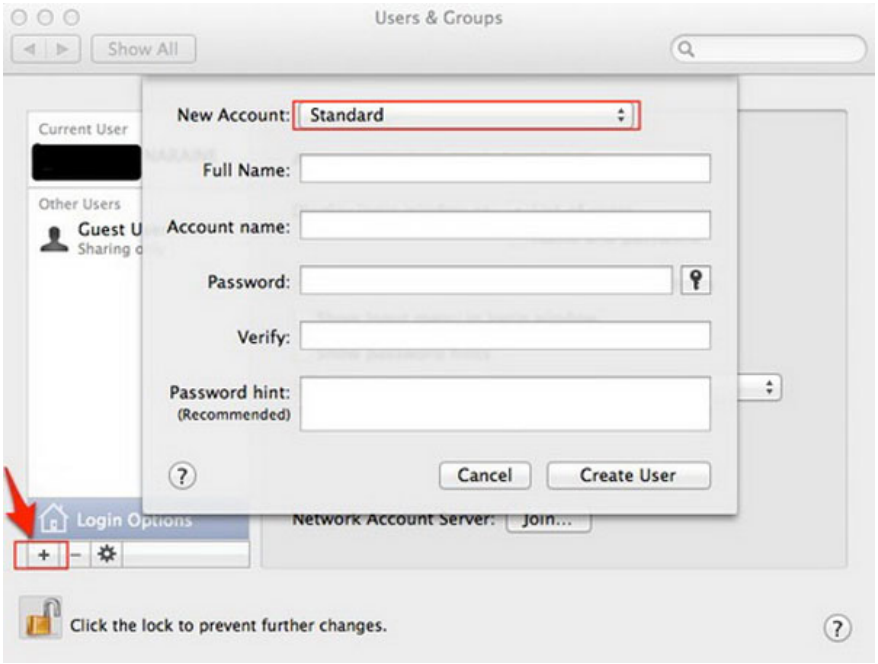
Tips to increase security for Mac OS X

Facing the risk of malware attacks for Mac users, Kaspersky Lab has provided valuable advice to enhance Mac protection.

Facing the risk of malware attacks for Mac users, Kaspersky Lab has provided valuable advice to enhance Mac protection.

Create a secondary account for daily activities

The default user account on Mac OS X is an administrator account or admin account, and creators of malware can take advantage of this account to harm computers. .



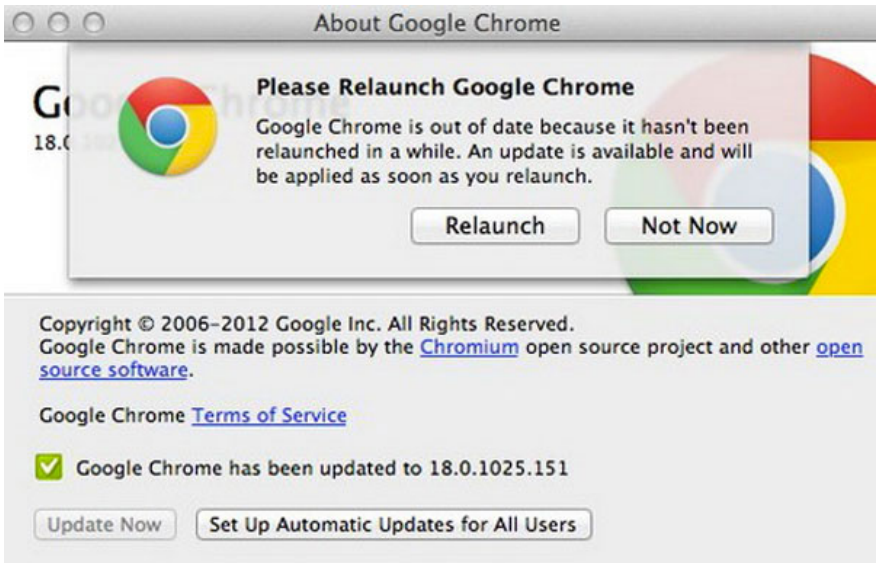
For daily activities, Kaspersky Lab recommends that users create a secondary account to log in and use for those activities. You should only log in as an admin when you need to perform management functions

To do this, the user switches to **System Preferences - Accounts.** Then create a sub account and use this account in everyday tasks like email checking and web surfing. This will help prevent malicious malware attacks that have been recorded in a completely new database or malware and help keep the drive safe from the attack of these types of malicious software.

Use a web browser that contains sandbox, has tracking function as well as fix security related issues

Google Chrome is considered the most suitable browser to use on Mac OS because it is updated more frequently than Apple's Safari browser. In addition, Google Chrome also has its own sandbox and sandbox Flash Player version.

Sandbox creates a barrier to protect the computer from the attack of malicious software. Google Chrome also has an automatic update mechanism that adjusts the machine's security holes.

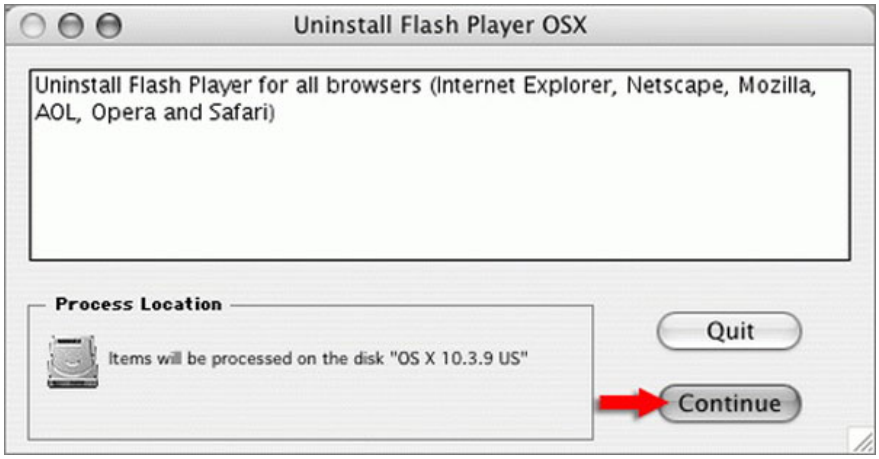


Google Chrome outperformed Apple Safari at home "Apple"

Remove standalone Flash Player installation

Adobe's Flash Player is a popular target that hackers specialize in exploiting bugs to hijack users' computers. An old version of Flash Player will definitely put users in dangerous situations when surfing the web.

To uninstall Flash, users can use Adobe's utility.



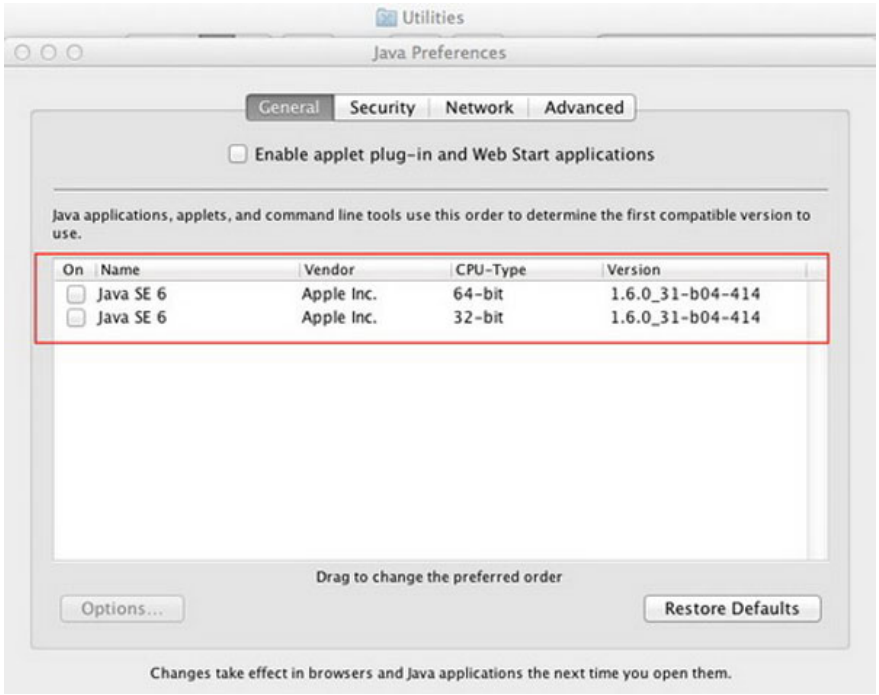
Remove Flash Player

Solve Java problems

Like Flash Player, Java is a favorite target for hackers to inject malware into a user's computer.

Because Apple Mac computers do not allow users to update Java directly, every few months. Therefore, the update time is prolonged, leading to a time to patch the vulnerabilities to avoid longer malware than computers running other operating systems.

The **Java Preferences** utility is located in **Applications / Utilities** and when you open this utility, users should not select other items in the **General.**



Kaspersky Lab recommends that users uninstall or lock Java on Mac

If you have to use Java for specific applications, one important thing to note is to disable Java in Safari and other web browsers. In the Safari browser, go to **Preferences-> Security-> Web Content** and uncheck '**Enable Java** '

Run "Software Update" and correct it when you get updates

Many recent attacks take advantage of old or up-to-date software to break into Mac OS X. Commonly used software includes Microsoft Office, Adobe Reader / Acrobat and Oracle Java and applications. other uses. Office for Mac operating systems 2011 protects computers better than Office for Mac operating systems 2008.

If you are still using the 2008 version, Kaspersky Lab recommends that users update the 2011 version as soon as possible. Whenever you see Apple's *'Software Update'* prompt, the user should use the fixes and restart the computer when needed.

Disable IPv6, AirPort and Bluetooth when not needed

Turn off unconnected connection services like IPv6, AirPort and Bluetooth. These three connection services are used by hackers as starting points for attacks. IPv6 is a relatively new communication protocol that Mac operating systems can use. However, this communication protocol is rarely used in practice. Therefore, the best advice to be able to secure that computer is to disable IPv6.

To disable IPv6 on the computer, select **Apple menu - System Preference** and then select **Network.** If **Network Preference** is locked, users click on the lock icon and enter the admin password to change. Select the network service that the user wants to use with IPv6 connectivity such as Ethernet, AirPort. Click **Advanced - TCP / IP** - the menu configures the pop-up windows IPv6 (usually set automatically) and select **Off.**

Enable full disk encryption (Mac OS X 10.7 + operating system) or FileVault

In Mac OS X Lion operating system, Apple has updated its encryption (FileVault) solution and full disk encryption is called *"FileVault 2"* . The advantage of this is to ensure the safety of the entire disk instead of securing each folder, which is very useful in case the laptop is stolen.

Install an effective security program

Today, Mac OS users need a security solution to secure their computers. There are quite a few options for Mac OS X users, including commercial and free.