CMSGu2013-03

National Computer Board

Mauritian Computer Emergency Response Team

Enhancing Cyber Security in Mauritius

Guideline on Securing Mac OS X

CERT-MU

National Computer Board
Mauritius

Version 1.1

August 2013

Issue No. 3

Table of Contents

DISCLAIMER: *This guideline is provided "as is" for informational purposes only. Information in this guideline, including references, is subject to change without notice. The products mentioned herein are the trademarks of their respective owners.*

1.0 Introduction

1.1 Purpose and Scope

This document provides steps that Macintosh (Mac) users can go through to consolidate the security features of their OS X system. However, this document should not be the only resource used to protect them from all security issues. Users need to consult their product vendors to determine the most secure implementation of their operating system.

1.2 Audience

The target audience includes all Mac users and system administrators working on Mac systems.

1.3 Document Structure

This document is organised into the following sections:

Section 1 gives an overview of the document's content, the targeted audience and the document's structure.

Section 2 provides a background on the Mac OS X Operating System.

Section 3 outlines the OS X Mountain Lion Security Features.

Section 4 provides a few tips for boosting the Security of a Mac system.

Section 5 concludes the document.

Section 6 comprises a list of references that have been used in this document.

2.0 Background

The Macintosh, more commonly known as Mac, is a line of personal computers developed by Apple Inc. It is used mainly by home users, students and creative professionals. Apple also develops the operating system for the Mac, which is OS X. OS X Mountain Lion (version 10.8) is the ninth major release of OS X (formerly Mac OS X), Apple Inc.'s desktop and server operating system for Macintosh computers. Following a soft transition started with Mac OS X Lion, Apple consistently refers to OS X Mountain Lion as "OS X" rather than "Mac OS X". The most basic system requirements of OS X Mountain Lion are 2 GB of RAM, 8 GB of available storage, and OS X 10.6.8 or later.

The Mac, like other personal computers, can run alternative operating systems such as Linux, OpenBSD, and, in the case of Intel-based Macs, Microsoft Windows. However, Apple does not license OS X for use on non-Apple computers.

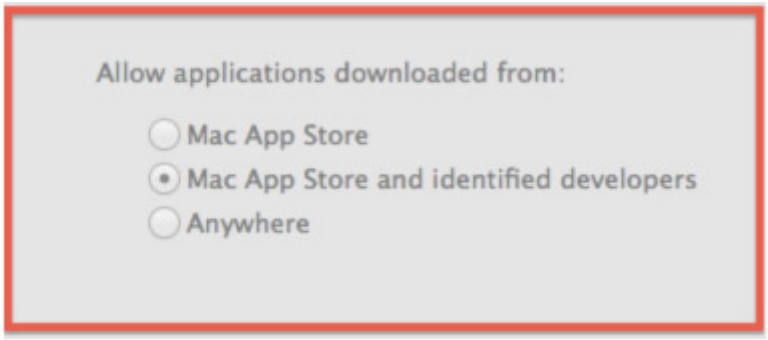
At first, the Macintosh 128K suffered from a lack of available software compared to IBM's PC, resulting in disappointing sales in 1984 and 1985. Distinctively, according to a recent Gartner report, Apple devices (Mac & iOS combined) are expected to outsell all Windows devices for the first time in 2013.

3.0 OS X Mountain Lion Security Features

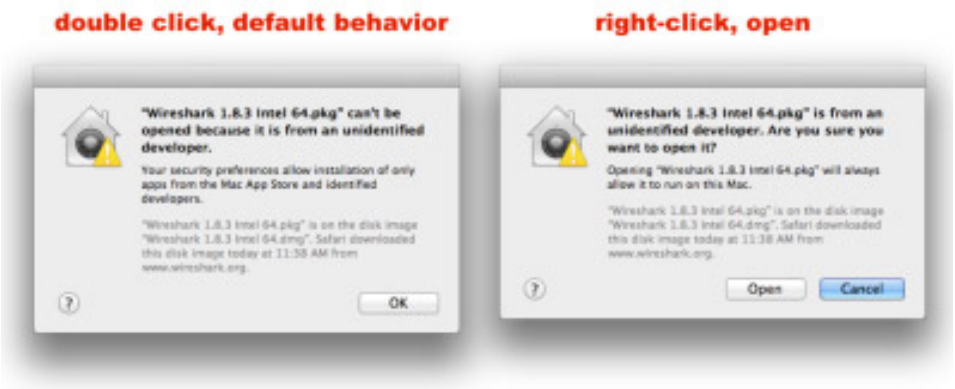
The following security tips take advantage of the latest Mountain Lion security features:

3.1 Gatekeeper

Gatekeeper's control resides under Preferences/Security & Privacy and its main function is to allow the user to control which apps can be run without further escalation and or attention. For example it is by default to 'Mac App Store and identified developers' so if you download an application that does not meet this criteria you will not be able to run the application immediately or more so accidentally.



You can either change the preference to "Anywhere" (not recommended) or simply right click (or control click) on the App instead of the normal single double click to open it.

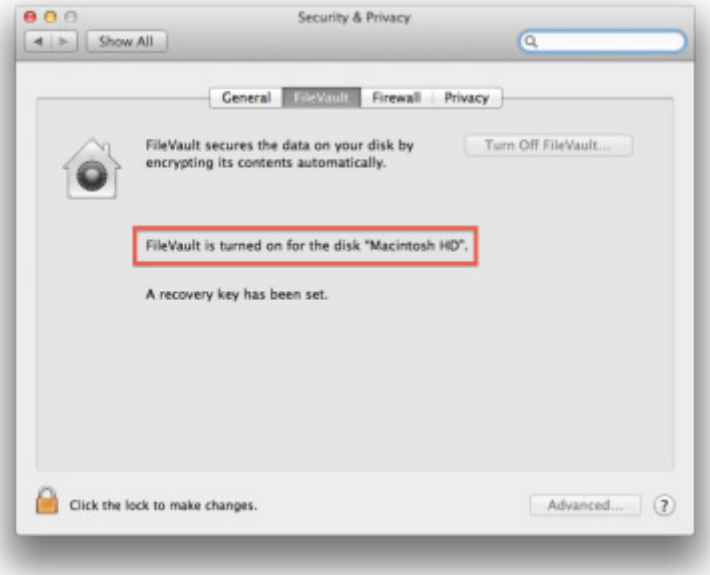


3.2 Software updates

Updates often get overlooked as a security measure; however fundamentally you want to keep your Mac updated with the latest and greatest updates. Most often users don't update their Macs to the latest because the update has phased out their application from working, or the user feels they are too busy to update their Macs. Don't be that user. Instead inquire with the software developer's support system to find out what they are doing about their incompatible product - many often become aware of this issue through their internal testing and generally try to push out a patch or updated version quickly. If they lag see if you can find an alternate product until they update. It's always good to have another good product on standby.

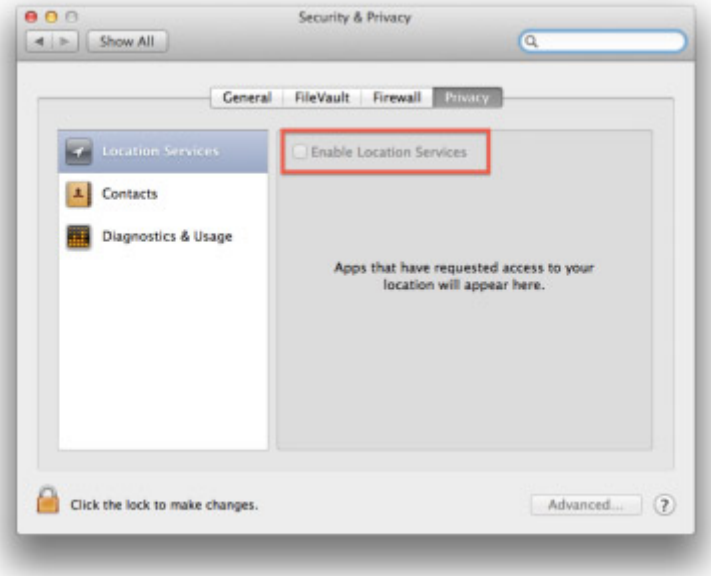
3.3 FileVault 2

Laptop and even Desktop encryption should be automatic nowadays. Losing a few thousand dollars of hardware is much better than losing all your data to someone later to find it pasted all over the Internet or worse sold on the blackmarket. Whole disk encryption should be used at any cost to protect against this type of attack.



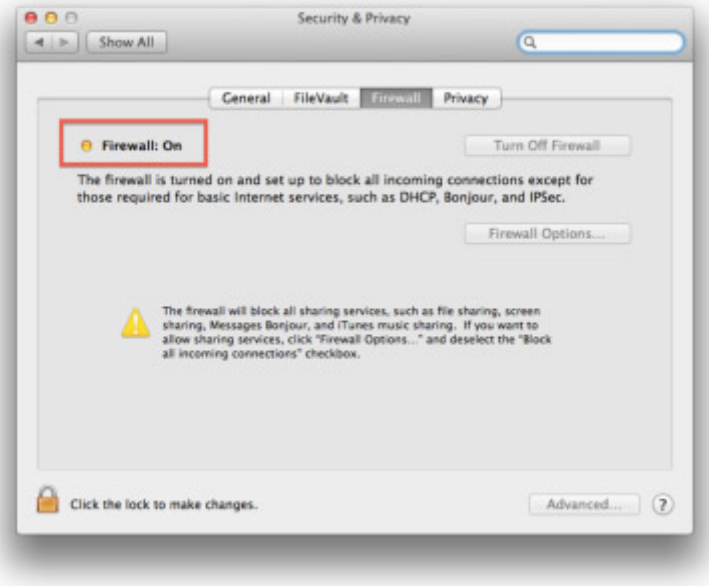
3.4 Privacy Controls

Privacy is important and should not be taken for granted. Make sure you keep track of who is keeping track of you by tuning your privacy controls accordingly.



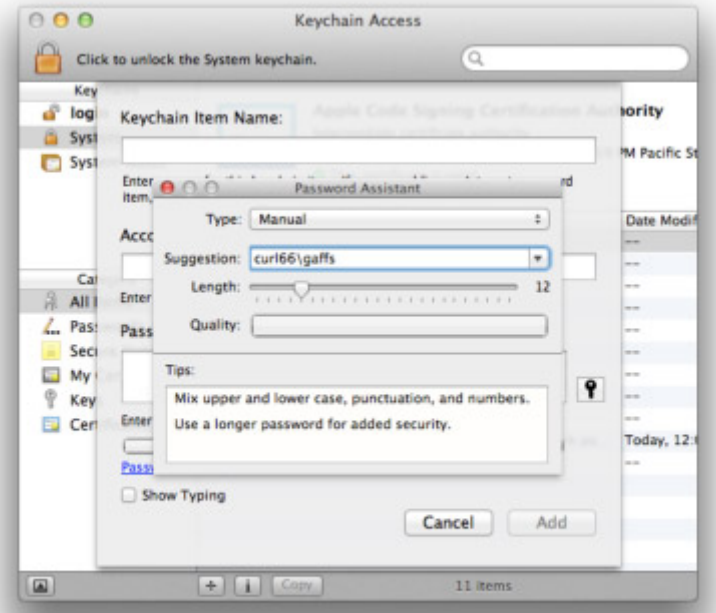
3.5 Firewall

The firewall interface under Preferences/Security & Privacy is very basic; there are a few third party interfaces available however keeping things simple is a good practice. Be sure to use the firewall to tune it to your needs whether it is at home, work or travel.



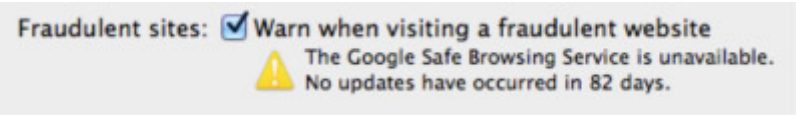
3.6 Password Assistant

Face it, for most creating a good password is hard. It involves a lot of thinking not only to come up with one that you don't already use, but then remembering it without having to write it down is a task within itself. This is where Keychain Access is your friend, use it. Inside Keychain Access is a handy tool named Password Assistant you can use it to quickly come up with a password and you can save it in your keychain to use on various logins.

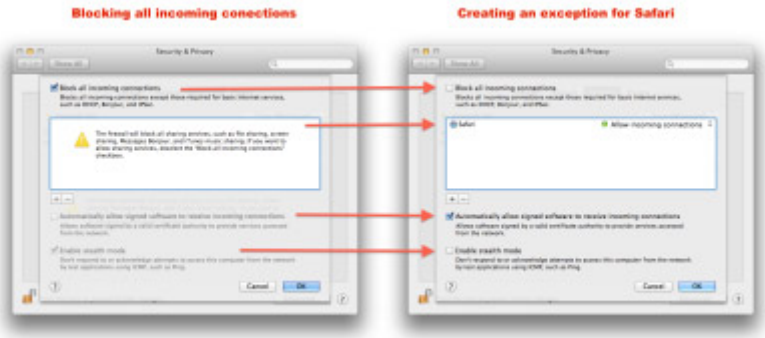


3.7 Anti-Phishing

For those that use Safari (6.0.2) over Chrome or Firefox you may have to make a firewall adjustment otherwise Safari may not be able to communicate correctly to receive updates from the The **Google Safe Browsing Service,** therefore leaving your browser out of date and more vulnerable.



Below are the recommended firewall modifications for this:

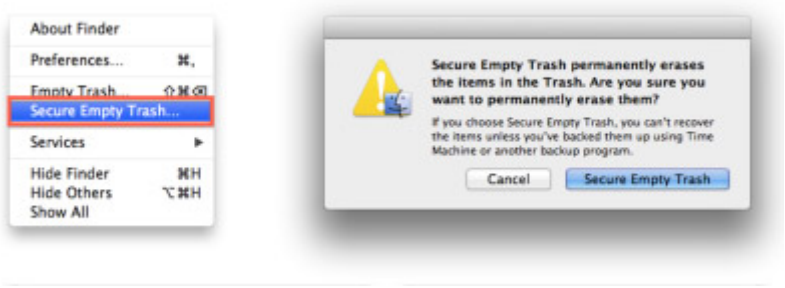


3.8 iCloud Mac Locator And Remote Wipe

For those that use iCloud your Mac can be enabled similar functionality as your iDevices for communicating with your Mac if it gets lost or stolen once it is reconnected to a network. The use of FileVault2 to encrypt your Mac gives you more assurance and in terms of privacy and confidentiality.

3.9 Secure Empty Trash

Another feature the Mac users may forget to use often especially on USB keys is the Secure Empty Trash Feature. By default files are simply marked for deletion and not really deleted making file recovery simple for an attacker. Using Secure Empty Trash things get much more difficult to recover.



3.10 Control Access

Make sure you are the only person accessing your account by requiring a password immediately after sleep or screen saver begins. Enable a hot corner to activate the screensaver and get used to hitting that hot corner before leaving your Mac. Get used to doing this at home and it will come naturally everywhere else.

3.11 Parental Controls

As a parent, you want your kids to have a safe and happy experience on the computer. OS X keeps an eye out even when you are not able to. With a simple setup in Parental Controls preferences, you can manage, monitor, and control the time your kids spend on the Mac, the sites they visit, and the people they chat with.

3.12 Sandboxing

The App Sandbox in OS X helps ensure that apps do only what they are intended to do. App sandboxing isolates apps from the critical system components of your Mac, your data, and your other apps. Even if an app is compromised by malicious software, sandboxing automatically blocks it to keep your computer and your information safe. OS X Mountain Lion delivers even better sandboxing protection in Safari. And it adds sandboxing to new apps like Notes, Reminders, and Game Center, as well as existing apps such as Mail and FaceTime.

3.13 Runtime Protections

The technically sophisticated runtime protections in OS X Mountain Lion work at the very core of your Mac to help keep your system safe. Built right into the processor, the XD (execute disable) feature creates a strong wall between memory used for data and memory used for executable instructions. This protects against malware that attempts to trick the Mac into treating data the same way it treats a program in order to compromise your system. Address Space Layout Randomization (ASLR) changes the memory locations where different parts of an app are stored. This makes it difficult for an attacker to do harm by finding and reordering parts of an app to make it do something it was not intended to do. Mountain Lion brings ASLR to the memory used by the kernel at the heart of OS X, so the same defenses now work at every level in your Mac.

3.14 Security Alerts

Innocent-looking files downloaded over the Internet may contain dangerous malware in disguise. That’s why files you download using Safari, Mail, and Messages are screened to determine if they contain applications. If they do, OS X alerts you, then warns you the first time you open one. You decide whether to open the application or cancel the attempt. And if a file contains software identified as malicious, OS X offers to move it to the Trash.

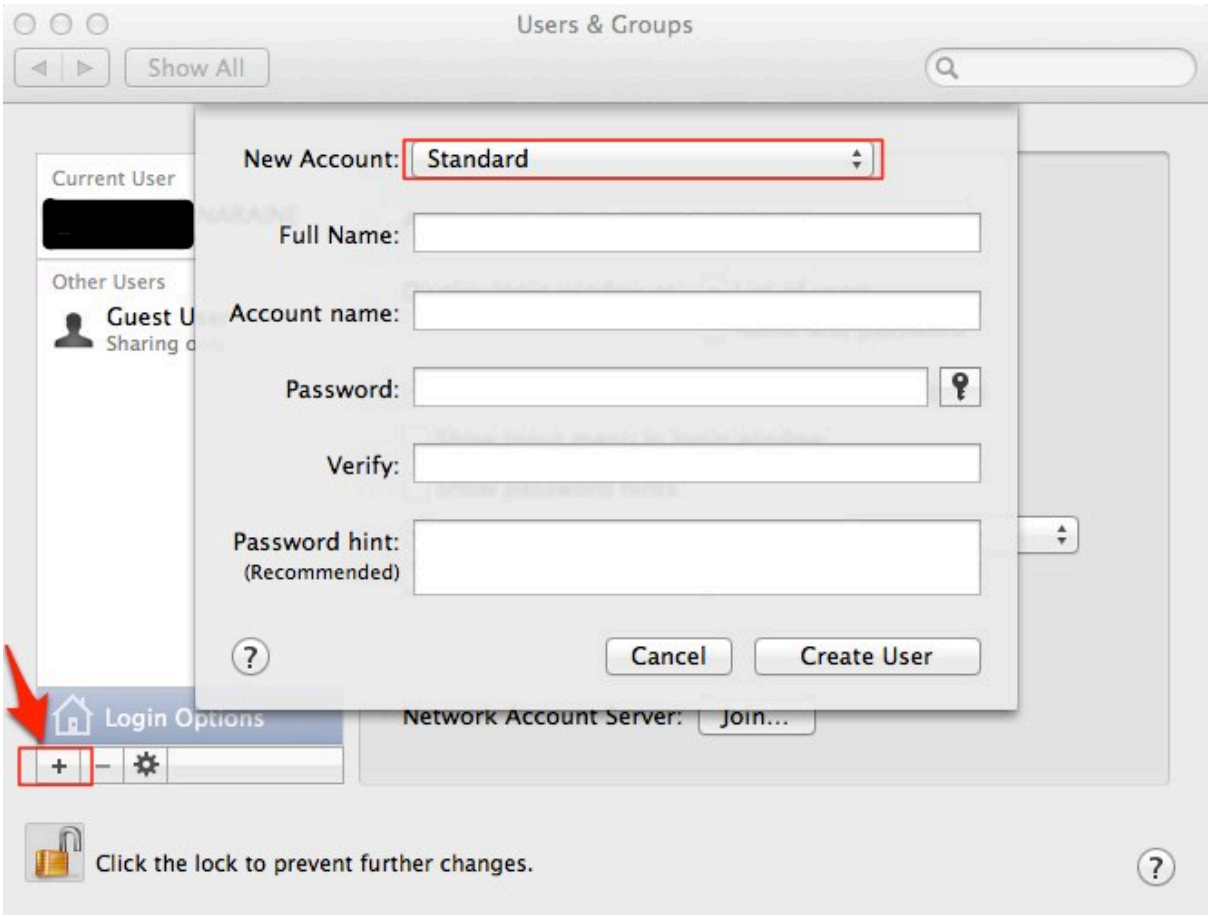
4.0 Tips For Boosting The Security Of Your Mac

There are presently more than 100 million Mac OS X users around the world. The number has grown swiftly during the past years and this growth is still expected to continue. Previously, Mac OS X malware was a somehow limited category and included Trojans such as the Mac OS X version of DNSChanger and fake anti-virus attacks for Mac OS X which boomed in 2011. In September 2011, the first versions of the Mac OS X Trojan Flashback appeared, however, they did not really become widespread until March 2012. According to data collected by Kaspersky Lab, almost 700,000 infected users have been counted at the beginning of April 2012 and the number could be higher. Although Mac OS X can be a very secure operating system, there are certain steps which users can take to avoid becoming a victim to this growing number of attacks.

4.1 Create A Non-Admin Account For Everyday Activities

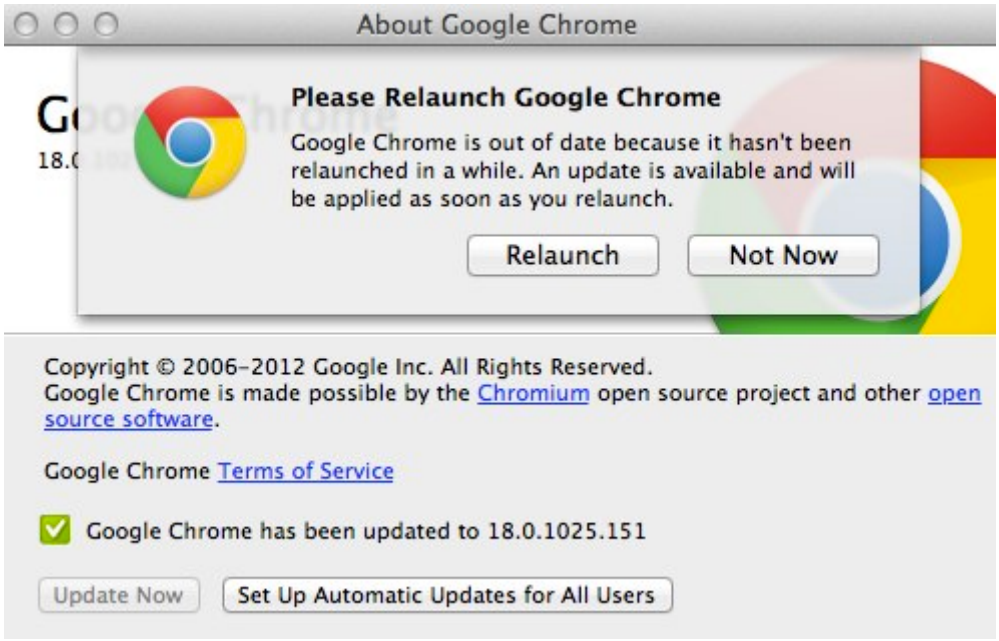
Your default account on Mac OS X is an administrator user, and malware writers can take advantage of that to infect your computer.

For everyday activities, it is recommended to create a non-admin user and to only log in as administrator when you need to perform administrative tasks. To do that, go to the "Accounts" pane of "System Preferences", then create a non-administrator user. Use the new account for everyday tasks like e-mail and web browsing. This helps to limit the damage from zero-day threats and drive-by malware attacks.



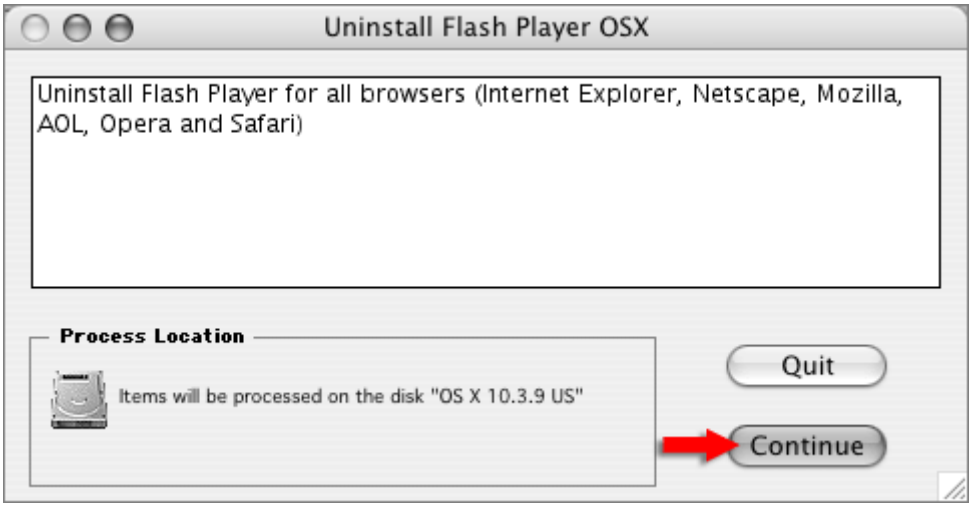
4.2 Use A Web Browser That Contains A Sandbox And Has A Solid Track Record Of Fixing Security Issues In A Prompt Manner

Google Chrome is recommended for many reasons; one of them being that it is updated more often than Apple's built-in Safari browser. In addition to its own sandbox, Chrome ships with a sandboxed version of Flash Player that puts up a significant barrier for malicious exploits. Google Chrome also has a silent, automatic update mechanism for patching security vulnerabilities. The new browser should also be set as your default web browser to benefit from the security options.



4.3 Uninstall The Standalone Flash Player

Over the years, Adobe's Flash Player has been common target for hackers looking to take control complete over your computer. An old version of Flash Player will most certainly put you at risk when browsing the internet. To uninstall Flash, you can use the two utilities provided by Adobe, for versions 10.4-10.5 and 10.6 and later.

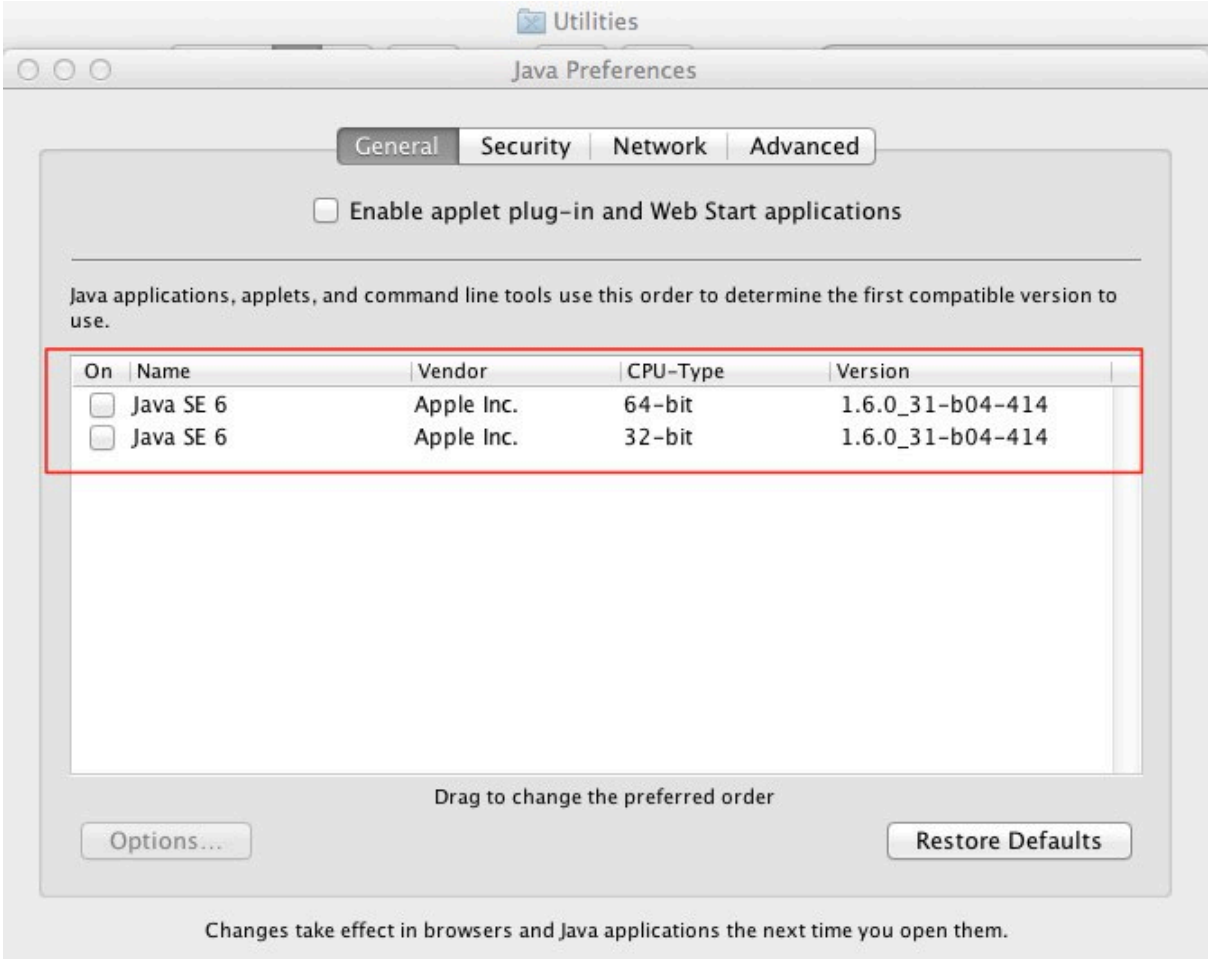


4.4 Solve The Java Problem

Like Flash Player, Java is a preferred target for exploit writers looking to install malware on your machine.

It is recommended that you completely uninstall it from your machine. Unfortunately, Apple does not allow Oracle to update Java for Mac directly. They do it themselves, usually several months later. This means the window of exposure for Mac users is much longer than PC users.

The Java Preferences utility is in /Applications/Utilities; uncheck the boxes next to the versions listed in the General tab.



If you must use Java for some specific applications, it is very important that you at least disable Java in Safari and other Web browsers. In Safari, go to Preferences -> Security -> Web Content and uncheck “Enable Java”.

4.5 Run “Software Update” And Patch The Machine Promptly When Updates Are Available

Many of the recent attacks against Mac OS X take advantage of outdated software. Commonly exploited suites include Microsoft Office, Adobe Reader/Acrobat, and Oracle’s Java, but there are other applications that can be abused as well. Office for Mac 2011 is much

better from a security point of view than Office for Mac 2008. Whenever you see the Apple's "Software Update" prompt, be sure to apply the fixes and reboot the machine when necessary.

4.6 Use A Password Manager To Help Cope With Phishing Attacks

Mac comes with a built-in password manager, the "Keychain".

Whenever possible, try to generate unique, strong passphrases for your resources and keep them in the keychain instead of remembering easier passwords. Whenever cyber-criminals manage to compromise one of your accounts, they will immediately try the same password everywhere, e.g. on GMail, Facebook, eBay and PayPal. Hence, having a unique strong password on each resource improves your online security.

Another, though more complicated advice is to have a separate keychain, with a 3-5 minutes password cache timeout, for important passwords only. In this way, if your "Keychain" gets compromised, you will not lose all the passwords.

4.7 Disable IPv6, Airport And Bluetooth When Not Needed

Turn off connectivity services when not in use or when not required. These include IPv6, AirPort and Bluetooth, three services that can be used as entry points for hacker attacks. IPv6 is a relatively new communication protocol which your Mac can use. This is rarely used in practice, in parallel to IPv4. Hence, it is safe and a good advice to disable IPv6 proactively.

To disable IPv6 on your computer, choose Apple menu > System Preferences, and then click Network.

If the Network Preference is locked, click on the lock icon and enter your Admin password to make further changes. Choose the network service you want to use with IPv6, such as Ethernet or AirPort.

Click Advanced, and then click TCP/IP. Click on the Configure IPv6 pop-up menu (typically set to Automatically) and select Off.

4.8. Enable Full Disk Encryption (OS X 10.7+) or FileVault

In MacOS X Lion, Apple updated their encryption solution (FileVault) and added full disk encryption. It is now known as "FileVault 2". This has the advantage of security of the entire disk instead of just your home folder and can be very useful if your laptop gets stolen.

4.9 Upgrade Adobe Reader To Version "10" Or Later

Adobe Reader has been one of the preferred targets of cybercriminals on the Windows platform and it still ranks high among the most exploited software in the world. Version 10 includes numerous security enhancements which make it a lot safer than any previous versions. Please make sure you get the latest version from the download page at Adobe - unfortunately, many of the older versions are still available for download and it can easily become confusing.

4.10 Install A Good Security Solution

"Mac's do not get viruses" has been a common theme ever since the famous 2006 commercial with the sick PC and the healthy Mac. Seven years have passed and the situation has changed dramatically. Nowadays, a security solution is absolutely mandatory for any Mac user. You can download and install a trial of Kaspersky Anti-Virus for Mac.

For Mac OS X power users, a utility like 'Little Snitch' can be used to determine when a program attempts to establish an outgoing Internet connection and give you the option to allow or deny this connection.

5.0 Conclusion

More and more users are using the Mac OS X around the world. The number has drastically increased over the years and is still expected to grow. Previously it was perceived that Mac computers were free from attacks and viruses, but nowadays this is merely a myth. There are ways to protect against these attacks, just like there are countermeasures for other operating systems. All Mac users are encouraged to secure their computers, especially before connecting them to the Internet, which is pervasive and full of malware.

6.0 References

- Wikepedia, http://en.wikipedia.org
- SANS, www.sans.org
- Apple, http://www.apple.com
- SecureMac, http://www.securemac.com