University Information Security Office
University of South Carolina

Securing Your Mac at Home

How to get the most security from your OS X machine

Kyle S. Brown

Kyle is an alumnus of the University of South Carolina and is currently the university's information security awareness specialist. He is part of the University Information Security Office where he works to help people understand the dangers of modern computing.

Basic Steps

At a minimum, these "Basic" recommendations should be implemented on your Mac. These steps should be completed before moving on to the "Intermediate" or "Advanced" sections.

Make sure your version of OS X is supported.

Find your OS X version:
http://support.apple.com/kb/HT1633

Unsupported versions of OS X do not receive important security fixes or patches that could leave your Mac vulnerable to attack. Although Apple normally supports at least two previous versions of the Mac operating system, OSX 10.9 Mavericks includes security fixes that are not yet available for previous versions.

http://apple.com/osx/how-to-upgrade

Keep Mac OS X up to date.

Update OS X:
http://support.apple.com/kb/HT1338

Remember to install the updates soon after they become available if you are interested in better protecting your computer from Internet criminals.

Install Anti-Virus software.

Sophos Anti-Virus for Mac Home Edition:
http://www.sophos.com

Anti-Virus software provides basic protection against malicious programs. In many cases, free anti-virus products provide just as much protection against malicious programs

Use a secure Internet browser.

Google Chrome:
http://www.google.com/chrome

Google is committed to continually improving the security of Chrome. It is often the first company to implement new security features within its browser.

Intermediate Steps

Once the basic recommendations have been implemented, the following steps should be completed for increased security:

Protect your Mac from known malicious websites.

OpenDNS* (free for personal use):
http://www.opendns.com

OpenDNS provides a service that will monitor the location of sites that are being visited, and protect you when needed. The service maintains a list of bad locations that it will block, if needed. The service can also be configured to provide parental controls for blocking inappropriate content.

***OpenDNS should not be set up on university-owned systems. It is known to cause problems when attempting to connect to resources like printers or shared drives.**

(Continued on back)

UNIVERSITY OF SOUTH CAROLINA

Keep your applications up to date.

Mac Informer:
http://mac.informer.com

Outdated applications have weaknesses that may allow an attacker to access or take control of your Mac. Keep the security of your Mac strong by updating your applications. Mac Informer will notify you when updates for your applications become available, and it will help you install them.

Keep a regular backup schedule.

Time Machine:
http://support.apple.com/kb/HT1427
Box (10GB Free):
http://www.box.com
iCloud (5GB Free):
http://www.apple.com/icloud/

Your photos and documents are hard to replace in the event of a catastrophic crash. By backing up your files, you can keep an already difficult experience from becoming worse. Do not wait until it's too late.

With the exception of Mac's built-in Time Machine, the rest of the tools above will store your data in the cloud. Backing up to the cloud does not require any additional hardware such as a flash drive, external hard drive, or CD/DVD-R.

When using a cloud storage provider, the following are recommended:

- Make sure you understand the provider's privacy policy.
- Use multi-factor authentication.
- Occasionally (every six months) backup to a physical media.

Encrypt your Mac.

Filevault 2:

http://support.apple.com/kb/HT4790

Whole disk encryption protects your data in the event your Mac is lost or stolen. Make sure to backup your data before encrypting your Mac.

Turn on the built-in firewall.

Prevent unwanted connections with a firewall:
http://support.apple.com/kb/PH11309

Attackers can use listening applications to harm your Mac. Use the built-in firewall to limit the number of accessible applications.

Subscribe to a Malware Domain Feed.

Ad Block Plus for Google Chrome:
https://adblockplus.org/en/chrome

After installing AD Block Plus, click "subscribe" in the Malware Domain section of the following link.
https://adblockplus.org/en/subscriptions

By using AD Block Plus and subscribing to the Malware Domain list, your browser will refuse access to known bad websites.

Disable risky browser plugins.

Disable Google Chrome plugins:
https://support.google.com/chrome/answer/142064?hl=en
Disable Mozilla Firefox plugins:
https://support.mozilla.org/en-US/kb/disable-or-remove-add-ons#_how-to-disable-plugins

Internet browser plugins (such as Adobe Flash and Java) are vulnerable to attacks and may allow an attacker to harm your Mac. If you are not regularly using plugins, try disabling them.

Use a password management tool.

Keepass Classic Edition (free for personal use).
http://keepass.info/
LastPass (free for personal use).
http://www.lastpass.com
iCloud (free for personal use).
http://www.apple.com/icloud/

Choosing strong and unique passwords is critical to keeping your data safe. Each online account should have a different password. Easier said than done, right? Well, password management tools will help you keep up with all your passwords. *(continued)*

Tools such as LastPass or iCloud can even enter your username and password upon accessing a familiar website. Do not let an attacker gain access to all of your important accounts by stealing one password. Remember, we do not want to make it easy for the attackers.

Advanced Steps

Caution should be taken with these "advanced" options, as these changes will dramatically change your web (and overall computing) experience.

Create a "secured" browser.

Since many attacks occur while browsing the Internet, users should secure their browser as much as possible. Unfortunately, after locking down the browser, some websites may not work the same. By using the locked down browser to access non-trusted sites, you can limit the chance of your Mac being harmed while still enjoying your web experience.

Disable Internet browser plugins *(on your secure browser).*

All browser plugins should be disabled except any that are used for security. If a website requires an additional plugin, use a different browser. Only access sites that you can trust with plugins.

Use a Javascript whitelisting tool.

Noscript (Firefox) and Notscript (Chrome) are only for the more adventurous and technically savvy users. Most websites use Javascripts to give us a better experience. Unfortunately, attackers choose to distribute malware using Javascripts. Javascript whitelisting tools allow us to quickly choose which websites Javascript can run on.

Beware, knowing which websites need to be allowed can be difficult at times.

Create a separate "admin" account.

When you are running as an administrator, attackers can install their malware easier. When possible, setup a separate account as an administrator. Most normal computing can be done with a standard account.

Only use an administrator account on your machine when it is absolutely necessary.

Notes