

Mac Security Basics for Snow Leopard & Lion

by Mike Sullivan

Cove Apple Club / February 22, 2012

Mac OS X is extremely secure by default, and every Mac comes out-of-the-box with over a dozen advanced security measures already “turned on” to keep you safe online and offline. Follow these simple tips to add even more to the ring of security already built-in to your Mac and enjoy a hassle-free, worry-free experience using your Mac.

1) **Remove Adobe Flash Player from your Mac.** Adobe’s Flash player is notoriously vulnerable to malicious Internet attacks, with Adobe issuing “Critical Alerts” several times a year, affecting hundreds of millions of PCs. All new Macs shipped after October, 2010 already omitted Flash Player from the factory install of Mac OS X. There is no reason to keep Flash Player on your Mac. See the “Going Flash-Free” presentation from the March 23, 2011 Cove Apple Club meeting in our Club Archives section at <http://goo.gl/bDThZ>

2) **Set Software Update to run daily.** Software Update checks in with Apple’s servers to see if there’s any updated software for your Mac. To set it to check for updates every day, choose System Preferences from the Apple menu, then choose Software Update. Set the Software Update preferences to Check for Updates Weekly.

3) **Use OpenDNS as the DNS service for your home LAN.** This incredibly useful free service requires no software or hardware, and guards your entire network against phishing attacks, malware sites, suspicious re-directs and more. Setup takes just a minute, and once configured, there’s nothing else to fiddle with! Visit opendns.com for details, or ask one of our Cove Apple Club nerds to help you get your home network set up with OpenDNS.

4) **Check that Safari is set not to open downloaded files automatically.** In Safari, choose Preferences, then choose the General tab. Confirm that “Open ‘safe’ files after downloading” is unchecked.

5) **Use a secure Wi-Fi network connection whenever possible.** Your home Wi-Fi network should use “WPA2” security protocol, which keeps your wireless connection to the Internet secure from snoopers. See the documentation that came with your Wi-Fi router for more information, or ask one of the Cove Apple Club nerds to help you secure your home Wi-Fi setup.

6) **Strongly consider a password automation and management package, like IPassword.** Several Cove Apple Club members use and **strongly recommend** IPassword as the best way to keep track of all your online passwords, logins, identities, and other sensitive information, and help provide comprehensive protection against phishing, “shoulder-surfing,” keystroke loggers and even man-in-the-middle snooping attacks. Ask around, visit 1password.com or see Mike for a personal consultation and help getting set up with IPassword. You won’t be sorry!

7) **Use a boot-up password on your system, especially your Mac laptop.** On your Mac, choose System Preferences, then choose Users & Groups. Click the Lock icon at the bottom-left, then click the Login Options icon (enter your administrator’s password when prompted). Set “Automatic Login” to Off, and choose “Display Login window as:” List of users, and select “Show the Sleep, Restart and Shut Down buttons.” When you’ve made your selections, click the lock icon again.

8) For more information on Mac security, best practices and how Mac OS X keeps you safe, see <http://www.apple.com/macosx/what-is/security.html>