Inoculate Your Mac

by Mike Sullivan | Cove Apple Club | April 11, 2012

Mac OS X is a very safe and secure operating system by design and by default, and Mac users are protected against millions of worms, Trojans and viruses that plague the Windows platform. These additional measures are a quick and easy way to further shield your Mac from exposure to vulnerabilities in non-Apple software and from malicious Web sites.

Use OpenDNS

OpenDNS is a free, automatic service that protects every device on your home LAN from malicious Web sites, phishing sites, domain sidejacking, and other Web-borne exploits. Best of all, it requires absolutely no software or hardware, no maintenance on your part, and it can even speed up your Internet connection!

- Read about OpenDNS: **`http://goo.gl/13aoh`**
- Install OpenDNS on your home router: **`http://goo.gl/1jAN4`**

Keep your Mac software up-to-date

- ➔ System Preferences ➔ Software Update: Check for updates: **CHECKED, Daily;** Download updates automatically: **CHECKED**

Remove Adobe Flash Player from your Mac

We've harped on this for years, and it makes more sense than ever to get this nasty, CPU-hogging, insecure and outdated browser plug-in off of your Mac. All new Macs since October 2010 have shipped without Flash Player installed, and no iPhone, iPad or iPod touch has ever contained Flash. There is simply no reason to have it around, especially now that *Adobe is ending development of Flash* for mobile devices!

- Going Flash-Free on your Macs step-by-step (March, 2011 handout): **`http://goo.gl/oee6h`**

Lock down your Safari configuration

You can make these quick and easy tweaks to settings in your Safari configuration to eliminate several potential vulnerabilities in external software and malicious Web sites.

- **Disable Java**: Safari ➔ Preferences ➔ Security:
  - Warn when visiting a fraudulent Web site: **CHECKED**
  - Enable Java: **UNCHECKED**
- **Turn off AutoFill:** Safari ➔ Preferences ➔ AutoFill: **UNCHECK all options**
- **Block 3rd-Party cookies:** Safari ➔ Preferences ➔ Privacy: Block cookies from third parties and advertisers: **CHECKED**
- **Prevent launching of downloaded files:** Safari ➔ Preferences ➔ General: Open "safe" files after downloading: **UNCHECKED**
- **Disable Java on your Mac:** Finder ➔ Go ➔ Utilities: *Java Preferences*: Enable applet plug-in and Web Start applications: **UNCHECKED**

Use 1Password or another password manager:

We've been over this and over this: in 2012, there is simply no excuse for not using a modern, secure, fail-safe password manager. Example: if you are using 1Password, even if your system has been infected by the Flashback Trojan, they have nothing to steal from you, since none of your passwords, logins or other info is stored in Safari!

To get with the 1Password program, visit 1password.com, have Mike over for a lecture and a personalized plan to get your act together, or see these links:

- Why your passwords suck (and what to do about it): **`http://goo.gl/6M7ul`**
- Throwing the deadbolt on Internet security (1Password follow-up): **`http://goo.gl/xByaR`**
- Mac App Store link: **`http://goo.gl/3pelN`**