NOV 15, 2017 6:11 AM PT | **Jonny Evans**

First, some common sense security tips

Malware is everywhere, and Macs are not immune. You can ignore the potential threat if you choose, but if you are an enterprise user holding confidential data, an educator in possession of private data, or even a Bitcoin collector who maybe clicked a few too many links on one of those dodgy faucet websites, you should know how to secure your Mac.

Before we get into some of the security technology inside your Mac (including a wide range of security improvements in High Sierra) it is important to point out that the biggest threat your computer faces is the person using it. Cyber attackers are highly sophisticated and can piece together lots of information about you or companies associated with you by simply getting a little more data a little at a time. Make it hard for those people by following simple tips, including:

- Avoid clicking links from people you don't know.
- Never download/install software unless you know where it is from.
- Use *strong passwords*, and use different passwords for each site — Apple's Keychain Manager makes this process ever so easy.
- Use two-step verification everywhere.
- Consider using a VPN service, such as NordVPN (which I use).
- Use Private Browsing.
- Use a disposable email address to sign up for services, websites and the like — that way you can reduce the spam you receive in your primary emails.
- Never access a confidential service (such as your enterprise intranet or online bank) over public Wi-Fi.
- Install macOS software updates as they appear.

What about virus checkers?

The jury remains out on virus checkers.

Many Mac users believe it slows Mac performance — but so too does unwanted adware, Potentially Unwanted Programs (PUPs) and malware if it lurks on your Mac.

I choose to scan my system regularly as I send and receive digital assets from lots of sources, and also believe I have a responsibility to ensure I don't inadvertently transmit Windows malware to others from my Mac.

Numerous applications are available. AVG for Mac is Macworld UK's most highly recommended (free version available) antivirus package; Malwarebytes for Mac is also popular. There are several paid solutions available.

Let's move on to look at some of the other security protection solutions in place on your Mac. (You'll find that you need to unlock System Preferences by tapping the padlock icon and entering your password to make changes in many of the following cases.)

Enable your Mac's built-in firewall

Your Mac's built-in firewall should be enabled by default. Check that it is in *System Preferences>Security & Privacy* where you choose the Firewall Tab. Choose Turn on Firewall, and it will be enabled. Tap Firewall Options, and you can choose which apps can receive inbound connections and even enable a Stealth Mode, which will make your Mac less visible on public networks by preventing it responding to probing network requests (such as Ping requests) that may reveal its existence.

Can we have a (pass) word?

I'm certain you already use a strong password to secure your Mac, but you can choose how strongly password protection is applied in System Preferences>Security & Privacy. Here you can set how long your Mac is left unattended before a password is required. (Immediately after sleep is the best protection if working in a shared environment.)

System privacy

The *Privacy* pane in *Security & Privacy Preferences* controls numerous items. You can choose which apps (if any) you allow to use Location Services, or you can disable them entirely. You can also control which apps are given access to other data on your Mac: Contacts, Calendars, Reminders, Photos, Twitter, Facebook, Accessibility and Analytics.

Browser privacy

You will also need to vet the security settings of your browser. The Safari browser in High Sierra has a selection of privacy-focused improvements. Open *Safari>Preferences>Privacy* to see the following:

- **Website tracking:** Prevent cross-site tracking and ask sites you visit not to track you.
- **Cookies and website data:** You can block all cookies and review what data sites have about you that is held on your system.
- **Apple Pay:** You can allow/prevent sites to check if Apple Pay is available on your Mac with this tool.

You should also open the *Security* pane in *Safari Preferences*. Here you can ensure you receive warnings when you visit a fraudulent site, disable JavasScript and block popup windows.

Manage Sharing tools

System Preferences>Sharing lets you choose to share services — files, printers, Bluetooth and more — from your Mac. I tend to keep all of these off by default but, you may find that some apps ask you to switch a service on (for perfectly legitimate reasons). When you finish using an app that is using Sharing tools, you should manually look inside these settings to make sure they are disabled again afterwards.

App access

Most enterprise security guidelines encourage you to strictly police the apps installed on your Mac if your computer carries confidential information, such as company files, enterprise secrets, patient data or student reports. Apple agrees, and that is why the company has made it much harder to install apps from sources other than the App Store.

You control App download behavior in the *General Pane* of *Security & Privacy Preferences*.

Here you can allow apps downloaded only from the App Store or only from the App Store and identified developers. In most enterprise set-ups, you'll choose the second, if only so you can install trusted but limited distribution apps made by the company.

Use FileVault

Apple's FileVault encryption is a powerful tool with which to prevent your data being abused even if your system is compromised.

FileVault is available in *Security & Privacy System Preferences.* When enabled, it encrypts the contents of your Mac automatically, and you will need to use your login password or a recovery key to access your data. The downside? If you can't remember either of those passcodes, you will *lose access to your data.*

Enable Find My Mac

Apple's Find My iPhone feature will also help you find your Mac if it is lost. You can enable this in *System Preferences>iCloud* where you should ensure Find My Mac is checked to on (and that you are logged in using your Apple ID).

If your Mac is lost, you may then be able to find it by visiting www.icloud.com using a web browser, logging in using your Apple ID, and finding the device in the Find My iPhone web application there.

Set a firmware password

You can also set a firmware password. This makes it impossible to start your Mac up from an external bootable volume unless you enter a password.

You'll probably find most enterprise Macs have this feature enabled by your tech support team — but you must be very careful when you choose to enable it yourself.

Why? If you forget your firmware password, the only way to regain control of your Mac will be by visiting an Apple Service Provider or Apple retail store.

You enable a firmware password by starting your Mac up into Recovery Mode (hold down *Command-R* during startup), and selecting *Firmware Password Utility* from the Utilities menu that appears at the top of the Recovery Mode screen.

- You will be asked to *Turn on Firmware Password*.
- You will then need *to enter your new password* (not your login), verify and set it.
- You can then quit *Firmware Password Utility* and *restart* your Mac.
- Once you set a Firmware Password, you will need to use it only when starting from an external drive, or if you boot up in Recovery Mode or Single User Mode.
- **Please don't ever forget this password**.

Good luck.

Armed with this selection of tips, your Mac should be as strong and stable as it can be for most ordinary use. You may also find a few more ideas to improve your Mac security in this earlier article. *Do you have any good suggestions to help secure your Mac? Let me know via social media below.*

Google+? If you use social media and happen to be a Google+ user, why not join AppleHolic's Kool Aid Corner community and get involved with the conversation as we pursue the spirit of the New Model Apple?

Got a story? Please drop me a line via Twitter and let me know. I'd like it if you chose to follow me there so I can let you know about new articles I publish and reports I find.
