Denver Mac client news

Welcome to our inaugural client tips newsletter being sent to current and past Denver Mac clients. Here you will find tips and information intended to help face the ever changing world of computers and the internet. Please enjoy these writeups intended to make your Mac faster, safer and more fun to use. And as always, reply to this email if you wish to be removed from our list or want to pass along better contact info.

Today's Topic: Security
One of the biggest problems with the internet today is that it puts you within reach of the guys you'd never associate with in your life. Bad dudes who'd corner you and steal your wallet in their home countries if they thought they could get away uncaught. And knowing this, steps that can be taken to minimize the risks associated with your new worst neighbors roaming the internet.

We're focussing on the Macs that live in your home and are connected to the internet through your Internet Service Provider's box, Comcast for example. Laptops, Phones, iPads and other devices that travel with you out the door require additional precautions. We'll cover that in a later post.

Virus Protection
Historically Macs have been relatively immune to virus threats but no more. Bad guys are zeroing in on the Mac community since the base of Apple users has sky-rocked in recent years because they are now seen as worth-while targets. Only a couple of years ago Mac users could snub noses at their Windows PC using counterparts who always required virus software be running. Now there are plenty of Virus software programs availablefor the Mac; *Norton, Avast, and many others*. You might be running one of these now.

Apple's Built In Security

Your Mac comes out of the box with a good amount of hacker and virus protection regardless if or not you use virus software. Here is what they are and what they do.

GATEKEEPER
(Allows download of ONLY Apple Approved programs)
XPROTECT
Apple built-in list of malware threats. A system file.
FIREWALL
Blocks other computers from accessing your Mac. Configured through your router or Mac system preferences.
ASLR
(Address Space Layout Randomization) Prevents hackers from seeing things in the computer's memory.
SIP
(System Integrity Protection) Keeps outside software from changing core settings.Only present with more recent Mac OS X softwasre.
Ref: https://www.apple.com/macos/security/

Among the biggest problems with these virus programs on Mac -

- They beat your computer to death by constantly running system checks and disk scanning. Virus software ultimately shortens the life of computers because they keep running the virus software even when you are not using the computer. The result is faster disk failure, shorter battery run times on portables, hotter Macs.
- In the world of computer viruses, someone has to die before the virus gets recognized and a fix gets issued. Security companies monitor the internet and computers for malicious behavior. When a new threat is found it gets added to their maintained virus list and then gets pushed out to everyone's virus software so other Macs can live.
- You can still get a virus or other malware if it is so new that it hasn't made the virus list just yet. When the virus program on your computer detects an item in the list a red flag goes up and the software springs into action preventing the threat. As time goes by, hackers develop new ways to infect your computer that aren't yet contained in the virus list. Your best defense if to update the list of virus definitions as often as possible.

What is today's best defense? **Install Malware Bytes protection software.**

Malware Bytes Icon

Its recommended that you install the Malwarebytes program. Malwarebytes has been around as a free program for a few years now. Recently they have gone “Big-time” with the release of the 3.0 version. With the 3.0 there is a paid and free version. The difference between the two is the paid version provides constant real-time protection as you peruse the internet while the free version requires a manual click each time a virus scan is run. Both provide the same updates pushed to your Mac as Malwarebytes identifies and updates their lists.

This is the most unobtrusive easy to use protection software we've seen. A final note on Malware Bytes. Running two virus programs can wreck havoc on your computer so if you are currently running a virus program you'll need to uninstall it before installing Malwarebytes. It is all you need for protecting your Mac on the Internet. As an added bonus, its much easier on your computer. You won't even know its running. Be sure to update the protection on a regular basis.

Download the free or paid version here: http://www.malwarebytes.com

Additional steps for your security.
Here's a short list of additional things you can do to further protect your internet experience.

Only download software to your computer from legitimate sites.

Don't follow links on websites to download software. It might be loaded with malware. If you are looking for new programs to add to your mac, go through the App Store that contains only software packages checked by Apple. Or download software directly from a reputable manufacturer. This works best for software like Adobe, Filemaker, Quicken and the most popular names in the business. Often times the software you're interested in will put up a link to download the software from the Apple App store.

Don't fall for phishing or click-bait.
Avoid clicking links in windows that might pop up on a website. Among the most notorious are the Adobe Flash needs upgrading to use this site scam. Flash updates have historically been easy picking' for hackers. During these exploits the user is presented with a popup window telling them Flash needs upgrading before the site can be used. When you click on the window there is a good chance you will be downloading a manipulated copy of Flash that puts your Mac in peril.

Even if the message is legitimate, never click on a popup window to update Flash or any other program, it is just not worth the risk to download the update from an unknown site. What to do?

When you see that Flash update popup window, head up to your Apple Menu and select System Preferences. If Adobe Flash is installed on your computer already you will see the Flash System Preference. Find it in the bottom row of your Preferences Pane. Click on the Adobe Flash pane, then look for update buttons. This ensure the Flash update comes to you directly from Adobe rather than someone else. Now go back to the site giving you the Flash update message and see if it is still there. If it is, its likely you just saved yourself a heap of trouble by doing the update through your system. Legitimate sites make this popup go away once it sees your Flash is updated.

Turn on your Firewall
Firewalls prevent traffic from other computers reaching your Mac. You have the choice of enabling firewall in the Mac, or in your internet router. Turning it on in the Mac keeps foreign computers from connecting to that

Mac. Turning firewall on in the Internet Router, meaning the Comcast, Century-link, or other router you have keeps foreign computers from touching anything in YOUR network, computers, network drives, cameras or anything else, unless an exception to allow it is set up in the firewall. It gets a little more complicated if you're using special services in your home like video doorbells, cloud storage, network drives or Private Networks but each is customizable as needed. Your Mac's firewall settings are found in your System Preferences under the "Security and Privacy" pane.

Turn off Sharing services that are not needed
Perhaps the easiest way of keeping bad guys off your Mac is to disable all the sharing features. To check the sharing status, head back to your System Preferences and locate the Sharing pane. If anything is checked and you can see no reason for it, uncheck the box corresponding to selected sharing service.

Maintain a current Time Machine backup of your system.
If all else fails and you do end up getting bad stuff on your Mac, the the most through solution is to simply erase and restore your Mac to “yesterday” or a designated time before the time your Mac got infected. This wipes the Mac and restores it to a state before the compromise. You'll lose "today's" work by restoring to an earlier backup, but that is remedied by pulling the current files off the Mac before issuing a restore.

Like this? Hate it? Opt out by replying to this message. Your email address will be removed immediately. Positive feedback graciously accepted if you find this is helpful.

Posted 1-13-2017
© denvermacintosh.com

System Preferences covered in this post