303.919.6807 http:// denvermacintosh.com

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.

Item One: 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.

Some of the biggest problems with running virus programs on Mac are,

- They beat your computer to death by constantly running system checks and disk scanning. Virus software ultimately shortened the life of computers because they keep running the virus software even when you are not using the computer. This includes shorter battery run times.
- In the world of computer viruses, someone had to die before the virus gets recognized and a fix gets issued. Security companies monitor the internet and computers for malicious behavior.

Apple's Built In Security

Macs come out of the box with a fair amount of hacker and virus protection. Here they are and what they do.

GATEKEEPER
(Allows download of ONLY Apple Approved programs)
XPROTECT
Apple built-in list of malware threats.
FIREWALL
Blocks other computers from accessing your Mac.
SIP
(System Integrity Protection) Keeps outside software from changing core settings.
ASLR
(Address Space Layout Randomization) Prevents hackers from seeing things in the computer's memory.

Ref: https://www.apple.com/macos/security/

When a new threat is found it gets added to the list and then pushed out to everyone's virus software so other Macs can live.

And how do new virus threats get recognized? Read on.
Here is how virus programs work. There is a baseline of of sneaky actions and types of files contained in a list of definitions within the virus software program. Anytime one of these actions or filetypes are found on your computer a red flag goes up and the software springs into action preventing the threat. As time goes by, hackers come up with new ways to infect your computer that aren't contained in the baseline list. So the people who make the software gather and update the list of threats as they are found and then push them out to their software running on your computer. This is known as a protection or threats definition update. Its basically a list of all the known malware that infects computers and all the new threats are gathered and put into the list where that updated list eventually ends up on your Mac.

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. Theres 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 to work. Both provide updates pushed to your Mac as Malwarebytes identifies and updates their lists. A final note on Malware Bytes. Running two virus programs can reek havoc on your computer so if you are currently running a virus program, uninstall it before installing Malware bytes. It is all you need. Plus it is 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

Item two: Additional steps and Added security.
Here's a short list of additional items 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.

Don't click on the 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 though the message might be a legitimate request to update an outdated Flash 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, do not click on anything. Instead 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.

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 cleanest solution is to simply erase and restore your Mac to “yesterday” or a designated time before the time you were infected. This wipes the Mac and restores it from a time before you were infected. 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.

Turn on your Firewall
Firewalls prevent traffic from other computers from 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 keeps foreign computers from touching anything in YOUR network. It gets a little more complicated if you're using special services in your home like video doorbells, cloud storage 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 not needed
Perhaps the easiest way of keeping bad guys off your Mac is to disable all the sharing features. Head back to your System Preferences and locate the Sharing pane. If anything is checked and you can see no reason to use them, uncheck the box corresponding to sharing.

Like this? Hate this? Opt out by replying to this message. Your email will be removed immediately. Feel free to reply with positive feedback if you find this is helpful.

Posted 1-13-2017

303.919.6807
http://
denvermacintosh.com

System Preferences used in this letter