Secure my Mac? Yes!

Jesse Wootton, BBA
President, Age of the Geek Computer Solutions, Kitchener, Ont.

Correspondence to:
Mr. Jesse Wootton, Age of the Geek Computer Solutions, 1170 Fischer-Hallman Rd., Unit 230, Kitchener ON N2E 3Z3;
www.ageofthegeek.ca;
jesse@ageofthegeek.ca

I have a Mac — I don't need antivirus software!" This is a major selling point for the increasingly popular line of Apple products. While this sentiment makes people comfortable with their personal computers, it scares information technology (IT) departments and gives a somewhat false sense of security. Although it is true that there has never been a "virus" for the Mac OS X operating system, there have been a few malicious programs that have caused trouble for end users. Malware (malicious software) consists of any unwanted program on your computer. This includes anything from viruses and spyware, to applications that are simply advertisements.

By definition, a virus is a program that self-replicates and installs itself on the host computer in order to spread and infect others. A virus requires no input from the end user. A Trojan horse is a type of malware that requires the end user to make a mistake and install it themselves. On the Mac, this requires entering your password. There have been a few Trojan horses that have received a lot of press and, although they are dangerous, they do not have the properties of a virus and cannot spread without user input. The number of threats that affect the Mac operating system pale in comparison to those that affect its Windows counterpart, but there are still ways to protect yourself from the few threats that exist.

MACS ARE NOT IMMUNE TO EMAIL SCAMS

Although most of us will not send a money order overseas at the promise of riches, being careful with your email will help to protect everyone on your contact list as well as yourself. Popular email hosts such as Yahoo, Hotmail and Google all provide convenient access to your account from any computer in the world. Having a secure password here is imperative. If your account becomes compromised, the first thing that will happen is that your contact list will be downloaded. Once scammers have that, they no longer need access to your account. They can spoof your email address so that people believe emails are coming from someone they know and trust. That picture of your recent vacation now contains a virus. The best thing to do is to use the built-in Mail application of Mac OS X and keep your contacts stored locally on your Mac instead of in the "cloud," where it can be more easily accessed.

KEEP AN EYE ON WHAT YOU DOWNLOAD

Pop-ups can be annoying, but are usually not doing anything to your Mac. What you need to be careful of is that pop-ups can trigger files to be downloaded to your computer. These will appear in your downloads folder (or desktop folder on older Macs). Basic principle: if you didn't download it on purpose, don't open it. There is an added benefit in OS X in that it requires you to input a password every time something is installed on your computer, so malware cannot be installed without your input.

BE A GOOD NEIGHBOUR — DON'T INFECT YOUR WINDOWS FRIENDS

Although the amount of malware that

can affect Macs is small, Macs can be carriers of malicious programs. This is why IT departments sometimes have problems with Macs. Having an antivirus program on a Mac is largely unnecessary for the end user, but it is a good idea if you share a lot of files with Windows-based machines. Here is an example. A Mac user downloads a picture of a cute puppy from a website. This picture has a virus attached to it, and, although it does no harm to the Mac user, the infection can spread once it is sent to a Windows machine. This is the main reason to run an antivirus program on a Mac. ClamXav (www.clamxav.com) is widely considered one of the best free antivirus programs for the Mac. Most of the major antivirus companies have Mac versions of antivirus software, but there is little need to pay for protection in Mac OS X. If you are worried about spreading viruses, using ClamXav to scan files you are sending is a good way to prevent it from happening.

KEEP YOUR MAC HEALTHY

There are a number of ways to ensure that your Mac is running to the best of its ability so that it is able to ward off malware and other security threats. Most of them are very simple. The first thing is to make sure that you have the latest updates from Apple. Even the older operating systems have updates. By clicking the Apple logo in the top left of your Mac and choosing software update, you can ensure you have the latest updates. These updates add features to some software as well as patch any security holes that have been found.

Repairing disk permissions regularly is the best way to keep your Mac running quickly. This is done by opening the "Disk Utility" program located in the Utilities folder of your Applications folder. Once the program is open, select your main disk "Macintosh HD" by default. Under the "First Aid" tab you will find a "Repair Disk Permissions" button. It will take a few minutes to complete and you may get a message that states certain things will not be repaired, but that is normal.

One last thing to do is to make sure you have enough disk space on your Mac. In the Finder, select your Main disk and choose "Edit" and "Get Info." This will tell you how much of your disk is being used and how much free space you have. The general rule of thumb is that you want at least 15% free disk space. This is a good number to go by, but if you have a large drive, you can get away with having a smaller percentage of free space. If you do not have enough free space, start by emptying your trash. A good free tool to find out what is taking up all your space is JDiskReport (www.jgoodies.com/freeware/jdiskreport/index.html). This can be downloaded for free and is very simple to run. If you have a lot of music, movies and pictures taking up most of your space, consider moving them to an external drive. Be careful how you store your data, and always have important data in more than one place. I cannot stress this enough — data recovery can run into the thousands of dollars just to retrieve information from one drive.

Competing interests: None declared.