

Apple Macintosh viruses reported

Posted At : April 27, 2012 2:44 PM | Posted By : Admin

Related Categories: Apple, Computers, Security, General Info

April 1st - the day when all sorts of jokes, stories, and elaborate hoaxes are played on the public by venerated news organizations, manufacturers, the government, and of course from the Internet. Our friends at Google launched a fantastic new product based on Morse Code. NOT!!

However, this past April, an issue that has been around for a while created quite a media stir and wasn't a joke. Apple Macintosh computers getting viruses or more precisely a thing called a "Flashback Trojan Horse". Thousands of words were written about over 600,000 Mac computers being attacked by malicious malware code. We had quite a few clients call us and bring-in their Macs - just to check.

So, is this real, a big deal, or not? Some facts and suggestions:

The first thing to understand is yes, this particular issue is real. However, the infection of 600,000 computers is actually quite small. There are literally millions of Apple OS X licenses out there. Not as many as PCs, but as these things go, this infection is pretty minor. Our shop checked a number of client Macintoshes and we checked all of The Computing Center's own machines. Not one of them had the Flashback Trojan.

The second point is that Apple and others were all over this. Within a day or two of the outbreak, Apple had an upgrade to its operating system available at no charge available to every Mac user. It removed the Trojan if it existed and closed the technology hole that allowed it to occur. By simply downloading and installing the latest OS-X upgrade (about a 30-45 minute process mostly depending on your internet speed), this problem is fixed. Several other companies had scanners and fixes available as well.

Third and most important: Apple Macintosh OS X based computers can catch viruses. OS X is not immune. It appears that it is more difficult to write a virus to infect OS X, but not impossible. The simple fact is that there are far fewer Macs than PCs, so it's a smaller target. Kids and social hackers aren't the ones writing viruses these days. Organized crime and some covert international government agencies are the ones creating most of the attacks. Criminals are looking for ways to extract money from you, your bank, or to hide their tracks while attacking others. Alleged international government agencies are likely looking for information or hiding their tracks while performing more covert surveillance. In the end it's a numbers game and there are more PCs.

So what to do? If you own a Macintosh, first make sure that you are running the latest version of OS X. Unlike Windows which delivers patches and downloads weekly, upgrades to OS X happen infrequently. Second, install some kind of anti-virus software. There are several free ones out there that are OK. Norton, Kaspersky, McAfee, and a number of Mac specific companies make very good and inexpensive anti-virus and anti-malware products. They are all easy to use and quite easy to install.

Lastly, just like PCs, practice safe computing. Make sure you know the websites that you are connecting to. Don't open email attachments unless you know the source. Don't wirelessly connect to just any WiFi network. And if you do suspect a problem, we have Macintosh specialists on staff to help you figure out what's wrong and get it fixed.