

THE COMPUTER CORNER

No. 247: Adware

Stan Kaplan, WB9RQR 715 N. Dries Street Saukville, WI 53080-1664
(262) 268-1949 wb9rqr@att.net

We have all seen it. You go online with your favorite browser, and suddenly, ads slide in from the sides, pop up over what you want to see, and generally act to distract you from your intended task. Sometimes they bug you so much you forgot what you intended in the first place because of their incessant intrusions and your efforts to close them. These are ads by advertising supported software, or adware for short.

So, this is unwanted advertising, thrown on your screen without your permission or consent. As an aside, the definition for a computer virus put forth many years ago is a program that does something to or with your computer without your permission or consent. So, we are really dealing with a type of program that has been around for a long time – a computer virus. There are just a couple of differences between a virus and adware.

A computer virus is a bad actor that often damages your data or programs, sometimes even when that was not the writer's intent. Adware is out to flash unwanted ads in your face, thus generating revenue for the developer. In other words, people write programs to infect your computer with popup ads, and they get paid for doing it. You may see ads for bogus miracle weight loss schemes, warnings about your virus-infected computer (when it really isn't infected with anything other than the adware), phony dietary supplement ads, and the like. Some would say that it is just good, old fashioned advertising, but it is not. Anything done without your express consent and permission should be illegal and not supported. If it were up to me, I would levy a \$100 fine on the advertiser for each instance of an unwanted popup displayed without permission. That would help stop it!

Signs that you are infected with adware (thanks to Malwarebytes for this list, and for solving some of the problems of adware and other viruses):

1. Advertisements appear in places they should not be.
2. Your browser homepage has changed without your permission.
3. Web pages you visit are not displaying as they typically do.
4. Clicked links take you to unexpected sites – different than you expected.
5. Your browser slows down markedly.
6. Your browser suddenly sports new toolbars, plugins or extensions that you did not ask for.
7. Your machine starts automatically installing unwanted software packages.
8. Your browser starts crashing a lot.

How did you get infected? One way is to download an infected program (the same way you can get infected with a virus by downloading an infected program). The other way

is called a ***drive-by download***, wherein just visiting a site lets the adware burrow in to your machine without your permission. Either way, you are hooked.

What to do? A first is to install an anti-popup program into your Firefox, Chrome or other browser. Adblock Plus, Adblocker Ultimate, DuckDuckGo Privacy Essentials are free and easy to incorporate into your browser. Another solution is to clean your machine - kill any existing infections. For a simple adware removal tool, install and run AdwCleaner by Malwarebytes. For the ultimate answer install and run Malwarebytes Antimalware (free) and run a scan. It will find any PUP (Potentially Unwanted Program), including those that feed ads, and will clean them all up. Its free for 14 days and will watch your back automatically during that time. After 14 days, it still works just as it did before, but you must run it manually each time. Pay their fee and you have the professional version that is totally automatic (I did!). It will prevent future infections, even as you browse. Go to majorgeeks.com for any programs mentioned in this article.

So, fight back! Kill those pain-in-the-rear ads, all of them. The computer belongs to you! Happy Computing!