

Kretchmar's Korner

How to Destroy Your Computer in Just Minutes

Why You Should Avoid Installing PUPS (Potentially Unwanted Programs)

By David Kretchmar, Computer Hardware Technician, Sun City Summerlin Computer Club, NV

April 2017 issue, GigiBytes Gazette

www.sccsc.org / tomburt89134 (at) cox.net

There are plenty of new computers being used that are performing much more slowly than they should. One of the quickest ways to turn a fast, new computer into a slow system crippled by malware is to start downloading software from the wrong sites. Or by downloading the wrong software from what appears to be the right site.

Newer computers being slowed by unwanted programs is a bother, but the damage done by PUPs can be much more serious; PUPs can be responsible for programs that make it impossible to access any of your files, or otherwise ruin your system.

Every time you download anything from the Internet you first issue permissions that enable the opening of a conduit or vector between the Internet and your computer. The



series of complex events is mostly invisible to you, except for your clicking on that virtual button that starts the whole process.

Bing and Google searches often can take you where you don't want to go. When searching for popular software, sponsored search results (which result in unwanted programs) often appear at the top of the search results page, along with links from the actual software source sites. Often those ad links try to install software on your computer that you do not want. It could be anything; it could

be a fake driver update program or a scam system cleaning program. Note that my Bing search for VLC media player (left) first showed 4 sites NOT associated with VLC – bad sites.

Testing Misleading Advertisement links

How bad is it? To find out, I installed a fresh Windows 10, plus all Windows updates, on a freshly formatted hard drive. I downloaded and installed the free version of Avast! Antivirus software that brought a hitchhiker of its own - Google Chrome. OK, I wanted Chrome, but not every user would, so I considered this an invasive act by a program I downloaded for protection.

I used Edge, Firefox, and Google Chrome and started using Google and Bing search engines to start searching for popular free programs. The programs I sought are often the first programs that get installed on a PC; Firefox, Google Chrome, OpenOffice, iTunes, Adobe Flash, Java, Adobe Acrobat, VLC, and WinZip. Then, I carelessly clicked on ad results, which appeared above or on the same first page as "real" search results. These paid ads were identified by notes and highlighted in a very pale color to differentiate them (slightly) from the actual search links that appeared nearby.

The ads didn't appear after every search and the ones that appeared varied among searches and were different for different browsers. Sometimes, the first paid ad link actually took me to the software's true source site (i.e. searching for Google offered www.google.com first). Often Avast would block a download it recognized as harmful, but Avast did not catch many problems.

For all of the searched for programs, I was able to bring up more questionable sponsored search results within seconds of repeated searching. Misleading results showed up in all search engines and I could not determine that any browser offered better or worse protection than others.

For each ad link, I clicked through and installed the respective programs via the link or button provided. Instead of delivering just the application I was looking for, all of the paid links attempted to tack on unwanted programs. In some cases, if I was careful to read all of the fine print and uncheck boxes, I could get the files I was looking for without a bunch of extra "added value" software, but it was very difficult.

For the purposes of this article, I acted as an inexperienced user (or an experienced user who's not paying attention), and clicked my way through ads and dialogue boxes that looked like the End User License Agreement (EULA) we're used to seeing through when installing software.

And ... They Got Me!

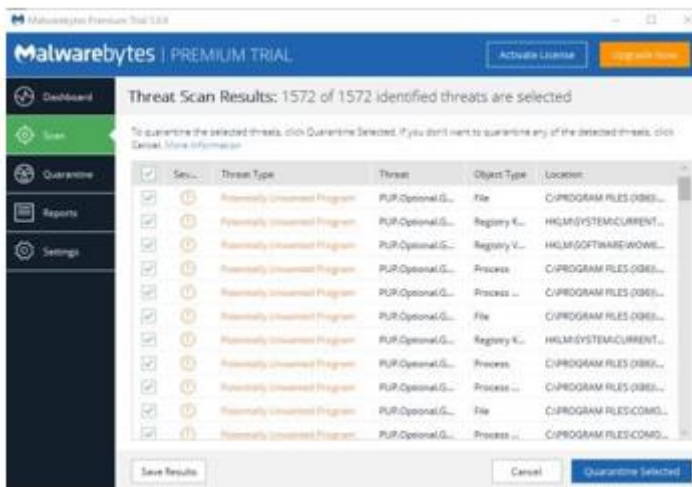
After installing just a few programs this way, I started accumulating browser toolbars (Bing, Yahoo, and Google), and noticed my search engine and home page had been hijacked to something unwanted. As I continued the process, Windows started slowing down to a crawl.



After installing all of the programs on my list, I opened Windows 10's Programs and Features and each browser's extensions and add-ons and counted 39 items that had been installed in addition to the programs I intended to get. On rebooting, three new programs launched popup windows at startup, including two that started running virus/registry scans as soon as they launched, and a couple that flashed warnings windows and offered fixes if I registered and/or upgraded to the full paid version.

Remember this was originally a clean install of Windows 10 that needed nothing.

Within a few minutes my computer became noticeably slower, plagued by numerous popups, and was becoming essentially unusable.



All of these were nasty, but if even a small fraction of them were, I would be in real trouble.

Conclusions and Recommendations
Most of us will have to download some third-party (non-Microsoft) software from the Internet. This does not have to be dangerous if you pay attention that the software is being offered from the true home site of that product.

NEVER download software from any sponsored link, unless the desired software creator is the sponsor.

Do not depend on your anti-malware program to protect you. It will catch some issues, but not all.