Science Translations
Established 1990
PC410.COM™
PC Updater News

Malware Awareness: What's a PUP?

Not every evil bit of software is a virus. Most of the software that scans our computers for bad software is no longer called anti-virus, but is known as anti-malware or endpoint protection. That's just a bigger category. Malware is the general name for all bad software, but a virus is just one specific type of bad code. A virus is generally a document that infects other documents, and most current malware threats are of other types than viruses.

Right now, most malware fits into these categories:

By Delivery method:

- **Drive-by download:** Arrives while visiting sites with bad content, including bad ads on good sites, without Endpoint Protection, mostly delivers adware.
- **Phish:** Email that claims to be something it is not, as fraud, or an attempt to allow malware to run.
- **Spear Phish:** Like phish, but targeted at one company or user, includes very specific references to names, or shows other internal knowledge of the target.
- **Trojan Horse:** Usually claims to be a document, but is really a program.

And by Type of Malware:

- **Adware and Spyware:** Displays ads on your computer, and tracks users without permission.
- **Ransomware:** Encrypts your computer and blackmails for ransom.
- **Cryptojackers:** Sits in the background and does cryptocurrency mining, slows down and overheats computers.

Most of everything above is blocked by endpoint protection software, with one exception, and that's Adware that has been categorized by the security community as a PUP. That's a "Potentially Unwanted Program." It's a friendly name for software that is not anything that anyone would want, probably named by lawyers who didn't want to brand a category of software as evil, because there are companies behind these PUPs, and some of them have their own lawyers. More on that at my SoftwareKB.com website, here:
A PUP is a Potentially Unwanted Program

Most of the PUPs are add-ons for browsers. Good add-ons can add features to Google Chrome, Firefox, and the the other browsers, but the PUP add-ons are mostly garbage attempts to offer free maps, translations, recipes, coupons, and any other digital information that you could easily find directly on Google by

doing a simple search for them. The problem is that these add-ons make their money by selling YOU, either as advertising targets or by sales of your information, targeting you for ads elsewhere based on where you've been online and what's on your computer. Nearly every offer that you see that offers these items is bad, and you should never allow them to install. Always ask: What's their revenue model? They're paying for advertising space to tell you to allow the installation of something that's *free*, so where do they get their money? If you aren't their customer, you're their product.

The good news is that all the endpoint protection programs have an option to treat PUPs as bad and block them. The bad news is that it is turned OFF by default. If you're running Webroot that I configured, that option is turned on. For any other software, you probably need to go into the options, find and turn on the 'detect PUPs' option. It may be in the 'real-time protection' section.

The visible result of installing any of these PUPs is that the computer slows down, and pops up more advertisements, sometimes even when the browsers are closed, because browser add-ons can run even when you are in some other program. So to get rid of them, you can generally check that PUP detection is on, and then start a full scan in your anti-malware software. Or look in the add-on list, and delete them. In each browser, there's a button or slider to turn off the add-on, and an option to delete it.

In Chrome, click the menu link, the three bars icon at the far right in the top toolbar. In the list, choose More Tools... and then Extensions.

In Firefox, click the menu link, also the three bars icon at top-right, and choose 'Add-ons'. In the left column, look at Extensions and Plugins.

For Internet Explorer, wait, stop. No one should be using Internet Explorer. It’s obsolete, and no longer considered to be safe. Use Google Chrome or Firefox, or in Windows 10, there’s the Internet Explorer replacement, Microsoft Edge.

Zoom In, Zoom Out

As web sites are updated for use on phones and tablets, sometimes, they’re just too big to fit on our monitors. In all the major browsers, you can zoom in by holding down Control (or Ctrl) and tapping the + symbol. Use - to zoom out. Ctrl and 0 resets the zoom back to the original setting. These shortcuts also work in most email programs.