**Volume #4 - Issue #152**
**March 23rd, 2018**

**This is a weekly publication dedicated to your personal cyber security. Our newsletter is designed to help the public recognize and avoid cyber threats while they are online. If you are not a subscriber, please go to [HomeCyberDefense.net](HomeCyberDefense.net) to sign up.**

# Removing Adware

Adware is the most common and least dangerous type of hack, but it can be really annoying. These programs track your habits, spending, and other user information in the form of “cookies.” Cookies are mini programs that are stored on your computer that allow sites to retain basic information about you. Normally harmless, cookies are the reason that, if you look at shoes on one site, you may find that same product appearing in windows on another. In other words, your behavior and preferences are being

tracked and cataloged, without your permission. (Luckily, you can turn your cookies off.) So basically, while malware is meant to be malicious and do damage to you and your device, adware is more of a nuisance, tracking you and relaying information to a 3rd party get you to buy something.

**Adware Symptoms:**
Slow web browser performance, annoying ads (searches, banners, text links, transitional, interstitial, and full page advertisements), browser redirects.

**Distribution:**
Adware is often included within freeware or shareware programs, and the installation of potentially unwanted applications can be caused by deceptive free software download clients and installers. Adware is also installed via fake Flash Player, Java, or Internet browser updates. Potentially unwanted programs are distributed by the use of misleading banners and other online ads.

**How to avoid adware infections?**
To avoid installation of adware, Internet users should express great caution when downloading and installing free software. If your download is managed by a download client, be sure to opt-out of installation of any advertised browser plug-ins by clicking on a ‘Decline’ button. When installing previously downloaded freeware, always choose ‘Advanced’ or ‘Custom’ installation options, rather than ‘Quick’ or ‘Typical’, since choosing the default options can lead to unwanted installation of bundled adware. Also, avoid participating in surveys or contests that may popup when you go to certain websites.

Here is where it gets interesting, the legality of spyware is a tricky business. It is regulated in the U.S. by such laws as the United States Computer Fraud and Abuse Act. However, there is a catch. While some of the many malicious malware creators have been arrested and cited under federal law, a large number are legitimate businesses that distribute adware are

working openly and prospering nicely. In their cases, you have actually invited them into you computer, knowingly or not. Let's say you decide to buy a downloadable game from a site. Before they allow you to spend your money, they demand that you consent to their "terms of licensing agreement" before installing. That multi-page document that you probably scrolled through as fast as humanly possibly without really reading is a fine bit of clever marketing wording that says, in effect, that they are going to install a program that tracks your every move and targets you for ads based on these moves. Since you consented to this in the terms & conditions, the courts have agreed that it's not an illegal download.

**Removing Adware**

Adware is usually easily removed. You can use relative inexpensive, or even free Malware removal programs to scan and remove aware. (But research what you are using first so you don't use a program that installs something worse on your computer. I am partial to MalwareBytes.) Or, if you are a do-it-yourself type of person, you can remove adware manually using the following steps:

**STEP 1**

From the "Start" menu, select "Settings" and then "Control Panel."

**STEP 2**

Double-click the "Add/Remove Programs" option.

**STEP 3**

Select the adware program and click "Remove."

**STEP 4**

Restart your computer to allow all changes to take effect.

**STEP 5**

Press Ctrl and Alt together and then Del to bring up the Task Manager window if the Control Panel procedure in the preceding steps does not successfully remove the adware from your computer.

**STEP 6**

Select the "Processes" tab.

**STEP 7**

Scan the list of processes that are running on your computer to identify any adware. “System” and “System Idle Process” are not programs that you need to worry about as being adware. To find out whether a process is adware or not, determine what the process does by looking it up in a process library such as the Uniblue webpage listed in the Resources section.

**STEP 8**

Select each adware process and click “End Process.”

**STEP 9**

From the “Start” menu, select “Search,” “Files or Folders” and “All Files and Folders.” Enter the name of the adware file, which will usually be an EXE or COM file, exactly as it was listed in the Task Manager window.

**STEP 10**

Delete the file or files returned by the search.

**STEP 11**

Restart your computer for all changes to take effect.

As stated before, if you are not comfortable doing the above steps, you can use a malware removal program such as MalwareBytes, or take your computer to a professional.

## This Week’s Cyber Alerts:

**Alert Issued 3/22/18** **The Password to Your IoT Device is Just a Google Search Away**

**Alert Issued 3/21/18** **880,000 Payment Cards, User Info Hit in Orbitz Data Breach**

**Alert Issued 3/20/18** **Cyber-Crooks Find a New Way to Share Malware**

**Alert Issued 3/19/18** **Google Tricked into Serving Scam Amazon Ads**

**Alert Issued 3/16/18** **Researchers Find 29 Types of USB Attacks, Recommend Never Plugging into a USB You Don't Own**

**Alert Issued 3/15/18** **POS Malware Found at 160 Applebee's Restaurant Locations**

**Alert Issued 3/15/18** **Why You Should Never Pay A Ransomware Ransom**

**Alert Issued 3/15/18** **Your Smart Camera may have been Spying on You**

**Alert Issued 3/14/18** **Microsoft Removes Antivirus Restriction Blocking Windows 10 from Getting Updates**

**Alert Issued 3/13/18** **macOS Malware Increased by 270%**

**Thank you for subscribing to our email!**

*Copyright © 2015-2017 House of File Technologies*