

The following is a list of the terms used to describe malicious software, a brief description of each, and how to deal with them.

Viruses

A virus is what attaches itself to a program or file so it can spread from one computer to another. The effects of a virus can range from harmless messages that appear on your screen to wiping out data on your hard drive. A good rule of thumb to avoid being infected is to **never** install a program, (*something.exe*), from an internet site unless you are sure what it is, and **never** open an email attachment unless you are sure who it's from. These days, every computer should be running a good virus scanning program as well. Clearpoint Computer Services recommends **avast! 4 Home Edition** from ALWIL Software.

avast! 4 Home Edition is a full-featured antivirus package. Home and non-commercial Windows 98/ME/NT/2000/XP users can register it at no cost. It's easy to use and does not slow down your computer.

VIRUS TIP: A good way to prevent your computer from sending viruses to everyone in your email contact list is to create a contact in your address book with the name !0000 with no corresponding email address. This contact will then be listed as your first contact. If a virus tries mail itself to everybody in your contact list, it will try to send it to !0000 first, and your computer will display an error message similar to:

“The message could not be sent. One or more recipients do not have an e-mail address.”

The offending message (and the virus) may then be automatically stored in your Drafts or Outbox folder. Go in there afterwards and delete it.

(This tip may not work if you use AOL.)

Trojan Horse

A trojan horse is an unwanted program that infects your computer so a hacker can remotely control it. The name comes from the Greek legend, because the scenario usually happens like this: You download a program from the Internet because it looks good - but once the program is opened (or run), it releases the unwanted program. The hacker then has access to your computer and can do anything from changing your screen settings to saving your credit card number to a file when you type it in.

The best way to avoid becoming infected is to never install any program unless you are sure it is safe.

Trojan horses do their best to stay out of sight and avoid detection, so they can be difficult to detect and remove. For that reason, getting rid of them is best left to trojan removal products.

Clearpoint Computer Services scans for trojan horses and uses proven trojan removal products to eliminate them.

Adware

An Adware program is what produces pop-up advertisements. When you accept the license agreement when installing certain “freeware” or trial software, you give your consent to run the adware imbedded in it. Trial software allows you to try out the software before you buy it. If you purchase a registration key, the ads are removed. Freeware programs, like Juno email, use adware to display sponsor’s advertisements. The advertisements usually run in a small section of your screen or as a pop-up on your desktop. When you stop running the software, the ads disappear. Most consider it a reasonable alternative offered to consumers who do not wish to pay for programs, games and utilities. With trial software, most or all features of the retail version are included, but you will be viewing sponsored advertisements while using the free version.

It is important to remember that not all companies who claim their software contains adware are really offering adware. There is always a chance that adware is spyware in disguise - and that programs with embedded spyware might not even state its existence at all. Due to its invasive nature, spyware has really given adware a bad name as many people do not know the differences between the two, or use the terms interchangeably.

Clearpoint Computer Services recommends Lavasoft’s Ad-Aware SE Personal edition to scan your computer for Adware. It’s free to use. The registered version includes real-time protection that allows you block Adware.

Spyware

Unfortunately, some freeware applications that contain adware track your Web surfing. Once installed, the spyware monitors user activity on the Internet and transmits that information to a third party in order to serve you personalized ads. For example, if you visit travel sites, you might see a banner that advertises a 40% discount on travel on a particular site. When the adware becomes intrusive like this, we move it in the spyware category. It becomes something you should avoid for two reasons. First is the privacy and security issue - spyware can gather information about e-mail addresses and even passwords and credit card numbers. Secondly, all the background activity spyware generates slows your computer down.

Oftentimes spyware is installed without the user's consent. It may be the result of clicking some option in a deceptive pop-up window, ([a pop-up download](#)), or as a [drive-by download](#).

Most anti-virus or firewall programs are not designed to protect you from spyware or adware, but there are many good spyware detection and removal tools available.

Clearpoint Computer Services recommends Spybot Search & Destroy. Spybot Search & Destroy can detect and remove spyware from your computer, and it’s free. The Spybot screen has a “Donations” button to contribute to their cause, but that is completely voluntary.

Important Note on Spyware and Adware:

License agreements often prohibit modifying software that makes use of Spyware or Adware. If you use freeware applications, read your license agreements before removing software components.

Pop-up Download

A pop-up download is a pop-up window that tricks you into downloading a program. The trick is to get you to click inside of a pop-up. Often, the pop-up window has no information about the program to be downloaded; instead telling you something like your computer is low on memory, and to “Click Here” to fix it. Never click anywhere inside a pop-up. Exit out of all pop-ups by carefully clicking once the “X” button in the top right hand corner of the pop-up window or by right-clicking anywhere inside the pop-up’s task button in the task bar at the bottom of your screen and then choose “Close” from the menu.

As general rule, stay away from web sites with numerous pop-ups and free stuff. If you can't figure out how a free site is making money, then there's a good chance they are getting paid to put spyware on your machine.

To avoid pop-up downloads, make sure your browser is equipped with a pop-up blocker.

Clearpoint Computer Services recommends the free Mozilla Firefox browser, which comes with a built-in pop-up blocker. For Internet Explorer users, the no-cost Google Toolbar has an excellent built-in blocker. Windows XP user with Service Pack 2 can use the tool built into Internet Explorer 6.

Drive-by Download

Unlike a pop-up download, which tricks you to into approval, a drive-by download is carried out invisibly to the user: it can be initiated by simply visiting a Web site or viewing an e-mail message.

Drive-by downloads work by exploiting flaws in your Web browser and operating system software. Windows and Internet Explorer are the primary targets. For Windows users, routinely installing Microsoft’s security patches is the best deterrent

Cookies!

Cookies are small files that are automatically sent to your PC when you browse certain Web sites. They are stored on your hard drive so the Web site can recognize you when you return. For example, when you are shopping online, cookies make it possible for you to add items to your “cart”, continue shopping, and "check-out" later.

Since they track where you have been, Web sites also use them to gather statistics useful to marketers. Information gathered via cookies can sometimes be matched with information gathered elsewhere to provide surprisingly detailed profiles of you and your browsing habits.

If you setup your Web browser to not allow a site to send you their cookies, oftentimes it prevents you from visiting that site. If you set up your Web browser to prompt you each time a site wants to send you a cookie, you will see lots and lots of pop-up messages asking if you want to accept them one at a time. So, most people go ahead and allow them. They don't take up much room, and you can delete them whenever you want. A cookie can stay on your machine for a long time, or they can expire after a session or on some date.

To view or modify your cookie settings, type the word "cookie" into your browser's "Help" index.

Browser Hijacker

Browser hijacking is a constant danger on the World Wide Web. It is a particularly offensive type of spyware that changes your default homepage to other Web sites, often porn sites. Why? So they can artificially inflate their "hit counts" to command higher advertising rates. They also bombard you with pop-up ads, add themselves as "Favorites" and enable third parties to snoop on your browsing activity.

Browser hijacking is hard to recover from without specialized hijack removal tools. In most cases, the hijacker will have made registry changes deep within your system. Sometimes these registry changes are accompanied by malicious files on your hard drive that change your settings every time you reboot your computer. So, even if you manage to fix your settings, they are changed back the next time you restart.

Browser hijacking isn't really a virus, so anti-virus programs can't always stop it. These programs have even been known to disable antivirus and anti-spyware software. Clearpoint Computer Services uses proven hijack removal tools to rescue your computer from Web hijackers.

Browser Helper Object (BHO)

A Browser Helper Object, like a browser hijacker, is a small program which runs automatically every time you start your browser. Usually a BHO is installed on your system by free downloaded program. Oftentimes the notification that you are about to install a BHO is contained in the End User License Agreements, which most people routinely "Agree" to during the installation process with the click of a button.

There are benign ones, actually designed to "help" you browse the World Wide Web. Others have the capability to completely control your browser. Most BHOs are unwanted pests which violate your privacy, cause system problems and lower performance.

Clearpoint Computer Services uses a free tool, BHODemon, to ferret out BHOs and eliminate the nasty ones. Once installed, BHODemon monitors your Windows Registry and alerts you when a BHO is installed.