



### Terminology to Understand

**Virus** - In computer security technology, a virus is a self-replicating program that spreads by inserting copies of itself into other executable code or documents (for a complete definition: see below). Thus, a computer virus behaves in a way similar to a biological virus, which spreads by inserting itself into living cells. Extending the analogy, the insertion of the virus into a program is termed infection, and the infected file (or executable code that is not part of a file) is called a host. [Wikipedia]

**Spyware** -Spyware is a broad category of malicious software intended to intercept or take partial control of a computer's operation without the user's informed consent. While the term taken literally suggests software that surreptitiously monitors the user as a spy would, it has come to refer more broadly to software that subverts the computer's operation for the benefit of a third party. [Wikipedia]

**Trojan Horse** - is a malicious program that is disguised as or embedded within legitimate software. The term is derived from the classical myth of the Trojan Horse. They may look useful or interesting (or at the very least harmless) to an unsuspecting user, but are actually harmful when executed. [Wikipedia]

### Key things you need to do to help maintain a healthy stable computer system.

1. Run windows updates on a regular basis (at least twice a month). Open internet explorer then at the top of the menu bar you will see "tools". Left click on "tools" and left click on "windows update". This will take you to Microsoft's windows update website. Only Genuine copies of windows will be able to perform updates.
2. Be sure to use current and up-to-date Anti-virus/Anti-spyware software. To get the maximum protection it is recommended to run two separate programs that specialize in both virus and spyware protection. IE: Norton, Panda, PC-Cillin for anti-virus and Spysweeper or Spyware Doctor for anti-spyware. Make sure to run system scans at least once a week and run their update utility each time to be sure you have the latest definitions before you scan.
3. No matter how much protection you have, you are still vulnerable to mal-ware (any program designed to cause harm to your PC) through infected websites, flaws in email clients, P2P programs, and undetected vulnerabilities in Windows as they become discovered. Your very best defense against mal-ware is going to be YOU. Meaning that by using certain precautions and being aware of what you or your family are doing on the internet will go a long way to help your system stay clean and running smooth.
4. It is in your best interest to not use or install P2P (peer to peer programs) such as: Kazaa, Bearshare, Lime Wire, WinMX, and Bit Torrent applications. These programs have a nasty habit of packaging spyware and trojan horses into their software. Furthermore, the copyrighted content that you are sharing is also considered pirated software. The RIAA (recording industry lawyers) is cracking down on piracy and actively monitors P2P networks looking for software pirates for whom they will take legal action against. So for yours and your computers sake stay off the P2P networks!
5. Be mindful of what websites that you visit. With 66% of the internet composed of adult material, it is very easy to type an innocent phrase into Yahoo! or Google and a link to adult content be displayed. Adult websites are notorious for infecting computers with unwanted Spyware and Virus's.

If you run into a instance where your anti-virus or anti-spyware software cannot remove an infection from your computer do not panic. PC Gurus is a phone call away and we can rescue your PC from any problem that might come up. Just Give Us A Call!