What's the difference between a Virus, Worm, and Trojan horse?

Very commonly we hear about these three types of computer problems and although the terms get used interchangeably, each is vastly different. They are all various types of malicious software but differ in their affects and how they spread. Being informed on the cause and effects will better prepare you in keeping your computer safe.

Virus
A computer Virus is embedded code or attached to a file where it infects the computer when the file is executed. Viruses are spread through users transferring files, usually unknowingly, through e-mail or file sharing. Even if you download the infected file the Virus cannot act until the malicious file is executed, which means it won't harm your computer until you run it. Note that the only way a Virus can spread is through user involvement; it cannot execute or transfer itself independently. It can infect other files on your machine however, it cannot replicate itself.

Worm
A computer Worm is similar to a Virus by design and is considered a sub-class of a Virus. The difference is that a Worm gains access to your systems transport features and is able to travel unaided by the user. A Worm also has the added ability to replicate itself, so instead of sending out a single Worm it can send out hundreds and thousands of copies of itself creating a vicious cycle. Because of its ability to reproduce it can end up using tons of system memory and bandwidth causing servers and individual systems to crash. Unlike a Virus, it cannot infect other files on your computer.

Trojan horse (aka Adware/Spyware)
Typically a Trojan will appear to be a useful and legitimate application from a legitimate source and could possibly promise to clean your system of viruses or search your registry for spyware. When you execute a Trojan the results could vary from as little as changing your desktop wallpaper, creating annoying pop-ups, or to the extreme of deleting and destroying files and programs. Trojans are also known for creating backdoors to your system that allows malicious users to gain access to files and information. Unlike a Virus or Worm, a Trojan cannot infect other files or replicate.

Frequently Asked Questions

Where does the name "Trojan horse" come from?

It originates from the Greek story of the Trojan War in which the Greeks gave a wooden horse to their foes the Trojans as a peace offering. Once the gift was brought inside the city walls, the Greek troops from the hollow belly of the horse snuck out and opened the city gates allowing their fellow troops to invade and capture Troy. This is similar to how users would accept a Trojan horse thinking it is something good, but once inside it unleashes malicious code which attacks your machine.

I hear a lot about spyware, what is it? How is it different?

Spyware is a Trojan horse distributed to your machine through pop-ups or spam messages that log information such as sites you visit, terms you search, or more extreme things like credit card numbers and passwords. Through the backdoor that Trojan's create, it sends this information to malicious users who can use it for annoying things like pop-ups and advertisements to very severe things like identity theft.

How do you know if your system is infected?

The only sure way of knowing is by running an antivirus or antispyware scan of your system with the most up-to-date definitions. However there are symptoms you can look for that may indicate your system is infected:

- Your system suddenly runs much slower
- Your system begins crashing or freezing abruptly
- You start receiving lots of pop-ups or weird error messages
- You see shortcuts to programs that you don't remember installing
- Your Internet Explorer settings change without your knowledge ie. Your home page is different.

What should I do if I think my system is infected?
If you think your system is infected the first thing to do is disconnect your network cable from the back of your machine or from the wall. This will ensure that if the infection is a Worm it will not be able to transfer to any other machine, and if it's a Trojan, no backdoors will be open to malicious users. Next you should contact a member of AHS Computing to take a further investigation into the problem.

If no support is available you should run an antivirus/antispyware scan on your machine using the most up-to-date definitions. Since your machine is not connected to the internet you will have to download the newest definitions from another machine and transfer them to the suspected machine via memory stick or CD. If an infection is found through a scan, let the software try to remove it (if it can find an infection usually it will be able to remove it). You can also search your findings in Google to see if there are any removal tools. Quite often Symantec http://www.symantec.com will have a useful tool available.

How can I prevent my system from being infected?

Make sure your Windows operating system is up to date. Be sure to install all high priority updates and any security updates in the software section from the Microsoft site http://windowsupdate.microsoft.com. These will update security features and fix vulnerabilities that can be exploited by malicious users and software.

Be sure to run an up-to-date and trusted antivirus program. Antivirus programs will continually update with new definitions as new viruses are found. This will be your best bet of preventing infections. Make sure to set your preferences so the program will auto-update and auto-protect. This way it will constantly check new programs being installed, files transferring from the internet, and e-mails being received or sent. You should only ever be running one antivirus program, running more than one could cause major problems.

With the uproar of spyware it is recommended to have a separate antispyware program; a lot of these can be downloaded for free via the web. Maintain your antispyware software the same as your antivirus software as they both operate similarly. Be sure to run scans periodically after updating in case the new definitions find files the old definitions missed.

Lastly, surf smart. When you're on the World Wide Web you are bombarded with links, files, advertising, and many other "free" services. Be suspicious of all content, whether it be from a web site you're visiting or a best friend forwarding you a program or joke. You could potentially be downloading an infected file. Keep in mind a simple Google search of any suspicious file or program name can reveal much useful information and possible prevention of an infection.