How Computer Viruses Work And How To Protect Your Computer

By: Matt Gundesen

Many people are afraid of tinkering with their computers because of the fear that they might inadvertently introduce a computer virus into the computer system.

Computer viruses have become the technological bogeyman that scares computer users all over the world. We have all heard of how dangerous computer viruses are and how it can damage your data. Of course, aided by the bloated images Hollywood movies paint with regards to computer viruses, a big majority now have this insane (but mostly unfounded) fears about it.

It is true that computer viruses are dangerous. Anyone who has lost vital information in their computers because of a computer virus will know how big a damage it can cause. But computer viruses are not these insidiously little pieces of code that could wreak havoc on the world. If you know what to do when you get a virus in your computer then you can definitely limit, if not totally stop, the damage it can cause.

But what is a computer virus? Well, it is a software with a small imprint that would usually attach itself on to a legitimate program or software. Every time this program is executed the virus is also executed and it tries to reproduce itself by attaching to other programs or it immediately starts affecting the computer. A computer virus and email virus basically have the same modus operandi, the difference though is that an email virus would attach itself to an email message or automatically send itself using the addresses in the address book in order to infect the people who receive the email.

A computer virus is usually embedded in a larger program, often a legitimate piece of software. The virus will be run when the legitimate software is executed. The computer virus would load itself into the memory of the computer and then it will seek out any programs where it can likely attach itself. When a likely program is found then the virus would modify the file in order to add the virus' code to the program. The virus would usually run before the actual legitimate program runs. In fact, the virus would usually perform the infection first before it commands the legitimate program to run. This process is so fast that no one would even notice that a virus was executed. With two programs now infected (the original program and the first infected program), the same process would be repeated whenever either program is launched worsening the level of infection.

After the infection phase, or even within the middle of the process of infection, the virus would usually start its attack on the system. The level of attack can range from silly actions like flashing messages on the screen to actually erasing sensitive data.

Fortunately, there are steps that you can do in order to protect your computer from viruses. Among the steps that you can take are:

* The simplest way to avoid a virus is to install a legitimate and effective antivirus program in your computer. The antivirus program is designed to look out for any kind of activity that could be seen as similar to a virus attack or infestation and it automatically stops it.

* You can opt to use a more secure operating system in your computer. For example, Unix is a secure operating system because the security features built into it prevents a virus from actually doing what it is programmed to do.

* Enable Macro Virus Protection in all of the Microsoft applications resident in your computer. Additionally, you should avoid running macros in a document unless you have a good idea of what these macros are going to do.

* Avoid using programs that you have downloaded on the internet especially when they come from dubious sources.

* Never open an email attachment that contains an executable file – these are files with the EXE, COM and VBS extensions.

About The Author:
Matt Gundesen is a certified expert in the field of antivirus software. To download Norton Antivirus as well as many other tools in the battle against computer viruses, please visit: http://www.antivirusdownload.com

Article Source: www.isnare.com