Title:
Removing Viruses From Your Computer

Word Count:
656

Summary:
One of the biggest threats that computer users are facing today is the
probability of a virus invasion. It is possible that your own PC might have been
infected with a virus that you have downloaded unknowingly from the internet, or
copied from other removable storage Medias like floppies or compact discs. While
some viruses are capable of doing extensive damage to your system, some may be
completely harmless but simply annoying. Whatever the problem is, it's always
best to t...

Keywords:
virus, viruses, computers, spyware, antivirus

Article Body:
One of the biggest threats that computer users are facing today is the
probability of a virus invasion. It is possible that your own PC might have been
infected with a virus that you have downloaded unknowingly from the internet, or
copied from other removable storage Medias like floppies or compact discs. While
some viruses are capable of doing extensive damage to your system, some may be
completely harmless but simply annoying. Whatever the problem is, it's always
best to try and remove these malicious applications (manually or using anti-
virus software) before they can cause any harm, and without deleting sensitive
and important files on your computer.

There is no one set of instructions you can follow to deal with a computer virus
because all viruses are different. There may be variants but each variant may
behave differently and independently. The steps mentioned here are general
remedies that may be used if ever your system is infected with a virus.

Active and inactive viruses:

A virus is usually located in a file, and it can be in one of these two states:
active and inactive. When the infected file has not been executed, the virus is
in an inactive state, and is not necessarily harmful. In such cases it is enough
to delete the file. When the infected file begins execution (when started by
user, by operating system, or by another program), the virus changes its state

from inactive to active, and begins to perform harmful activities on the system.

Identify the virus:

There is a webpage for every virus that has ever been identified by anti-virus companies, that explains how the virus executes itself, and usually how to remove it and disinfect the system. Here's one useful resource available for identifying viruses on your computer:

The Symantec Antivirus Research Center Online Encyclopedia or the McAfee Virus Information Search Center (http://www.symantec.com/avcenter/vinfodb.html): Try using these virus search engines to locate information about the virus on your computer. The Symantec search is capable of identifying viruses according to the symptom experienced by the system (such as the subject line of the email message that contained the virus or the error message the virus causes on the computer), but it's best if you know the name of the virus beforehand. Also remember that different computer viruses produce different "symptoms".

Using Anti-virus Software:

Once the virus has been identified, the best thing to do next is to run an anti-virus software, scan and clean the system. If you have anti-virus software on your computer (most users do), make sure the software is up-to-date.

Most anti-virus software run periodical, scheduled or manual scans on your computer according to preference, and if fully updated, will promptly identify any malicious activity or files on your system. You then have the options of deleting, quarantining or analyzing the virus depending on the type of antivirus you employ. If you're not too acquainted with the software, the only recommendation is to immediately delete the file, thereby eliminating any threat posed to your system's security.

Protect yourself from future threats:

Once you have removed the virus(es), it would be a good time to make sure your computer is protected from future threats by following these simple steps:

1.Make sure the anti-virus software on your computer is always up-to-date

2.Run real-time protection if your anti-virus has the feature (most anti-virus software do)

3.Do not download or run any suspicious or unrecognized email attachments or

file from the internet

4.Always run your anti-virus and scan any removable storage Medias before using them

Contact technical support:

If you can't solve the problem yourself, you should contact technical support immediately by phone or email. Every anti-virus company has one. They will be able to help and guide you. Do not take any drastic steps, like formatting any of your drives, if you don't have prior experience.