

## [How To Keep Your Computer Virus-free](#)

Somewhere out there in cyberspace are malicious vandals hard at work dreaming up new computer viruses. Eugene Kaspersky, (of Kaspersky Lab Virus Research), in a November 23, 2005 article posted in Security News, said, "The number of new viruses and Trojans is now increasing every day by a few hundred. (Our) virus lab receives between 200 and 300 new samples a day." That is Not a misprint. He said 200-300 per DAY!

The worst ones we hear about. The large majority are quiet and anonymous like termites, often doing much damage before they are detected. Like human viruses, their effects run the spectrum from mostly benign to potentially fatal to their unwilling and unwitting hosts. Also as in human viruses, there are two different approaches to dealing with them: Prevention and Cure.

Preventing virus infection begins with guarding the portals of contact. Do not open suspicious e-mails or attachments without scanning them first. Most anti-virus programs have a right-click option to scan a selected file for viruses, which makes scanning easy. Similarly, when you download software, eBooks or whatever, always save to a file, then scan the file before opening. If you bring in data or software by floppy disk, CD or other portable media, the same rule applies; scan it first!

A good firewall can help somewhat in keeping viruses at bay, but there are too many ways to hide them in regular data or software transfers for a firewall to catch them all. A firewall (like chicken soup for human flu) can help, but don't rely on that alone.

As Benjamin Franklin said, "An ounce of prevention is worth a pound of cure." However, sooner or later, some viruses are going to get through your defenses somehow, and you will need to turn to cures.

If you should get hit by a really bad virus, you could lose most of your files before you know that there is a problem! The first step to enable cures is to prepare well in advance, positioning and backing up your files for easy recovery. Set up your computer with a small hard drive (4-10giga) for your C: drive and a much larger hard drive for all your data. Use your C: drive for programs only. Keep copies of your software purchase receipts, registration and activation codes and setup info in a file on your data drive. You can always download them again, if you can give the seller your purchase info to show that you already bought.

Almost all virus infections will be in the program section of the C: drive, so scan it daily. This won't take much time since you have arranged for it to be relatively small. Then scan your (larger)data drive once or twice a month.

Hopefully the information presented so far has been applicable. You might also want to consider the following:

You should still back up your data files frequently. If you cannot backup everything, at least backup the crucial information that would be difficult or impossible to replace. CD and DVD burners are a good way to do this backup, as are removable hard drives.

Finally, you will need good anti-virus programs to go after the viruses and either quarantine or (preferably) destroy them. There are many anti-virus solutions being touted and hyped out there. Some are good, most are not. Here is how to find the good ones:

1. Look for programs that offer both active and passive protection. Active protection means that part of the program remains memory-resident, actively watching for potential incoming viruses. When they detect a virus they can sound an alarm and give you a series of options for dealing with it. Passive or on-demand protection will let you ask for a scan of specified areas when you want it, but it waits for you to ask.
2. Select your anti-virus software based on the recommendations of independent testing agencies. Checkmark (by westcoastlabs.org), AV-test.org and PC World magazine are among the most respected independent testers of anti-virus software. For ratings of anti-trojan software, check with Anti-trojan - Forum. Use more than one anti-virus and anti-trojan program. Very few detect all problems, but what one program misses, another may find and defeat.
3. Keep your anti-virus programs up to date. There is a running gun battle going on between virus writer-disseminators and virus catch-and-destroy experts. New viruses are found; new anti-virus program patches to find and destroy them are usually ready within hours or days. Until your software is updated, you are still vulnerable to the new viruses.

In addition to using anti-virus software on your personal computer, consider using an Internet Service Provider or e-mail service that includes server-side anti-virus and spam e-mail filtering as a third layer of protection.

In summary, be careful, get good software, run it often and update it frequently... and stay alert to new developments! This struggle between new viruses and better anti-virus software is ongoing, and developing rapidly.

Those who only know one or two facts about virus can be confused by misleading information. The best way to help those who are misled is to gently correct them with the truths you're learning here.

### About the Author

Michael Hehn writes articles about various topics.

Find out what he has to say about norton-anti at [Norton-Anti](#)

Source: <http://www.onlineearnings.net>