



Article published on March 8th 2012 | [Software](#)

Computer viruses do all sorts of things that you don't want. Some are harmless, doing little more than forwarding themselves to other people after embedding themselves in your system. Other, worse viruses steal or destroy your data: they can be so destructive, in fact, that you lose everything from your saved e-mails to all of the files your computer needs to start up.

Once you get a virus on your computer, it can take a lot of time and money to remove it. There's no guarantee that you'll recover all of your precious data, or that the virus won't forward itself to other people – like the names in your e-mail address book – for further destruction. It's far easier and better to prevent viruses from entering your system in the first place.

The first and best defense is competent anti-virus software. It might be hard to figure out which one is right for your system, as there are numerous programs available online and in computer stores. You can narrow down your choices by ignoring ineffective programs in favor of the most functional and the easiest to use.

You should look for a program that runs from the moment you start up your computer until you turn it off. It should scan all incoming files as they are being downloaded so that you won't inadvertently execute a virus that you receive in an e-mail attachment. You should also be able to download updates to the anti-virus definitions (files that help it stay on top of the latest viruses). When you find this, install it and make sure that it is always updated. It's useless to you and your computer if you don't update it regularly: once a week at the very, very least.

Tip: you can download trial versions of many anti-virus programs. Use trial versions to figure out which program works best for you so that you don't invest in a package that ends up being more difficult and less effective than its competitors. If you do this, make sure to purchase the software at the end of the trial period so that you have the most up-to-date coverage (and all of the full version's features).

The anti-virus software will protect your computer in most cases, but there are a few more things that you can and should do in addition to installing and using this software. These extra precautions won't cost a lot or take much of your time, so there's no good reason to neglect them. Think of it as making a small investment versus losing your computer for a few days to the repair center and paying the technicians their usual, hourly rates to eradicate the virus(es).

-Use a firewall. This is especially important if you're on a high-speed connection (i.e. anything but dial-up), as your system is more vulnerable. Firewalls are usually easy to install and configure, but you can always contact technical support or a computer expert if you have trouble. Even if you end up paying setup fees to have the software configured, you'll only have to pay it once – versus having to pay labor and other charges every time a virus finds its way into your computer.

The firewall also offers protection against hackers, spyware and other intrusions. A good firewall program will justify the cost of your investment when you think of all the attacks that it will catch and prevent.

-Know what you're downloading. Grab files from official sources when possible. For example: when Microsoft updates Windows, download from the official Microsoft site. This will reduce the likelihood of a virus invading your system by posing as an update or other important piece of software.

Tip: do the same for all of your other files. If you want video clips of your favorite band, visit their official Web site first. Sticking with sites that you trust will improve your chances of getting hassle-free, virus-free downloads.

-Use common sense. If you donâ€™t know what a file contains, donâ€™t open it until youâ€™ve scanned the antivirus program. Another safeguard is to confirm the fileâ€™s origins â€“ i.e. that your aunt attached it to an e-mail, or that your son downloaded it last night â€“ before you open it. Knowing its source doesnâ€™t guarantee that itâ€™s safe to open, but it helps track it down so that, if it does contain a virus, you can inform the sender that he or she has a problem.

You shouldnâ€™t have many virus problems if you follow these guidelines all the time. There might be a couple of intrusions here and there, but you can prepare for them. Back up all of your important data at least once a week and make sure that you own legal copies of all your favorite programs. If something goes wrong, youâ€™ll be back up and running with all of your data and programs â€“ instead of trying to rebuild everything youâ€™ve installed and created since you bought the computer.

Article Source:

<http://www.articleside.com/software-articles/keep-viruses-out-of-your-computer.htm> - [Article Side](#)

[ElleGacy](#) - About Author:

eLegacy provide range of services and solutions in digital marketing like small business a [Affordable Search Engine Optimization Services](#), a [SEO Doctor](#). Our comprehensive line of services encircles current market scenario itself - addressing important market needs from start-ups to further continuation.

Article Keywords:

Affordable Search Engine Optimization Services, SEO Doctor

You can find more [free articles](#) on [Article Side](#). Sign up today and share your knowledge to the community! It is completely FREE!