



Are All Anti-Virus Programs the Same ?

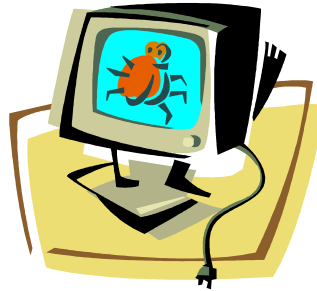
Steve Stryhalaleck

One of the most common things a computer technician works on is removing viruses. Over the years we have done quite a few articles on protecting your computer (and even your phone) from viruses. But it seems that people are still dumbfounded when they get an infection.

It used to be that keeping the definitions updated for your particular anti-virus program was good enough, but that no longer holds true. About once a year the anti-virus vendors release new versions of their anti-virus programs. It is important that the latest versions of these programs are installed and updated as they hold many upgrades and feature additions to help prevent virus infections.

The virus market is constantly changing and is very fluid. Because of this the virus writers are constantly coming up with new ways to infect your system and bypass your anti-virus program. It is also a common misconception that all infections are viruses. There are actually many types of infections such as malware, Trojans, adware, and worms to name just a few. Over time the virus writers have developed

new techniques, such as Trojans and malware to deploy other types of infections. Some infections are meant just to cause havoc, while others are meant to try to gain valuable information such as credit card numbers and account numbers stored on your computer.



Currently there are over 50 different anti-virus programs out on the market and they attempt to stop these new threats with their own methods, some being more successful than others. It is important to keep your anti-virus program up-to-date with the latest program version in addition to keeping the definition files up to date. Older programs are simply not able to easily detect these new threats.

Although there are many different programs on the market there are a few larger names

such as Norton, McAfee, Sophos, and Kaspersky. Since these providers have a larger portion of the market share the bad guys target these programs and write their viruses to work around them. That being said, generally speaking, when it comes to anti-virus, it is better to use the higher end, better known anti-virus programs, as opposed to the lesser known free versions.

What about Macs? They do not get viruses right? As we have covered in past articles Macs are vulnerable to getting infections as well. For the virus makers it is all about bang for your buck. They are trying to achieve the highest penetration that they can. Windows has about 88% of the market worldwide but Apple's share is currently at 10% and growing. As they grow in popularity they will be targeted more often, much like popular anti-virus programs and Windows are.

If you have questions about your current anti-virus protection and what the best solution is for you and your company you can contact us at support@mhconsults.com or via phone at 866-9MH-TECH (964-8324).

How to Keep Your PC Secure While Surfing the Net

Worms, Trojans, ad-ware, key loggers and viruses are all sorts of malicious code that will attack your computer. They can seriously harm your system and info while also hogging system resources or reducing PC performance and web bandwidth. Here are some steps to protect your PC from malicious software.

- 1. Update your operating system regularly.** Ensure that the operating system is updated with the most recent security patches.
- 2. Buy good anti-virus software This program must be able to scan e-mail and files as they're downloaded from the net to help prevent malicious software reaching your system.** It is also crucial to make sure that this anti-virus software is updated often.
- 3. Know your processes.** Knowing what's running on your computer will increase your capability to identify doubtless dangerous processes. In a PC, Press CTRL+ALT+DEL and get to grips with the processes running at any time. If you're doubtful what an individual process does, you can look it up for free online.
- 4. Install a firewall.** You should not forget to install firewall software or use the local Windows firewall. A good firewall impedes unauthorized use of, and access to, your computer from external sources (for example hackers or hijackers) while also giving you further defense against the more common Trojans and worms.
- 5. Invest in anti-spyware software.** In reality, many professionals go as far as suggesting installing two or three solutions since any single package won't be forceful enough to find all the entries and changes to your registry and other files. This may be going a little far, however, ad-ware is a dangerous threat and protecting yourself is important.
- 6. Backup your data.** Prevention is way better than cure. And, if you're a common computer user, you need to backup your info on a day-to-day basis.

-From www.wikihow.com



Online Back-up Solutions for Your Home Office

Chris Duffy

Have you ever had a hard drive crash? Many things cause hard drive failure, for example a virus can corrupt many files on your computer before you are even able to back them up. As hard drives get older they start to wear out from daily use and the heat they produce. Ask yourself what you would do if your hard drive were to crash and all your pictures, mp3's, and important documents were lost forever. Portable hard-drives are a good solution, but they have a higher failure rate, and can also be left behind accidentally in the case of a fire or other disaster.



For a small yearly fee you can have all of your files backed-up securely over the internet. Currently for home users, there are two major companies that offer back-up solutions: Carbonite and Back-Blaze. Both are great programs and back-up solutions for their low cost and offer the ability to access files stored on their servers from anywhere in the world. Both of these online backup solutions offer encryption in order to keep your data safe

and away from prying eyes. One thing to remember about these types of backups is that they are not a place to store extra data; if you delete a file from your computer these solutions will delete that file from their servers after about 30 days.

Back Blaze is a great backup solution that is highly rated by many in the IT field from big businesses to the small "mom and pop" shop. It also backs up portable media devices such as external hard drives and will backup multiple copies of documents in case you accidentally delete one or make an unwanted change. Another great feature of Back Blaze is that it is backed-up offsite in multiple servers in an area with a low occurrence of natural disasters in order to keep your data safe. Both Back Blaze and Carbonite have the ability to access data online from anywhere in the world. A notable feature of Back Blaze is that you can limit the amount of bandwidth you use at any give hour of the day. So let's say that you require a lot of bandwidth for work throughout the day, you can set Back Blaze to not do backups during the day, or to only use a little bit of your network, then after work hours you have Back Blaze utilize your full bandwidth. Back Blaze also has a month to month payment pro-

gram where Carbonite only has yearly.

Carbonite is also a great backup program that has been around for many years and has a bullet proof reputation. A few downsides to Carbonite are that you can't backup external media and that if you have more than 200 GBs of data (very uncommon) your back up speeds are reduced. Carbonite also lets you access your backed up data from most popular smart phones and access the files on these devices. Like Back Blaze, Carbonite offers a scheduling of when you can have your backup run. Carbonite does offer the ability to have all of your data sent to you on DVD or a flash drive for a premium.

Keep in mind that these online backup options are geared towards a home user or small home office. Whether you choose to go with Back Blaze or Carbonite you should rest easy knowing that all of your data is backed up safely and that it is accessible anywhere in the world at any time. If you have any questions about online backups or would like help in setting up an online backup that works for you please call M&H Consulting at 866-964-8324 or you can email us at [sup-port@mhconsults.com](mailto:support@mhconsults.com) and we will be happy to help.

TAKE \$\$\$CASH\$\$\$ FROM M&H CONSULTING

Refer a new Tech-For-A-Day client to M&H Consulting and mention this offer to us, and you will receive \$25 for each PC the new client has. Call for details.

