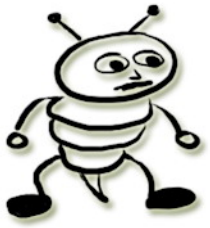
Clean PC

Removing viruses and MalWare from your computer



Many computer users have a false sense of being protected against viruses and spyware.

- Just running a virus scanner does not mean that your computer is clean.
- It takes a mix of the right software tools to keep your computer clean.
- Proper usage of software to keep your computer clean, is very important.

This report will help you on your way to keeping your computer clean.

What NOT to use ?

Symantec, Norton, McAffee

These are the big players in anti-virus software.

- Often they require you to buy a license, which has to be renewed regularly.
- They do not fully protect your computer. I have seen many computers that were full of viruses while using these virus scanners.
- They are a big drain on your computer resources and slow down your computer considerably. They usually consist of many parts that are installed in various places on your computer. Un-installing it can be an annoyance for unexperienced users.
- Many people who use these virus-scanners, are reluctant to remove it from their computer:
    - They paid for using the software, so they wrongly assume that it must be better than free virus-scanners.
    - If they want to uninstall it to try out some other virus-scanner, they are often unsure if they can get it re-installed later. So they stick to a policy of "not touching it".

Lesser-known anti-virus software

There are a lot of different anti-virus solutions. Many people want a free software, and end up downloading some relatively unknown software. Often it fixes only a small number of threats. But there is also a chance that it is infected software claiming to be an anti-virus software.

While being lesser-known does not necessarily mean that it is bad software, it is recommended to stick to software that has built a good reputation.

What to use for decent protection ?

Below is a list of some free software tools that do a very good job at cleaning your computer.

- Don't assume you are protected by other software, until you have tried these tools.
- Don't assume that the software listed below will guarantee your computer to be 100% clean. In experienced hands, they are very powerful tools. But many people have little knowledge about computers. Cleaning viruses can be a difficult task, even for experienced users.

1) HijackThis

http://free.antivirus.com/hijackthis/

* This is not a normal virus scanner. It is meant for unexperienced computer users to create a log file of their computer settings, which can then be analysed by an experienced computer user. Unless you really know what you are doing, don't fix anything that the scanner finds. Besides possible threats, it also shows results that are not a threat. And fixing those things could easily break software on your pc.

* There is a handy feature in HijackThis that allows you to check and edit your "hosts file". You don't really need HijackThis to do that, but unexperienced users often don't know where to find their hosts file. So this software makes it easier to find it:

- Click on "Open the misc tools section" in the main screen.
- Then click on "open hosts file manager" to see the hosts file on your computer.

The lines starting with # are just comments you can ignore.
Below the comments there should be only 1 line saying: 127.0.0.1 localhost

If there are more lines with different IP number, you are hijacked:

- Choose "open in notepad"
- Remove all lines, and only keep the 127.0.0.1 localhost
- Choose "Save" in notepad (not "Save as"). The edited hosts file will be saved over the hijacked hosts file.
- Check your hosts file again in HijackThis to make sure that it only shows the 127.0.0.1 localhost line.

If your hosts file is hijacked, your computer will be redirected to malicious sites while surfing to a website.

- So when you think you are downloading an anti-virus software, you might actually be downloading more viruses from malicious websites. That is why you should check your hosts file BEFORE installing new anti-virus software.
- If you already have anti-virus software on your computer, it might be downloading updates from a malicious site too if your hosts file is hijacked.

2) HouseCall

http://housecall.trendmicro.com

If not sure which version to download, download the 32-bit version.

This is one of the best virus-scanners you can find.

- It is always updated with the latest virus-definitions list.
- It does not interfere with other anti-virus software that might be running on your computer.
- One disadvantage is that this is an "on-demand scanner". That means it only scans your computer when you manually start the scanner. It does not offer permanent protection while you are using your computer.

Using it correctly:

- By default, HouseCall does a "quick scan" which only catches the most common threats. This is good when you are using HouseCall for the first time, to clean the most common infections as quickly as possible.
- Even if you did a quick scan, it is best to do a full scan. You can choose full scan in the settings below the scan button.
- When the scan is complete, you can choose to fix the infections it found. This should be done with caution because it is always possible that it will delete an infected file that is important for your Windows to run correctly.

3) SpyBot (Search and Destroy)

http://www.safer-networking.org/en/index.html

This is one of the best scanners against spyware, adware, and other malware.

- When installing SpyBot, choose to install "Resident". But do not install "TeaTimer", because it often causes problems.
- Before scanning, it is important that you update the list of spyware it recognizes (the "definitions list"). There is an update button in the SpyBot software. Update the definitions before every scan you do with SpyBot. New threats are added to the definitions list all the time.
- After scanning and fixing threats, also use the "immunize" button in SpyBot. It will protect your InternetExplorer (IE) against spyware. This is important, even if you never use IE.

4) AVG anti-virus

http://free.avg.com/ww-en/homepage

- I am not saying that this is the best virus-scanner that will protect you from all possible viruses. But it is a very decent scanner that does a good job. It does at least do an equally good job as any paid virus-scanner.
- This is a good "permanent" virus scanner. Permanent means that it keeps running while you are working on your computer, to help you avoid getting infected while surfing or downloading. Like any permanent virus-scanner, this can slow down your computer a bit. But it is not as heavy as some of the big anti-virus solutions, so it is acceptable to run it permanently on your computer.

Using it correctly:

- Disable other virus-scanners you might be running first. You should never run more than 1 permanent virus scanner at a time, because they would conflict with each other. Many people tell me that they don't want to uninstall their paid virus scanner. When you used the previous tools I recommend, you will see if your paid virus scanner is really keeping your computer clean. And if it's not keeping you clean, then you better get rid of it, no matter if it's paid for.
- Make sure to update the virus definitions list before scanning.
- Run a full scan with AVG.
- Clean up the infections it finds (but always with caution).

5) HijackThis Experts analysis

After having used the above software, your computer is probably clean. However there is always a chance that some difficult-to-clean virus is still hiding in your computer somewhere. This is where experts would use HijackThis again.

The HijackThis scan report shows software (both good and bad) that is installed on the computer in places that are a favorite target for viruses. For example:

- software that is loaded at boot-time (when your computer is starting)
- software that was downloaded from the internet (ActiveX, Java applets, ...)
- and more

It is not recommended to fix anything in the HijackThis scan results, unless you really know what you are doing. It is better to show your scan report to a friend who knows how to interpret the report. Or you might find help in one of the many virus-help forums where the more experienced computer users help the less-experienced to check their HijackThis scan result.

Many viruses try to hide themselves by using file names that make it look like a legitimate Windows software.

The following site keeps a database with more details about the software that HijackThis might find on your computer. It is organized in numbered groups, just like HijackThis displays it in the report.

http://www.systemlookup.com/lists.php

The basic idea is to check all the clsID numbers (the weird numbers between {curly brackets}), to check all the file names and the places where they are installed. Not always easy, not even for experts. But sometimes this more detailed look into your computer environment is required to clean the most difficult viruses.

Some more tips

Temporary Internet Files

While surfing, your browser saves temporary files to a "temporary folder". Where exactly it saves those files, depends your browser settings. Keep in mind that if you have several browsers installed on your computer, you often have several different temporary folders too.

These temporary internet files are a common place for viruses to hide. It is good to clean them regularly. But it is especially good to clean the temp folder(s) before scanning for viruses, because the folder can contain many thousands of files which makes a virus scan take a lot longer.

In InternetExplorer and FireFox, and most other browsers, you can often clean the temp folder from within the options or settings menu. The InternetExplorer Temp folder is usually the most vulnerable where viruses tend to hide.

Recycle Bin

On a well-managed computer, the Recycle Bin ("Trash Can") should generally be empty. Inexperienced computer users often use the Recycle Bin as a sort of backup folder. They keep removed files in the Recycle Bin with the thought that they might need it again later, and over time a whole lot of garbage can pile up in their Recycle Bin.

System Restore

Many people have a habit of creating a backup ("System Restore") of their Windows installation. This can easily backup viruses too ! And later when you restore the backup to your computer, you would be putting back those viruses.

As an experienced computer user, I do not use those automatic backups. But I'm not going to tell you that you can't use it.

However, if you do use System Restore:

- Make sure that your computer is clean before making a backup.
- Always do the backup manually. If you let Windows do it automatically at scheduled times, you don't really know what it's doing.
- Don't use SystemRestore as your first solution to fix problems with your computer. First use the appropriate anti-virus tools to try to fix the problem, or have an experienced person check out your problem. System Restore should only be used as a last resort. It can easily mess up your computer too.
- If your computer was infected, make sure to "Disable System Restore" on your computer. This will remove old (possibly infected) backups. Then you can re-enable it and make a clean backup.

Too much software

Many people install a lot software on their computer. Often times they stop using certain software at some point, without uninstalling it. If you don't use software actively, it is worth considering to un-install it. A virus-scan will finish more quickly if there are less files on your harddrives.

Very popular among internet marketers are those "browser toolbars" that some websites offer. While they are not necessarily bad, they are very often programmed badly so that they are an easy entry point for viruses and spyware. Again, if you don't really use it, uninstall it.

CheckDisk and Defrag

After cleaning viruses, it is usually a good idea to use CheckDisk and Defrag.

These are 2 tasks that are typical for Windows computers. They have nothing to do with cleaning up viruses, but are considered good maintenance to keep your harddisk optimized for good performance.

How to do this is outside the scope of this report. But you can find more info on google. For example if you use WindowsXP, you could google "WinXP defragmentation".

Checking your Windows logs

Log files are always a good help to keep an eye on things that might be going wrong on your computer. Unfortunately, most computer users don't even know that their computer keeps logs.

In WindowsXP and later, you will find these logs in ControlPanel, under "Administrative tools" in the EventViewer section.

The "Applications log" shows software that is having a problem. It might reveal problems like your virus scanner not being able to do its work correctly, because the anti-virus software was maybe not installed with the correct administrator access permissions. For a well-running computer, your applications log should be relatively clean. But I have seen many computers that have thousands of errors showing. Frequently recurring errors should be fixed to keep your computer running smoothly. Google can be of great help in understanding the sometimes vague error descriptions in the logs.

Checking your internet access

Being connected to the internet (or even a local home network), always comes with the risks of outsiders trying to abuse your computer. Getting your computer connected to the internet, makes you the "network administrator" for your computer or home network. Of course, most home users don't even know what that means, so it would be crazy to expect them to be good at it too.

"Netlimiter 2 monitor" is a software that can help you to get a better idea of what is happening on your network. It shows all software that accesses the internet from your computer, together with stats about how much traffic was sent or received by each software. Suspicious internet activity from your computer, can be detected by keeping an eye on these stats.

http://www.netlimiter.com/download.php

Why viruses are booming

- Being connected to the internet is the most common cause of computers getting infected with viruses these days. You can get infected by surfing to a malicious website, by simply opening an email, by downloading files, and many other reasons.
- Another major cause of viruses spreading like wildfire, is that so many people are starting to use computers and the internet every day. The majority of computer users does not have a decent background in how to use computers safely. They usually don't know how they get infected in the first place, and often unknowingly help spread the viruses even faster by performing risky tasks on their computer.

Internet marketers are a very vulnerable target for viruses:

- They are connected to the internet to perform their online business.
- Many of them are relatively unfamiliar with computers. Even if you have been internet marketing for several years, that does not necessarily mean that you fully understand all there is to know about computers and viruses.
- Since internet marketing is about making money online, it is of course a favorite target for the creators of viruses who hope to get in on the action and profit from your marketing efforts.
- Many people run websites. Hackers love to hack into their webspace or server, and perform illegal tasks while the webspace owner gets blamed because the abuse came from their webspace. (Running a website ... it's not for everybody !)

People who surf on Traffic Exchanges (TE) are an easy target:

They surf to hundreds or even thousands of different websites every day. Many of those websites are infected because the TE owner doesn't use a permanent virus scanner to avoid approving malicious sites on his TE. Both the TE owner, and the TE surfer, should use a permanent virus-scanner, and check their computer thoroughly on a regular basis. But often that does not happen. Many use no virus-scanner at all, others use a bad one or don't update their virus definitions before scanning.

Hoaxes

Also a big pest are those emails that go around. You have probably seen them:

"Warning, there is a new virus going around that is not detected by any anti-virus. Please forward this to all your friends before they get infected."

Usually it's complete nonsense. There is no "new, undetectable" virus. But forwarding the email to your friends, often contributes to spreading any other viruses you might have unknowingly on your computer.

Jokes with an after-taste

It's quite popular to email "funny stuff" to friends, like those funny cartoons or jokes. Very often they are infected files that are distributed as executable(.exe) files or PowerPoint(.ppt) files. And everybody who receives it, thinks it's so funny they really have to forward it to all their friends too.

While the joke might indeed be funny, you should think twice before forwarding that kind of attachments because you might be sending your friends more than you think.

Keep safe !
Valleyken
http://helpdesk.adboardz.com