5 basic steps to eradicate Spyware

Spyware causes pop-up ads, changes system settings, changes links to home pages, search pages, and especially reduces performance and destabilizes the system. Spyware is one of these

Spyware causes pop-up ads, changes system settings, changes links to home pages, search pages, and especially reduces performance and destabilizes the system. Spyware is one of the major and exhausting challenges for computer users and system administrators. How to safely and effectively destroy spyware and "rootworm extraction"?

What do you think about spyware removal is complicated?Too simple !Just download some antispyware and then everything is "in place".Indeed, to kill spyware, users need to download and use some effective antispyware, but not enough.To eliminate "root" spyware is not easy, follow these 5 basic steps, helping to eliminate spyware simply and quickly:

Step 1: Backup data

Before trying to remove spyware, you need to back up important data.Some spyware can make major changes to system settings and when removing them can cause errors, or affect the entire system.The best way is to use the software to backup the entire hard drive as programs Norton Ghost or Acronis True Image . At the very least, you should copy important files in the *My Documents folder* . Some programs like Spybot Search & Destroy also

perform some limited backup functions, but creating a backup manually is an important step that you should not ignore.

UseSystem Restoreof Windows XP, which allows the system to restore a stable state when something goes wrong.System Restore can help you get back to the backup point when the system is "clean" - not infected with spyware.

If you believe that spyware has been in your system for several weeks, chances are that the recovery points created by System Restore are also infected.Therefore, please remove all restore points that cause this suspicion.Some anti-virus and spyware software may detect infected recovery points, but most of these software cannot "clean up" spyware.

A best way to clean up all recovery points:

1. Right-click *My Computer*
2. Click *Properties* , and select the *System Restore* tab
3. Check " *Turn off System Restore on all drives" option* and click *Apply* .Please wait a few minutes for Windows to remove all restore points.
4. After you have finished deleting the system, go back to the dialog box and uncheck "Turn off System Restore on all drives".This allows restarting System Restore but does not have any backup points.
5. To make sure there is a good recovery in the future, you need to create a new recovery point.Go to Start-> Help and Support and select "Undo changes to your computer with System Restore.".At that time, System Restore will run and create a new restore point for you.

Step 2: Observe carefully

The fastest way to scan for spyware is to go to *Add / Remove Programs* . Why scan spyware to *Add / Remove Programs* ? Here are some reasons. First of all, *Add / Remove Programs* is a particularly important place to analyze Windows system problems, and software installed on computers. The list of software in *Add / Remove Programs* will tell you which software the computer is using and determine which programs need to be backed up.

Next, *Add / Remove Programs* also allows identifying peer-to-peer file sharing applications like LimeWire or Kazaa . Because these peer-to-peer apps allow sharing non-copyrighted software, music, movies, photos . and also a "nurturing" environment and distributing spyware. So, use *Add / Remove Programs* to remove peer-to-peer file sharing applications.Because it has no effect if the virus and spyware have been wiped out, the user continues to maintain "the source".

Finally, by carefully reviewing the list of *Add / Remove Programs* , you can find secretly installed programs, or during the installation of an application the adware is stealthily installed.

In the list of found programs, carefully remove suspicious software.The software below 99% are unwanted software for users, they often offer ads and change "strange behaviors" in the browser:

1. GAIN
2. Media Access
3. Media Gateway
4. My Web Search
5. MySearch

6. Search Assistant - My Search
7. Secure Delivery
8. Select CashBack
9. Surf Accuracy
10. The Best Offers
11. WebRebates
12. Web Savings from eBates
13. WhenU Save
14. YourSiteBar
15. Zango

When the above software has been removed, they will require a reboot.If only one of them requires a reboot, answer "No" until all has been removed from the Add / Remove list.

Google is also a useful tool to remove unwanted software from the list.Searching for names of strange software is also a good way to track information about unknown software.If you want to know which programs are running in the system, look at them in Task Manager (press **Ctrl + Shift + Esc** in Windows XP), and search in the database ofPC Pitstop's known software databaseguarantee programs..If you are not sure whether the software is spyware or not, please leave it there.You still have the opportunity to delete them in the following steps.

Step 3: Select spyware removal software

If the system is only infected with adware, *Add / Remove Programs* can be effective.But when the infection is more severe, it's best to use antispyware software.These software can completely remove infected files and protect the system from being infected again.

Before considering buying an expensive anti-spyware program, try out some free spyware removal utilities.Not "cheap of mine", the following free software is really powerful, and highly appreciated likeAd-Aware SE Personal,Spybot Search & Destroy,Microsoft Windows AntiSpyware.

Some top-of-the-line anti-spyware software like SpySweeper is cheap and the spyware removal rate is very high, which is also an attractive option.

If you want to use the versatile toolkit, integrate anti-spyware, viruses, firewalls . like Norton Internet Security 2006, MacAfee . are good and expensive toolset.

Note : Some antispyware software is very dangerous.Many of these software are "launched" on the Internet are often ineffective, and often they are advertised via Google.These software are "bad" to the point of not destroying any spyware and they themselves distribute spyware.Moreover, some other software use the tactics of "extorting" users, when they have downloaded and forced users to continue using and paying for their tools.

Step 4: Kill spyware

In general, antispyware software works according to the following basic principles.When loaded, these software will scan running processes, files and keys in the Registry to find unwanted programs and settings.After the file scan has been completed, they provide a report of what is found and you can choose to remove the spyware at this step.Users also have the option of removing all spyware immediately, or putting them in a quarantine repository in case they want to use it later.

However, do not really believe in these tools too much.A file or process identified as a spyware, but it is unlikely that it is a spyware.In fact, every spyware removal tool has different capabilities and standards for eliminating unwanted software.So, you should use 2 or more antispyware software as the best and most effective way.For example, neither Spybot nor Ad-Aware detected the 180Solution 'Zango spyware, but Microsoft Antispyware did.But in all 3 anti-spyware software, only Spybot is the only software that can turn off the anti-virus warning in Windows Security Center.

When the system has worked well, make sure to re-enable System Restore, and create a clean restore point.Very useful if you want to go back to a clean recovery point when the system is infected again.

Note about Cookies

Some spyware scans and filters out cookies that are reported as cookies.Often these cookies are used for advertising purposes of a particular Web site.These cookies monitor your Web surfing behavior and offer ads that are appropriate for your "gu".However, users will not benefit from these useless and annoying ads.So when it detects cookies of this type, it is best to let antispyware clean them.

Step 5: Solve difficulties with the Internet

Some spyware removal tools are still not completely removed, your defense system needs to be really powerful and updated regularly.Keep up to date with the latest updates from vendors.Most antispyware software supports automatic updating of the latest spyware samples and patches in software packages.

Next, update security information, especially spyware information, regularly.Leading antispyware, virus and tool vendors such as Symantec, McAfee, and Computer Associates give warning information about the biggest threats from their Web sites.

For help and methods to kill Spyware, some Internet forums are a great place to visit.The best 2 Web sites among them areSpyware WarriorandPC Pitstop.Before putting your problem on the forum, read the questions related to the problem you are looking for, most likely the answer is available to you.

Minh Phuc