

## ***My Secrets To Cleaning Malware From PCs***

[Warning! Before following the instructions in this document, you MUST read the disclaimer on the last page.]

### **ABOUT MALWARE:**

These instructions should be followed closely. Malware (viruses, trojans, worms, adware, & spyware) can often get on top of your anti-malware checker(s) and make them think everything is clean, when in fact it is not. The simple test of whether or not your PC is infected?... If it is very slow to respond to your clicks, then you are probably infected with something. Usually I find PCs with too many brands of “harmless” adware. When your PC gets one or two of these adware “helpers”, no problem. When it gets 6 or more, then you have a problem, because they fight each other for control of your PC. Once they get involved, their very presence allows VERY nasty viruses & trojans to get settled in. Thus the major slow-down. It is not unusual to find PCs with over 100 malware nasties infecting them! Especially on those PCs owned by users who don't keep their anti-virus software up-to-date.

### **MANUALLY APPLY UPDATES:**

In order to clean your PC when it is horribly whacked-out, you should first get a free copy of “Spybot Search & Destroy”, then update it MANUALLY. By manually, I mean don't use the program's built-in update feature. Many viruses are smart and can see you attempting to update the application. They can make your PC think it has updated Spybot (as well as your other anti-virus software), when in fact it has NOT. I've seen some malware that stopped the update process! Instead you should download the latest version of the program and also the latest update, then run both while disconnected from the Internet. That's how you fool smart viruses and malware. Follow the instructions below to get a free copy of Spybot. I've tried many free anti-malware products and found Spybot to be the best. [No, I don't work for the makers of Spybot!]

NOTE: if your PC is sooooo slow that it is painful to attempt to download stuff from the Internet, then you will need to use another un-infected computer to download the Spybot files and transfer them by CDR or USB Memory Stick to your infected PC.

### PREPARE TO INSTALL SPYBOT:

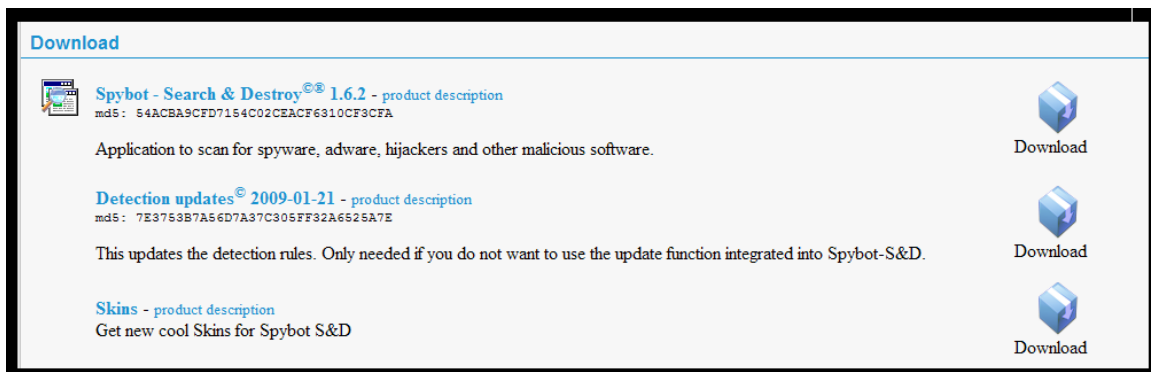
If you already have “Spybot – Search & Destroy” on your PC, you should first uninstall it by going to CONTROL PANEL | ADD REMOVE PROGRAMS and removing the application. Always uninstall it no matter how new it is. That’s how you wrestle it away from a nasty virus or trojan. If you aren’t sure you have it already, go to ADD REMOVE PROGRAMS anyway and see if it exists. Next, use Windows Explorer (right-click on the START button and select Explore) to browse to “C:\Program Files” and delete the “Spybot - Search & Destroy” directory, **if it exists**. Be careful not to delete anything else! Then close Windows Explorer. Always uninstall a program, before deleting its folders. Don’t try it the other way around, or it will get messy.

### DOWNLOADING THE LATEST VERSION:

Go to the following link, using Internet Explorer. Do not GOOGLE the Internet for Spybot or any other anti-malware product, or you will be sent to fakers who will infect you! The following link is the true home of Spybot...

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

When you get to that page, scroll down until you see the following section...



The screenshot shows a webpage titled "Download" with three items listed:

- Spybot - Search & Destroy<sup>®</sup> 1.6.2** - product description  
md5: 54ACBA9CFD7154C02CEACF6310CF3CFA  
Application to scan for spyware, adware, hijackers and other malicious software. **Download**
- Detection updates<sup>®</sup> 2009-01-21** - product description  
md5: 7E3753B7A56D7A37C305FF32A6525A7E  
This updates the detection rules. Only needed if you do not want to use the update function integrated into Spybot-S&D. **Download**
- Skins** - product description  
Get new cool Skins for Spybot S&D **Download**

Click the “Download” icon (on the right side) for “Spybot – Search & Destroy 1.6.2” (or later version). On the next page you will see several “Download here” buttons in a column to the right. Click the one associated with “Safer-Networking, Ltd. #1”. It should be approximately the 4<sup>th</sup> button down. In the next screen, click on the icon of a cube, found above the words “Download Spybot – Search & Destroy”. **Save** this file to a new empty folder you create, in a location and with a name of your choosing. Don’t forget where you put it and what you named the folder!

**Note: If you don’t know how to create and name a new folder during the SAVE process, package your PC up, sell it, and buy a Macintosh. You’re doomed. : P**

After the download is complete, go back to the screen shown above and click the “Download” icon for “Detection updates 2009-xx-xx”. [where xx is some month & day]. Save this file to the same location as the previous download.

### **INSTALLING SPYBOT:**

When download is complete, close Internet Explorer and all other applications. Disconnect your PC from your Internet cable or stop your wireless connection. While installing and cleaning, you don’t want the malware to “phone home”. Open Windows Explorer (right-click on the START button and select Explore). Browse to the folder you created in the steps above and install Spybot by double-clicking the file titled “SpybotSD162.exe”.

### **CONFIGURING SPYBOT:**

As you go through the installation process, accept the default settings, with the following exceptions:

- I suggest you de-select all the choices under “Select Components”, such as “Icons for starting blind user mode”, etc.
- In the “Select Start Menu Folder” I always check “Don’t create a Start Menu folder”, but you can leave it unchecked if you wish.
- In the “Select Additional Tasks” I uncheck all boxes except “Create desktop icons”. You may want some of the other options. It’s your choice.
- **IMPORTANT!** Uncheck the box for “Run SpybotSD.exe” in the “Completing the Spybot –Search & Destroy Setup Wizard” window. Then click the “Finish” button. [You don’t want to run the program yet.]

### **UPDATE SPYBOT:**

Next, go back to the folder you created and run the update by double-clicking on the “spybot\_includes.exe” file. Accept the default settings. When it’s done, you will see the word “Completed” above the green line. At that point, click the CLOSE button.

### **TURN OFF SCREEN SAVERS AND POWER OPTIONS:**

If you have any screen savers set to automatically turn on after several minutes, turn them off. Also stop any “hibernation” or other “power-down” settings found under CONTROL PANEL | POWER OPTIONS. Allowing your PC to go into Standby or Hibernation while a malware scan is performed can have negative results. This, by the way, is true if you ever do a “defrag” too.

**RUN SPYBOT:**

Close Windows Explorer and find the icon on your Windows Desktop for “Spybot – Search & Destroy”. Double-click it to start the program, then you should follow these important steps:

1. Ignore any warning popup messages regarding other programs
2. In the Spybot –S&D Wizard, DO NOT click the “Create registry backup” button. Instead, click the NEXT button.
3. DO NOT click the “Search for Updates” button. Do click the NEXT button.
4. DO Click the “Immunize this system” button and wait for it to finish. You’ll know it’s done when the green progress bar gets all the way to the right in the larger window behind the small Wizard window.
5. Click the “Start using the program” button.
6. Be sure you have selected the top button titled “Search & Destroy” found in the left-hand pane.
7. Click the “Check for problems” button and wait until it has finished scanning. While it’s scanning you can maximize the Spybot window by double-clicking the blue Title Bar at the top of its window. You should see a progress bar located at the bottom of the Spybot window. It may take 10, 20, or more minutes to finish, depending on the size of your hard drives.

**CLEAN UP THE NASTIES:**

If Spybot finds any malware, it will expect you to hit the “Fix selected problems” button, before going on. And make sure that all were selected with a green checkmark, before hitting that button. Attempt to fix everything. Occasionally it will say it can’t fix one or more problems until the PC starts up again after a shutdown. That’s fine. Re-boot as often as needed. **Always re-run Spybot until it no longer finds any problems.** I recommend re-booting your PC between runs of Spybot. Use FILE | EXIT to quit Spybot.

**USE A FREE ONLINE VIRUS CHECKER:**

Once you are satisfied that your PC is ‘clean’, I highly recommend you re-connect to the Internet and go to the following link and run “HouseCall”. It is a free online virus scanner from TrendMicro that may very well find more nasties on your PC, which Spybot could not find...

<http://us.trendmicro.com/us/home/>

When you get to the homepage at the above link, look for a link titled FREE TOOLS under the “For Home” section. Click it and it will take you to a page with a link to HouseCall. When you run HouseCall, it may require you load some ActiveX tool or Java helper. That’s okay. Do so and let HouseCall scan your system completely. I recommend you run HouseCall even though you may have an anti-virus application like Norton or McAfee already installed and “up-to-date”. That’s because viruses can fool your previously installed anti-virus software into thinking it is up-to-date, when it really isn’t. Because HouseCall is “external”, there is less likelihood it will be adversely affected by your PC’s malware.

### **UPDATE YOUR USUAL ANTI-VIRUS APPLICATION:**

After you have run HouseCall and think your PC is clean, update your installed anti-virus checker application over the Internet, as per its instructions. If your license has expired RENEW IT! You can’t live in a PC world without anti-virus software. Finally, run a complete scan of your PC with your usual anti-virus application.

### **FREE ANTI-VIRUS SOFTWARE:**

If you’re too cheap to buy a major brand of anti-virus software (Norton, McAfee, BitDefender, TrendMicro, Kaspersky, or AVG to name a few), then you can get a pretty good free one at...

<http://www.free-av.com/en/index.html>

### **ADDITIONAL ITEMS TO CHECK:**

I also like to clean out the contents of all my **TEMP** folders, found under **C:\** and **C:\Windows** or **C:\WinNT**. Also go to START | RUN and enter “%temp%” [without the quotes]. Then hit OK and delete all files and folders found there. Each user of your PC should do this. Don’t delete your TEMP folders, only what’s inside. Some things cannot be deleted. That’s okay, because they’re in use. Delete all but those items.

Also clean out your Recycle Bin found on your Windows Desktop. Finally, go into your Internet browser and delete all the temp files. In Internet Explorer, that’s found under the TOOLS | INTERNET OPTIONS menu item, under the GENERAL tab.

Also under TOOLS in Internet Explorer is “MANAGE ADD-ONS | ENABLE OR DISABLE ADD-ONS”. There, I like to disable most everything except Flash, Acrobat, and items associated with my anti-virus application. Helper type Tool Bars worry me. I suspect many of them “invite” adware products. By the way, when you’re in that screen, drop down the SHOW list and select “Add-ons that have been used by Internet Explorer” to see the real story!

**REALLY, REALLY BADLY INFECTED PCs:**

Occasionally, I run into a PC that is so screwed up, the above steps seem impossible to employ. That's when I get free copies of "HiJackThis" and "Process Explorer" to beat up on the nasties. Using these tools requires a bit more PC savvy than the average user has. However, if you are diligent, you can study the instructions and gain enough knowledge to break through the wall.

"**HiJackThis**" (now owned by TrendMicro) can be found at...

[http://www.trendsecure.com/portal/en-US/tools/security\\_tools/hijackthis](http://www.trendsecure.com/portal/en-US/tools/security_tools/hijackthis)

HiJackThis can be used to turn off the auto-starting feature of most all applications and processes that start at boot-up. Many are good and should be allowed to auto-start. Be sure you don't want it, before stopping one.

"**Process Explorer**" (now owned by Microsoft) can be found at...

<http://technet.microsoft.com/en-us/sysinternals/bb896653.aspx>

You can use Process Explorer to kill processes that you can't ordinarily stop within the Windows Task Manager. However, you need to know which processes might be malware and which are needed. Stop the wrong needed process and Windows will crash. Hey... you can always learn which is which by 'trial and error'. Or, if you want to know if a process is good or bad, try the "**Process Library**" at...

<http://www.liutilities.com/products/wintaskspro/processlibrary/>

**FINAL NOTE:**

If any anti-virus cleaner claims it can't clean a particular trojan or other malware, I recommend you attempt to find a specialized cleaner for it. Copy down the name of the nasty and then do search on the Internet. A good place to start is at the following site. I trust them to have **good tools** and be virus free...

<http://www.majorgeeks.com/>

**-- HAPPY HUNTING! --**

**Disclaimer:** The reader is wholly responsible for any unwanted or disastrous results that may occur while following the instructions in this document. Care should always be taken to backup critical data, before attempting to use any of these instructions. The author of this document offers the information found herein as suggestions and opinions. While the author attempts to assure the content to be accurate, it must be noted that as malware improves and the mentioned utilities change, the outcome of following the guidelines in this document may also change. Therefore, the author cannot be held responsible for the usage of this document. You've been warned!