

6/22/04

## Removing Spyware with SpyBot Search & Destroy

Version 1.3, for SpyBot 1.3

### OVERVIEW:

Spyware and Adware is a plague on the Internet. Sometimes it seems that half the Internet is composed of thieves and con men. Unfortunately, these people have software that helps them, too. Various websites have Spyware and Adware software that will either load automatically or will ask a user to load them on their machine- Which many users will do. Spyware will track where you go on the Internet, and reports this back to companies who may use it for any purpose they please. Adware takes over your Internet Browser software (such as Internet Explorer), and can change your Home Page, cause advertisements to pop up every time you click on a link, and may insert ads into web pages which never had them to begin with.

**FREE** donation-supported software is available to remove Ad-aware and Spyware. One of the first programs was Ad-aware, from <http://www.lavasoftusa.com>. Ad-aware did an excellent job, but has failed lately to stop some of the more complex Adware and Spyware software on the Internet. We are now recommending the product "SpyBot Search & Destroy" as the most effective software for resolving Spyware and Adware issues.

Note that SpyBot Search & Destroy, like Ad-aware is FREE. There are many commercial Spyware/Adware removing softwares; most of these have more in common with Spyware or Adware than they would like to admit! Disturbing and misleading marketing practices are common for these commercial products, using some of the same Adware techniques that they claim to prevent. We don't recommend ANY commercial software for this purpose. Much of this software treats a single symptom (such as "popup blocking", and may actually conceal the real problem- Adware on your machine that is CREATING these popups. SpyBot Search & Destroy has been doing an excellent job of resolving Spyware and Adware issues for the past year, and has evolved into the most potent single solution for this problem that we have ever found.

Note: Anti-virus products ignore Spyware and Adware. (We are not exactly sure why this is so.)

For additional info, see **Spyware and Adware page**;

<http://www.softprose.com/information/antivirus/spyware.shtml>

SpyBot's tutorial is at:

<http://www.safer-networking.org/index.php?page=tutorial>

Another tutorial is at:

<http://www.net-integration.net/reviews/spybot1.html>

### HOW OFTEN should I run SpyBot?

SpyBot S&D should be set to Update automatically every time it is run, to make certain that the detection patterns are the most recent. SpyBot S&D should be run every time you suspect that there may be a problem. If you want a schedule, about once every week should be adequate, although many users prefer to have it run once a day, at night, as a Scheduled Task.

### IS SPYBOT CLOSING RIGHT AFTER IT RUNS?

A WARNING from the Spybot website:

CoolWWWSearch.SmartKiller (v1 and v2) is a new, real ugly variant of CoolWWWSearch. When running, it will close every browser window you use to visit a large list of anti-spyware-sites, and even will close Spybot-S&D and some other anti-spyware applications as well.

So if your copy of Spybot-S&D (or the anti-spyware application of your choice) closes a few seconds after starting, or your browser closes whenever you try to visit an anti-spyware site, check our CWS.SmartKiller removal utility on this page:

CWS SmartKiller Utility: <http://www.safer-networking.org/minifiles.html>

Download Spybot Search & Destroy from:

<http://www.safer-networking.org/>

### On The Download Page:

The creators of SpyBot Search & Destroy need to eat. The software works, and performs a major function which they do not charge for; however they ask for donations on the download page. A link to PayPal makes this easy to do for people with a PayPal account. This donation is OPTIONAL; the program will work the same with or without a donation.

If you like the program, you may want to come back later and donate something.

There will be a number of Download options. Scroll down. Pick the first option- Download SpyBot Search & Destroy". (The version as of this writing is 1.2.)

### SELECT THE FIRST ITEM:



This will give you a page of Mirror Sites where you can download SpyBot Search & Destroy.

When you Download, you can Save to your computer or Run from this location. We suggest Saving the program to your computer, in a place where you can find it again if you want to give a copy to a friend. (We like the Desktop...) After the download, there may be a convenient OPEN button- Use this to run the installation.

### RUNNING SpyBot for the First Time:

#### Pick Your Language:

ENGLISH has a white flag with a red cross on it. (Left image below.) This is intended to represent the flag of the Bailiwick of Guernsey, an English-speaking island British crown dependency in Europe, located in the English Channel. Although a subject of the British Monarchy, Guernsey is not a member of either the United Kingdom or the European Union.

FROM: <http://www.dpcommission.gov.qg/About/about.pdf>



(FROM <http://www.plcmc.org/forkids/mow/continent.asp?continent=Europe>)

This flag is actually incorrect. Although reported in some popular sources as the Flag of the Bailiwick of Guernsey, the actual flag has superimposed on it a Yellow Cross of William the Conqueror: (See the Right image, above.)

See: <http://zhenghe.tripod.com/g/guernsey/flags.html>, and

#### From the CIA Fact Book -

<http://www.cia.gov/cia/publications/factbook/index.html>

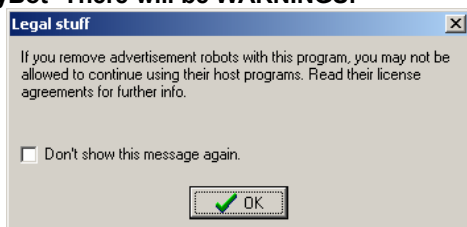
*The island of Guernsey and the other Channel Islands represent the last remnants of the medieval Dukedom of Normandy, which held sway in both France and England. The islands were the only British soil occupied by German troops in World War II.*

#### Create a Start Menu Item, Desktop Icon, or QuickLaunch Icon

These are all convenient options for launching SpyBot.

Choose other Defaults, such as Internet Explorer protection with "SDHelper".

#### Run SpyBot- There will be WARNINGS:



There will be a warning that "If you remove advertising robots with this program, you may not be allowed to continue using their host programs..." which makes sense- If you delete the Spyware or Adware part of some software, the software may stop working. Just say OK. (Think about it- If your spyware stops working, is this a terrible thing?)

#### Registry Update:

SpyBot may offer to Create a Registry Backup. This is a nice feature, only takes up a little disk space, and can be very useful if your registry gets damaged.

#### DO YOU HAVE Ad-aware Installed?

If so, you may have another warning that SpyBot may find Adware and Spyware that Ad-aware has already found and removed. (Ad-aware stores removed programs and files in a "quarantine folder"- they are not deleted.) Just Say OK.

After the installer is finished, look on your Desktop or in the Quick Launch toolbar for a shortcut to SpyBot-S&D.

When you run the program for the First Time, the SpyBot Wizard will appear. This can help you to configure the program. If your office has a Proxy Server (rare, but it does happen) than special adjustments may need to be made.

SpyBot S&D has an Easy and Advanced Mode. The Easy mode works fine, and the Advanced mode has additional options. You can run the program in either mode from the shortcuts installed in the Start Menu>Programs>SpyBot - Search & Destroy folder.

#### How do I STOP SpyBot S&D once it is running?

Spybot should respond to the Windows CLOSE command, Alt-F4. Just be sure the SpyBot window is ACTIVE (selected) when you do Alt-F4.

SpyBot S&D will show a "Stop Check" button. It make take a while for this button to work, but it should eventually respond.

OR:

Do Ctrl-Alt-Delete, and press the tab for "Processes." Look for SpybotSD. (To sort by name, click on the NAME column heading.) Select it, and hit "End Task". There will be a confirmation dialog. This always works, but is rather aggressive; try the other methods first.

#### SpyBot S&D Versions:

SpyBot periodically issues a new VERSION. **These new Versions cannot be updated, and your updating will stop.** To restore the Update function, you must download and install the most current version of the program.

We have found that it is SAFE to re-install the most current version without first removing the existing version. However, if you get instructions during the installation, you may need to first remove the previous version. To do this, go to the Start Menu>Settings>Control Panel>Add Remove Software and REMOVE SpyBot. Then run the most current installer to reinstall the program. You will need to reenter any customized settings. (See below.)

#### Command Line to run SpyBot S&D Automatically:

If SpyBot is installed with the Default Settings, you don't need to make any fancy changes to the settings to run the program automatically! Just use the below line in a Shortcut or in a Scheduled Task to run the program automatically whenever you want, with full automation:

```
"C:\Program Files\Spybot - Search & Destroy\SpybotSD.exe" /taskbarhide /autoupdate /autoimmunize /autocheck /autofix /autoclose
```

(NOTE that the below Settings changes for Automation>System Start are, however, STRONGLY recommended, and that the changes listed below are good for ALL installations of SpyBot S&D.)

**To change SpyBot S&D Behavior as a Default:**

Go to Start Menu>Programs>C:\Program Files\Spybot - Search & Destroy  
Run Spybot.

Go to the MODE menu at the top of the screen. Select "Advanced Mode".

(There will be a confirmation dialog, say "Yes".)

Go to Settings.

Select Settings (again, same name.)

This allows you to fully customize Spybot.

Make settings as follows: (See the sample Configuration.ini I list below for a quick copy and paste solution!)

Spybot Customization Guide:

**DISCLAIMER: These settings are merely a suggestion. ACCEPT THESE SUGGESTIONS AT YOUR OWN RISK!**

SpyBot may or may not make changes that damage your software systems. The below settings give SpyBot UNRESTRICTED control to make changes automatically to your system.

If you don't trust SpyBot, do NOT make these changes.

**Main Settings:**

UNCHECK "Display confirmation dialogs before making critical changes."

NOTE: This change gives SpyBot free rein to make any changes it wants!

UNCHECK "Display Compatibility Warnings"

**Automation>Program Start:**

CHECK:

Run checks on program start.

Fix all problems on program start.

Immunize on program start if program has been updated.

Don't ask for fixing confirmation. (AGAIN, permission to make automatic changes!)

(Spybot 1.2 had another thing here to Close if OK, but 1.3 does not have option.)

**Automation>System Start:**

CHECK:

(WANT TO RUN AT STARTUP? Many users are happy to let SpyBot run on startup; it will run in the background and should not interfere with other programs. Select "Automatically run program at system startup")

CHECK ITEMS BELOW to automate runs that happen on Startup

(Note: Often SpyBot will need to run a second time at startup to complete the cleanup chores.

These settings are IMPORTANT to have this run occur automatically and without user intervention to answer the dialogs.)

Run check on program start.

Fix all problems on program start.

Immunize on program start if program has been updated.

Close program if everything's O.K.

**Web Update**

CHECK:

Search the web for new versions at each program start.

THERE IS A CONFIRMATION DIALOG for this option, as it implies that you have either a 24/7 Internet connection OR that you are willing to accept a dial-up connection to the Internet each program start.

Download updated include files if available online. (This downloads the most recent updates each time the program is run- A REALLY REALLY GOOD IDEA.)

**Where is the SpyBot S&D Configuration Stored?**

Open the folder shown below

**Windows XP / 2000:**

C:\Documents and Settings\All Users\Application Data\Spybot - Search & Destroy

**Windows 98 / ME:**

C:\Windows\All Users\Application Data\Spybot - Search & Destroy

There is a file here called "Configuration.ini" that controls SpyBot's behavior at startup. This file can be edited directly (see the sample Configuration.ini file below) or can be edited by the SETTINGS control in the SpyBot S&D program.

IF you are going to edit this file manually, please be sure SpyBot S&D is NOT currently running.

BELOW IS A CONFIGURATION.INI SAMPLE for Version 1.3  
IF SpyBot S&D is not running, the below text can be copied and pasted into the Configuration.ini file described above, and can replace the current contents.  
PROVIDED AS-IS with no warranty, implied or otherwise.  
**RUN THIS CODE AT YOUR OWN RISK.**

#\*\*\*\*\* A CONFIG THAT RUNS SPYBOT \*\*\*\*\*  
#\*\*\* BUT DOES NOT RUN ON STARTUP- \*\*\*  
#\*\*\* replace contents of Configuration.ini with below \*\*\*

```
[Installation]
DesktopIcon=Advanced
QuickLaunch=Advanced
```

```
[Installation\StartmenuItem]
Easy=0
Advanced=0
```

```
[Main]
Legals=1
ShowDetails=1
AutoSave=1
CreateBackups=1
CreateTrackBackups=1
CreateSystemBackups=1
IgnoreIncludeFileError=1
Confirmation=0
Compatibility=0
Priority=Normal
RecoveryAged=1
EasyMode=1
CreateSystemRestorePointSpyware=1
CreateSystemRestorePointInternals=1
```

```
[Main\WaveAlert]
WaveAlertFile=0
```

```
[Automation\ProgramStart]
AutoCheck=1
AutoFix=1
RerunAfterFix=0
AutoImmunize=1
DontAsk=1
WaitStart=0
WaitPrograms=0
WaitMore=0
AutoClose=1
```

```
[Automation\SystemStart]
AutoRun=0
RunOnce=0
AutoCheck=1
AutoFix=1
WaitStart=0
WaitPrograms=0
WaitMore=0
AutoClose=1
```

```
[Automation\WebUpdate]
AutoCheck=1
AutoDownload=1
RemindUpdate=0
CheckBetas=0
CheckAllLanguages=0
CheckSkins=0
CheckSignatures=0
UseProxy=0
```

```
[Automation\WebUpdate\Proxy]
ProxyAddress=0
```

```
[Logfile]
WriteCheckLog=1
WriteFixLog=1
IncludeLogDetails=1
OverwriteLog=0
```

```
[Look]
BlindUser=0
Menu=MainMenu
DisplayHeader=1
FloatInfo=1
InfoPanelHighlight=0
```

```
[BugReport]
UseDefaultMailer=1
IncludeSysInfo=1
IncludeResults=1
IncludeActiveX=1
IncludeBHO=1
IncludeBrowserPages=1
IncludeProcessList=1
IncludeStartup=1
IncludeWinsockLSPs=1
IncludeClipboardText=0
IncludeClipboardImage=0
IncludeSpyFiles=0
CarbonCopy=1
```

```
[Expert]
ShredTracks=1
ShredRecovery=1
ShowResultsButtons=1
ShowRecoveryButtons=1
```

```
[Expert\Viewer]
HelperUseFiles=0
HelperUseFolders=0
HelperUseRegistry=0
```

```
[Filesets]
Spybot - Search & Destroy=1
Cookies.sbi=1
Dialer.sbi=1
Hijackers.sbi=1
Keyloggers.sbi=1
Malware.sbi=1
Security.sbi=1
Spybots.sbi=1
Temporary.sbi=1
Trojans.sbi=1
System Internals=0
Usage Tracking=0
Tracks.uti=0
LSP.sbi=1
Revision.sbi=1
```

```
[Durations]
Spybot - Search & Destroy=0.000198379624634981
Cookies.sbi=3.98148404201493E-6
Dialer.sbi=0.0014395486068679
Hijackers.sbi=0.000732916669221595
Keyloggers.sbi=6.58217613818124E-5
Malware.sbi=0.000139594907523133
Security.sbi=0
Spybots.sbi=0.00110307870636461
Temporary.sbi=1.85187673196197E-7
Trojans.sbi=0.000477754627354443
System Internals=1
Usage Tracking=1
Tracks.uti=1
LSP.sbi=1.85180397238582E-7
Revision.sbi=9.02778992895037E-7
```

```
[Main\AlertSounds]
AlertSpyFound=0
AlertNothingFound=0
```

```
[Automation]
SystemStart=NoAutomation
```

```
[Windows]
SplitterResults.Maximized=1
SplitterResults.RestorePos=232
SplitterStartup.Maximized=1
SplitterStartup.RestorePos=232
ListResults.Column0.Width=338
ListResults.Column1.Width=100
ListRecovery.Column0.Width=210
ListRecovery.Column1.Width=100
ListLanguages.Column0.Width=210
ListLanguages.Column1.Width=100
ListStartup.Column0.Width=210
ListStartup.Column1.Width=100
```

### 'SoftProse Sez' UPDATE EVERY TIME:

Note that Automatic Updating, configured under "Settings" (see above) is the BEST way to update SpyBot S&D. Below details the Manual update process.

After Spybot S&D is installed and running, go to UPDATE, and Search for Updates. Then Download Updates. Be prepared to do this every time you run the program, even if you run it several times in the same day- Some spyware changes on a daily basis, and these updates are vital. Press the button to SEARCH FOR UPDATES. Updates are shown in the list below.

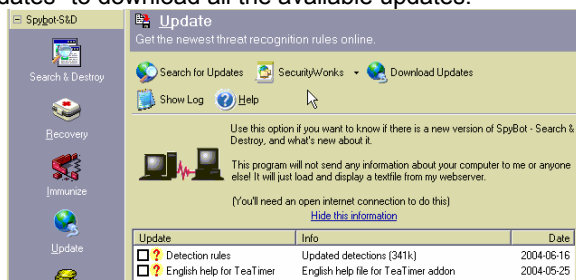
If there are NO UPDATES NEEDED, you will be told in the Status Bar in the bottom left corner of the screen.

Otherwise, updates will be shown. Make sure they are checked, and press the Download Updates button. The status of the download will be shown in the Status Bar in the bottom left corner of the screen.

IF the download succeeds, a Green Check will appear next to the updates. If it FAILS, there will be an Exclamation Mark. Check for Updates, and repeat the download process again until all updates show a Green Check. (Note: Major updates may have special instructions.)

Below shows the page with two updates available:

Check the boxes on each item, and press "Download Updates" to download all the available updates.



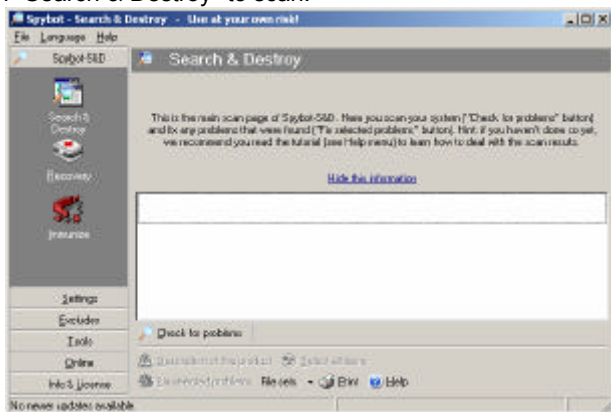
### DO THE UPDATES FAIL?

The biggest problem with Updates failing is a VERSION CHANGE. Changes in the program's VERSION will require a re-installation of SpyBot S&D to resume updates. (See above for more info.)

Some users are on networks which BLOCK these updates. This can be frustrating; there is a fix. Updates can be downloaded manually from the SpyBot website from their Download page, see the Download option for Updates- it is called the "Includes" file.

### Scanning your Computer:

AFTER LOADING THE MOST CURRENT UPDATES, click on "Search & Destroy" to scan.



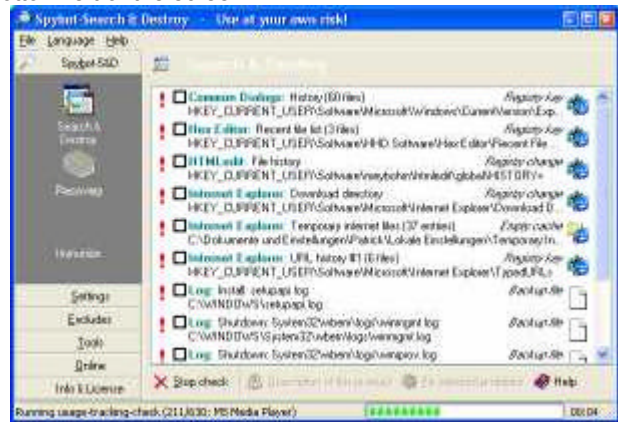
Below instructions were adapted from:

<http://www.safer-networking.org/index.php?page=tutorial>

Net-Integration also publishes a tutorial at:

<http://www.net-integration.net/reviews/spybot1.html>

Press the "Check for problems" button. The scan will run; the status of the scan will be shown in the Status Bar in the bottom left of the screen.

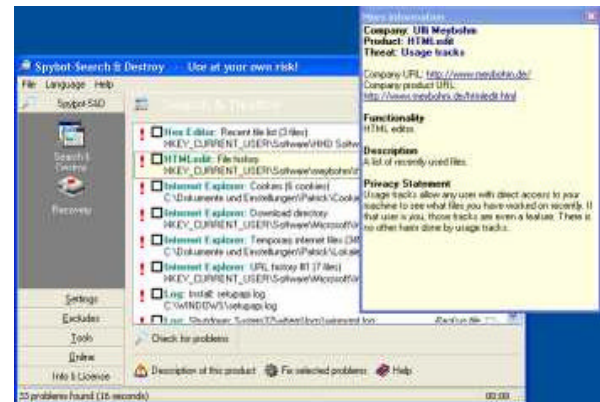


As problems are found, they will be shown in the list.

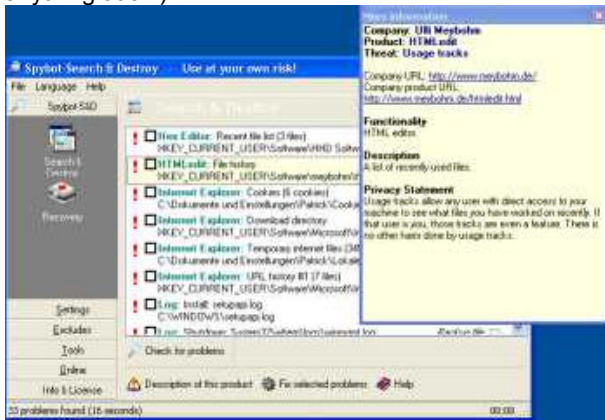
**RED** problems are significant, and are Automatically Checked.

**GREEN** problems are OPTIONAL, and are NOT automatically checked.

(See below how to install the secret "Select All" buttons.)



AFTER THE SCAN, you may want to review the items found. We suggest REMOVING EVERYTHING, especially items checked with Red. It is good, however, to see exactly what may be on your computer. SpyBot S&D even gives you custom information about each item, by clicking on the Green Links for each found item. (**Don't Panic** if the list is long. The program always finds SOMETHING if you use the Internet for anything at all.)



There is a "Fix Selected Problems" button visible. Press it to fix all the checked items.

Some items cannot be checked, because Spyware and Adware software is running and cannot be removed. If so, SpyBot will ask you if you want SpyBot to run when you next start your computer. Say YES, and SpyBot will run before the desktop loads when you next start your computer. After you reboot your computer, let SpyBot run again (Check for Problems), and then "Fix Selected Problems"- This should take care of everything.

**SpyBot S&D will kill some interesting things:**

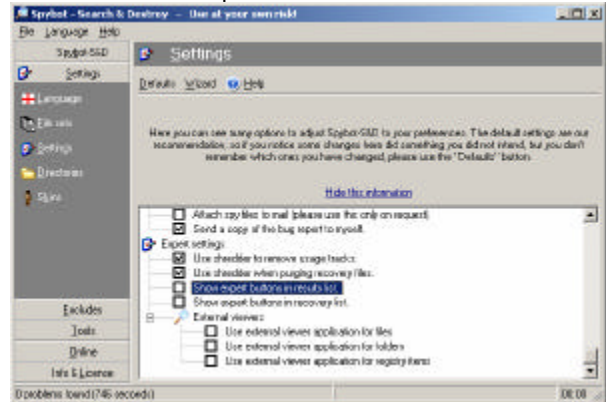
- 1) Lists of recently run documents may be cleared.
- 2) Bfast shopping cookies and software may be deleted.
- 3) Some "store toolbars" such as Amazon's Alexa may be removed.
- 4) "Gator" software such as Precision Time and Date Manager are Spyware, and will be removed.
- 5) Comet Cursor is removed; this is Spyware.

**Enable the "Secret Buttons" for Select All-**

Are you in Easy Mode? (You won't see "Settings" there.) Quit SpyBot if it is running.

Go to Start Menu>Programs>SpyBot -Search & Destroy>SpyBot S&D [advanced mode] and run the program from here.

Go to Settings. Click on "Settings" (a subtopic of Settings.) Under the topic "Expert Settings", check "Show expert buttons" and "Show export buttons".



**SUMMARY:**

Spyware and Adware are a blight on the Internet, preying on the user community. Anti-virus software should stop ignoring this problem, and should address it for what it is. Until this time, users should protect themselves by regularly using some of the excellent free tools available to scan and repair their machines.