

# SpyBot Tutorial

## Overview

This is a short tutorial to show you the first steps you have to do to remove Spyware and other crap from your computer, using Spybot-Search&Destroy.

## 1. Download

Obviously, the first thing you need to do is download Spybot-S&D from our [download page](#).

The download page first gives you a bit of donation information; if you like the program, I encourage you to come back later and donate something. But right now, you want to download. The downloads are on the same page, just scroll down a few lines, and you will see a table with three download locations. Clicking on one of them will lead you to a page offering the download. Each of these pages is a bit different, but you should be able to find the download link there without problems.



## 2. Installation

The file you have downloaded will be named *spybotsd13.exe* or similar. To install Spybot-S&D, all you have to do is run the file, and the installation program will start (if you have downloaded with Internet Explorer, the download dialog will give you the option to open the file directly). The installer will show you the license and ask you for the installation location. You can go with the default settings here and just click your way through the installer by using the *Next* button.



After the installation has finished, you will see a *Spybot - Search & Destroy* button on your desktop and in your start menu. Click on it to start Spybot-S&D the first time.

## 3. First run

The first time you start Spybot-S&D, it will display a *Wizard*, a small window helping you through the first steps. It gives you the possibility to add or remove the icons you have or haven't created during install, for example. Lets just say you want them and procede to the next page.

If you are using a proxy in Internet Explorer, Spybot-S&D will show you this proxy and a button will give you the opportunity



to use it for Spybot-S&D, too. If the text field is blank, you don't need to do it, but in most cases this will show an internet address, and you should import this proxy setting.

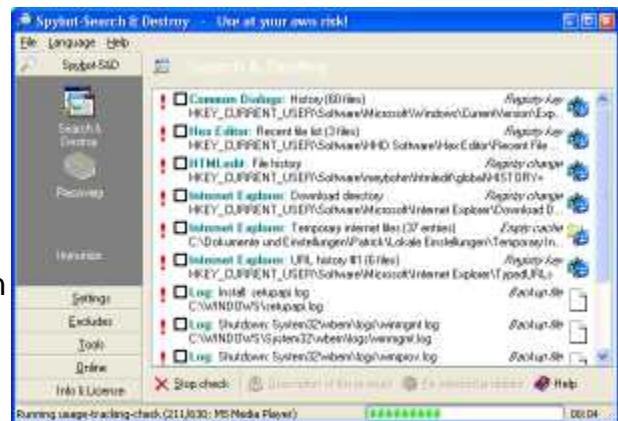
The next page deals with updates. It is very important to keep up-to-date. Using the two buttons this page offers will do the updates for you, if you want to do it at a later point, [read this](#).

The last page of the wizard will ask you to read the help file. The help file is always a good resource if you are unsure what to do, so please do at least read the first pages of it.

#### 4. Doing a scan

After the tutorial has finished, you may find yourself on the *Settings* or *Update* page. As the default settings are ok right now, and you've already updated, lets ignore them for now and do the first scan.

The left side of the program has a navigation bar that can lead you to all functions of the program. The first section there (the top-most button) is labeled *Spybot-S&D* and leads you to the main page. Right now, you will see only an empty list and a toolbar at the bottom. The first button in this toolbar is named *Check for problems* - that is the button you've got to press to start the scanning. Lean back and watch the scan progress.



#### 5. Interpreting the results

At this point, you could just jump to point 7, and remove the results. Instead we recommend that you first have a look at what all the stuff is that Spybot-S&D detected. The first thing you should know is to distinguish between the **red entries**, which represent [spyware](#) and similar threats, and the **green entries**, which are [usage tracks](#).

[\[link\]](#)



For the usage tracks (I hope you have followed that link to read what they are), removal is non-critical, but depends on your personal preferences.

Ignoring the usage tracks for now, you should have a look at the red entries which represent the real threats. While you of course can trust us that we have chosen the

targets using strict [criteria](#), you can check for yourself if you click on each product and read the product information that will be shown in a pop-up window.

## 6. Decision on exceptions

All problems displayed in **red** are regarded as **real threats** and should be dealt with. But while you read the product description, you may still decide to keep a threat, or just a [usage track](#). Maybe you don't want your list of most recently used Word documents removed? At this point you have three options.

- You could decide on ignoring all [usage tracks](#). In that case you could open the *File sets* page on the *Settings* section of the program, and disable the *Usage tracks* entries.
- Or if you want to just keep all tracks from a specific product, just [right-click a product in the results list](#).
- Finally, if you want to keep just one file, that is possible [the same way](#).

## 7. Removing the threats found

So now you should know about everything you've found. It's time to use the *Fix selected problems button*.

Once you start thinking about removing the usage tracks, too, you may think that ticking all the green entries is hard work. This is for a simple reason - to force you, the newbie - to look at the results. Once you know what you are dealing with, there is a hidden [Select all](#) button available for you.