

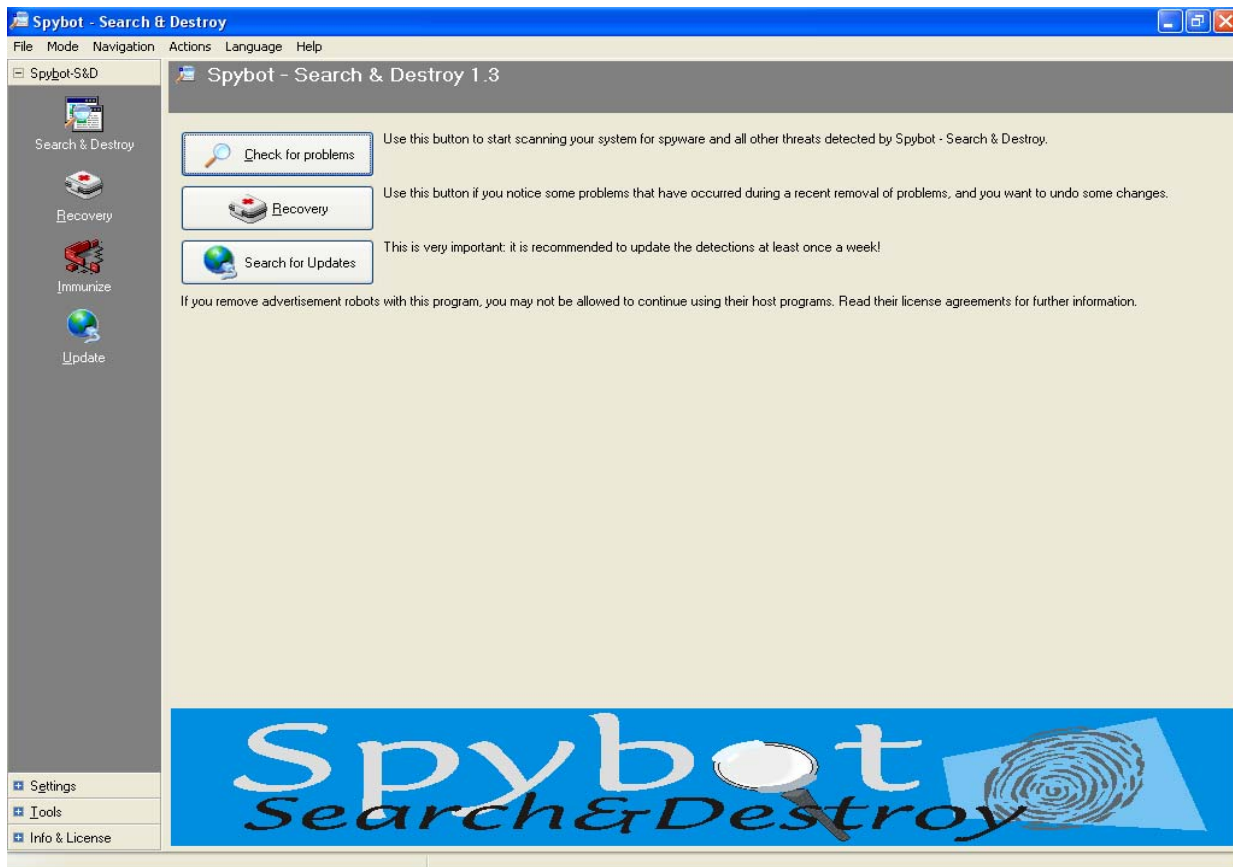
Instructions for Spybot - Search and Destroy

Step 1 – Initiate Program

Either Click on the Spybot Search and Destroy icon on your desktop, OR Click on Start/Program Files/Spybot-Search and Destroy/Spybot-Search and Destroy. The icon will look similar to the one shown below:

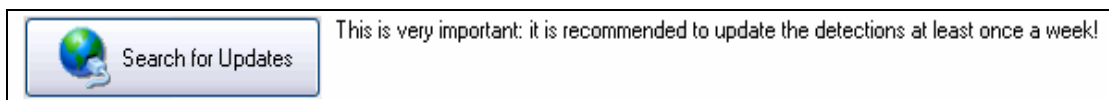


Spybot - Search & Destroy.Ink

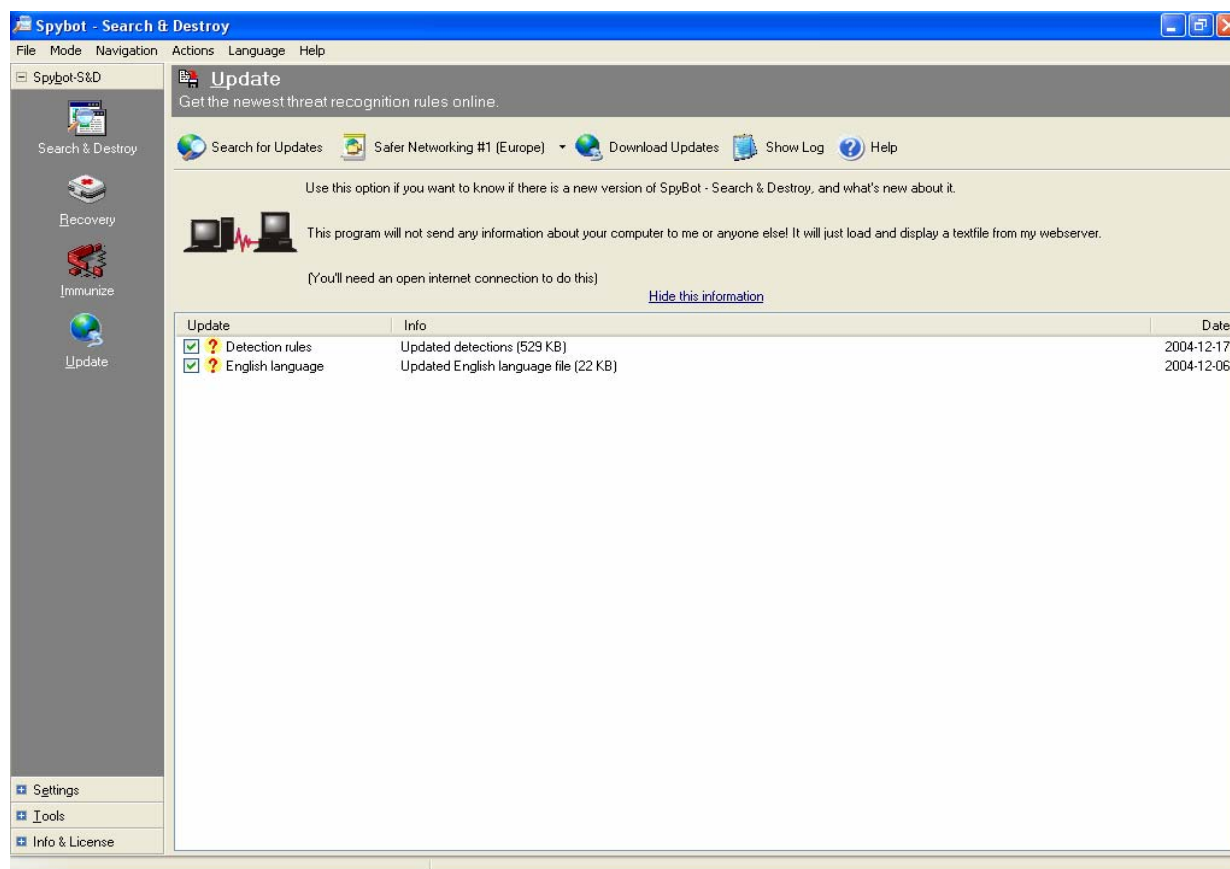


Step 2 – Check for Updates

Click the button “**Search for updates**” to make sure your Spybot program is up to date.



Once the search has completed, look to see if any items appear in the large white results window.



If downloads are available, click on each of the empty boxes so that green check marks appear as shown above. Verify the download location is “Spybot.Us by Rootboxen.net (USA)” and click the “**Download Updates**” button.

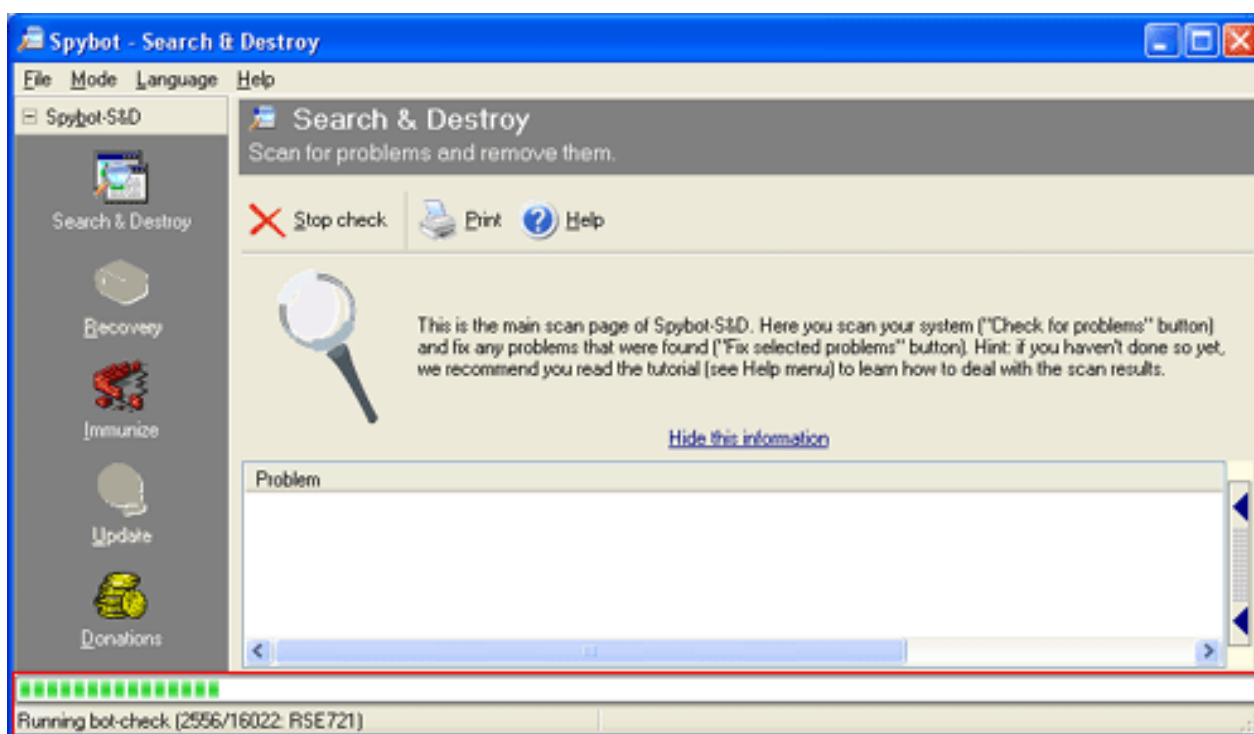


Step 3 – Scan for Spyware

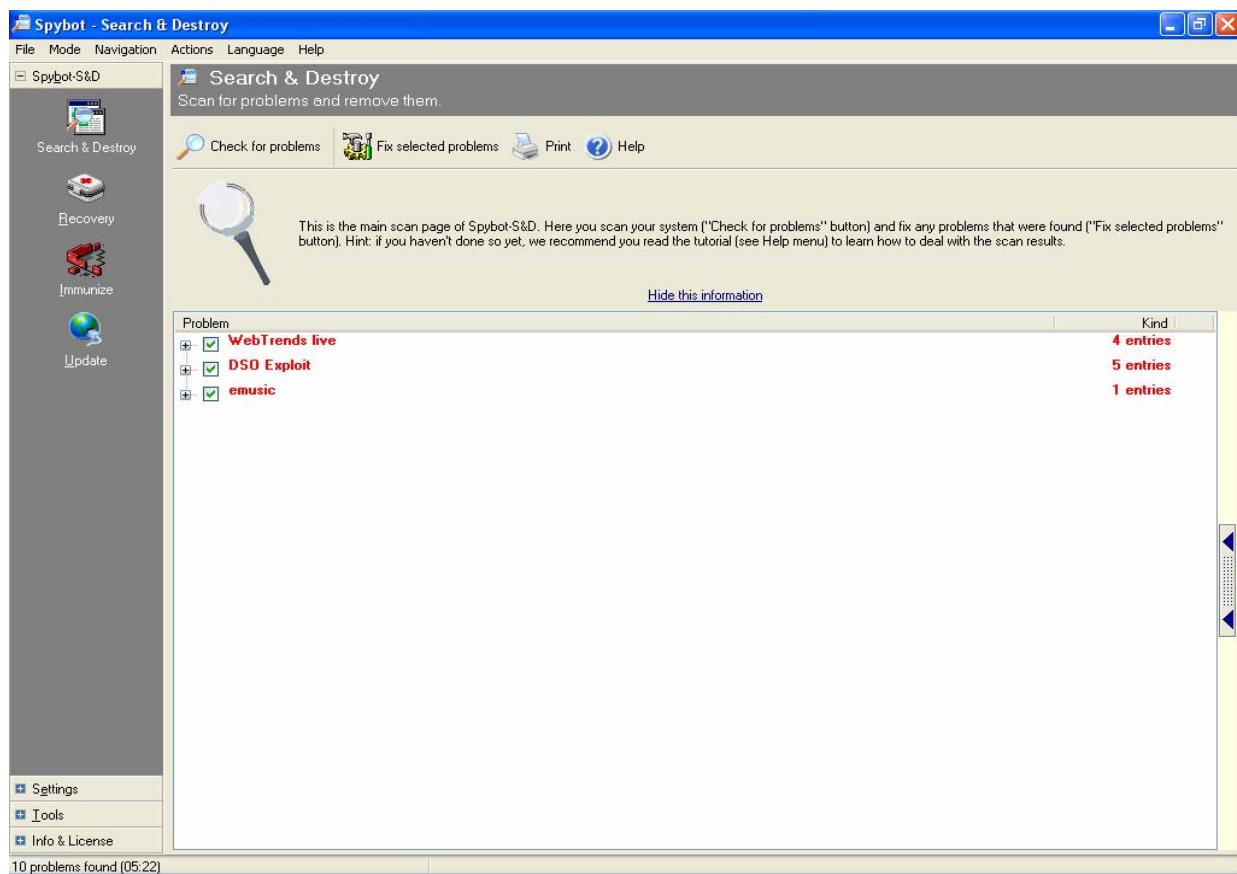
Once the updates have been downloaded, click the Search and Destroy button on the left panel. Then click on the button ‘Check for problems.’



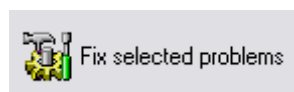
Spybot will scan your machine. This process will take approximately 30 minutes depending on your machine. If you have spyware, problems will appear in the white window.



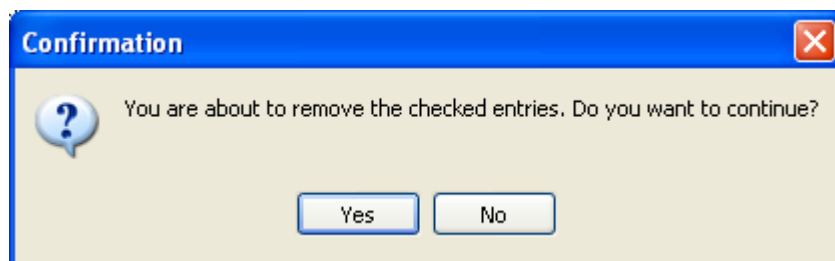
When Spybot is finished checking your machine, it will show you a list of the problems that it has identified.



Click on the button 'Fix selected problems'.

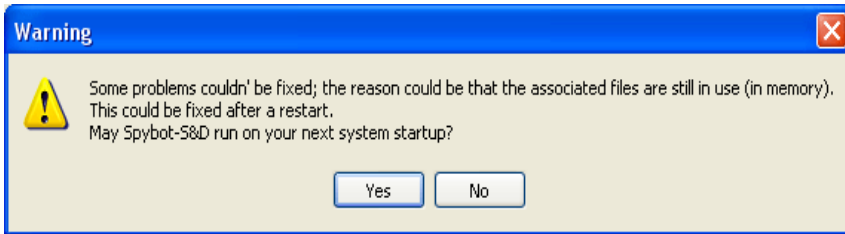


When it asks for confirmation, please click Yes.



Spybot will then delete the problems. When it is completed, spybot will replace the small green check (in a box) to a larger green check mark (with no box). You will also get confirmation that Spybot fixed the problems.

If Spybot can not delete all problems, it will ask you if Spybot can run again at boot time.



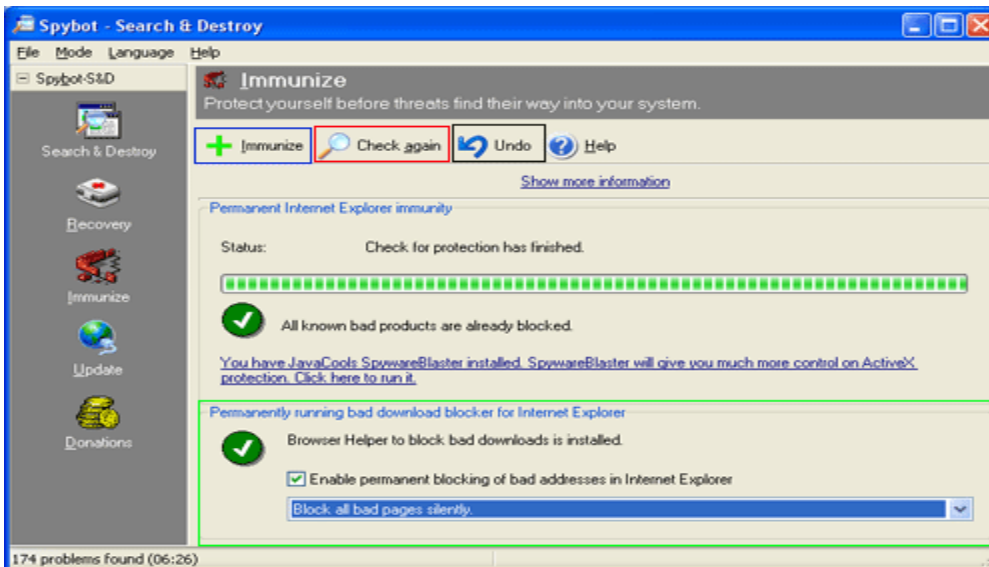
Please click 'Yes'. This will cause Spybot to run again automatically, the next time you re-start your PC.

Step 4 – Immunize your System

Spybot - S &D also has the ability to immunize your computer from downloading and running known malicious ActiveX controls or other programs from known malware sites.

Known malware sites are blocked by Spybot - S&D installing a Browser Helper Object (BHO) called SDHelper.dll into Internet Explorer. Spybot will also add its known list of malware sites into your Restricted Sites section of Internet Explorer which removes all permissions to run web programs from that particular site.

You can access the Immunize feature by clicking on the Immunize button on the left hand vertical toolbar. When you click on the Immunize button you will be presented with the screen shown below.



This screen allows you to immunize your Internet Explorer from malware sites and the malware itself. Click on the "**Immunize**" button, in the blue box shown above, to immunize your Internet Explorer.

If you would like to undo the immunization, you can click on the **Undo** button, in the black box to remove this protection.

If you would like to make sure Internet Explorer has all known malware immunized, you can click on the "**Check Again**" button, in the red box. Spybot - S&D will then immunize any missing malware it has in its database. You should do this occasionally to make sure you have the latest protection.

The section, designated by the green box that is titled Permanently running bad download blocker for Internet Explorer is very important. By putting a checkmark in the "**Enable permanent blocking of bad addresses in Internet Explorer**", Spybot - S&D will stop you from downloading any programs from known malware sites. This feature allows you to specify how Spybot - S&D should react when you visit a malware site and attempt to download something. These options are discussed below:

Block all bad pages silently - Spybot - S&D will block silently with no notification to the user.

Display dialog when blocking - Spybot - S&D will notify you when it is blocking something.

Ask for blocking confirmation - Spybot - S&D will prompt you for confirmation as to whether or not the particular program or script should be blocked.