



If you have not installed Spybot, start with Step 1. If you have Spybot 1.3 installed, proceed to Step 4.

1. Download

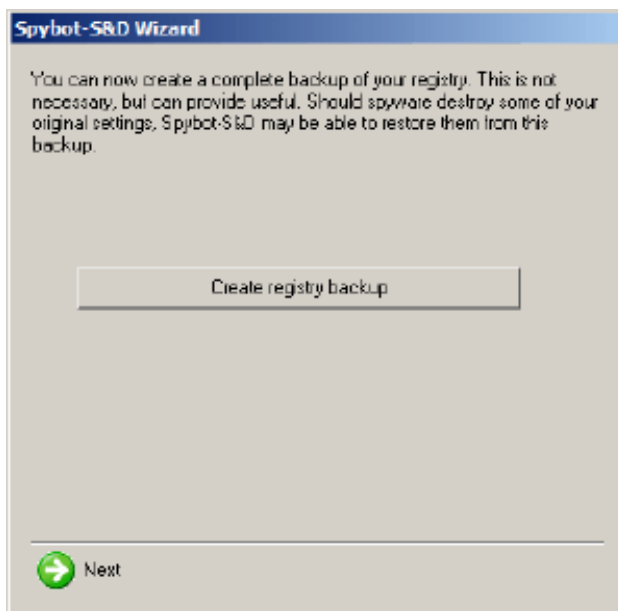
The first thing you need to do is download Spybot-S&D from our district website, <http://smokymtn.tennessee.edu/downloads/spybot13.exe> . Save this file to your desktop.

2. Installation

The file you have downloaded will be named spybot.exe. To install Spybot-S&D, all you have to do is run the file, and the installation program will start. 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



When you run for the first time, you will see the Spybot - S&D Wizard.

The first Screen will create a backup of your system registry. Click the Create Backup Button. When it completes, click Next.

The next screen will search for updates and allow you to download any that are available. Click the Search for Updates button. If any updates are found, then click the Download All Available Updates button. When complete click Next.

The third screen will install Immunizations for your system to help prevent the return of spyware. Click the Immunize This System button. When complete click Next.

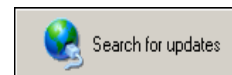
The last screen will allow you to read the Tutorial, Help files, or Start Using the Program. Click the Start Using the Program button. This will take you to the main Spybot screen. You may now skip to step 6 and begin a scan of your system for spyware.

4. Starting the program



Start with downloading any updates. It is very important to keep up-to-date. Click the Search for Updates Button.

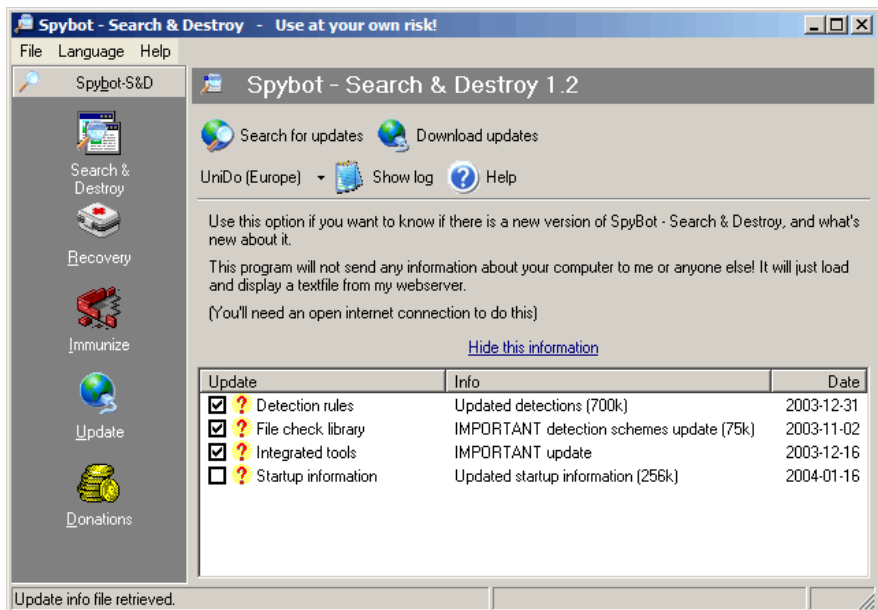
Start with downloading any updates. It is very important to keep up-to-date. Click the Search for Updates Button.



This page shows the current updates that are available. Near the top center of the page you will see a drop down button



This is the location that contains the update. Click the down arrow and you will see a list of other sites. Click one of the sites marked (USA) and then click

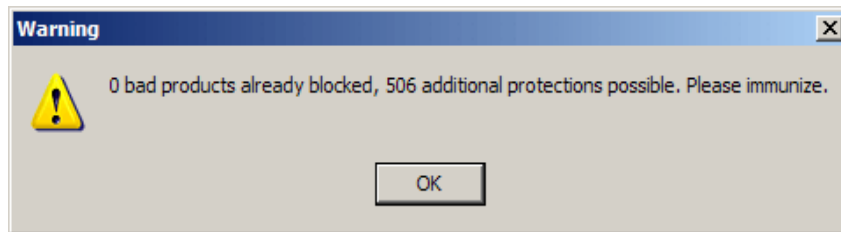


5. Immunizing

When all updates have finished, the program will probably shut down and restart itself. Once it has restarted, click the Immunize button in the Left side panel.



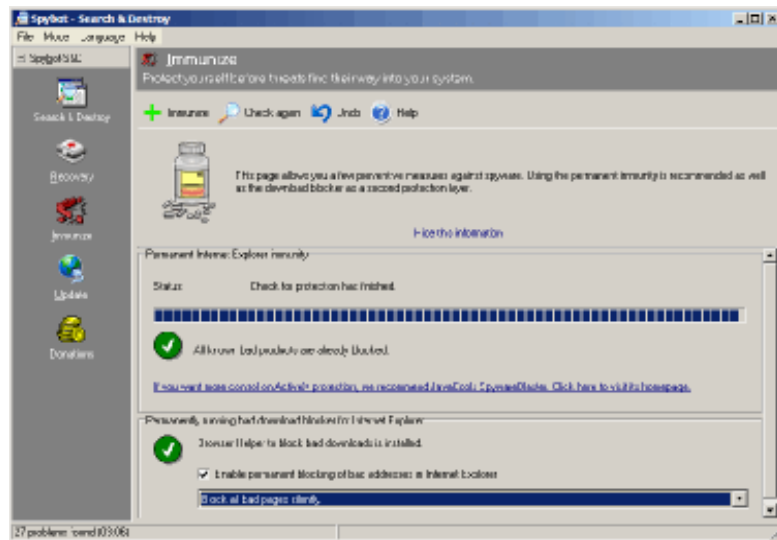
You will get a message like the following. Click OK.



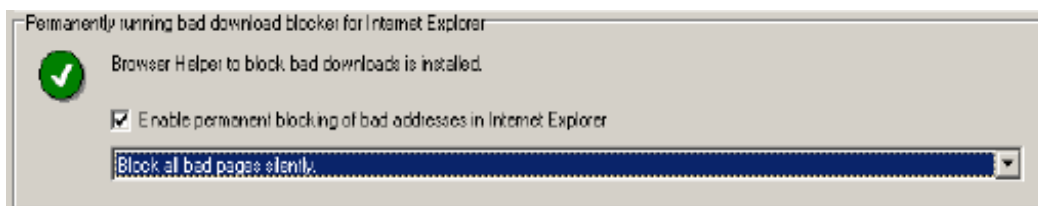
You will now be at the Immunize Screen. Click the Immunize button.



This will install the protective code. Click OK on the message screen.

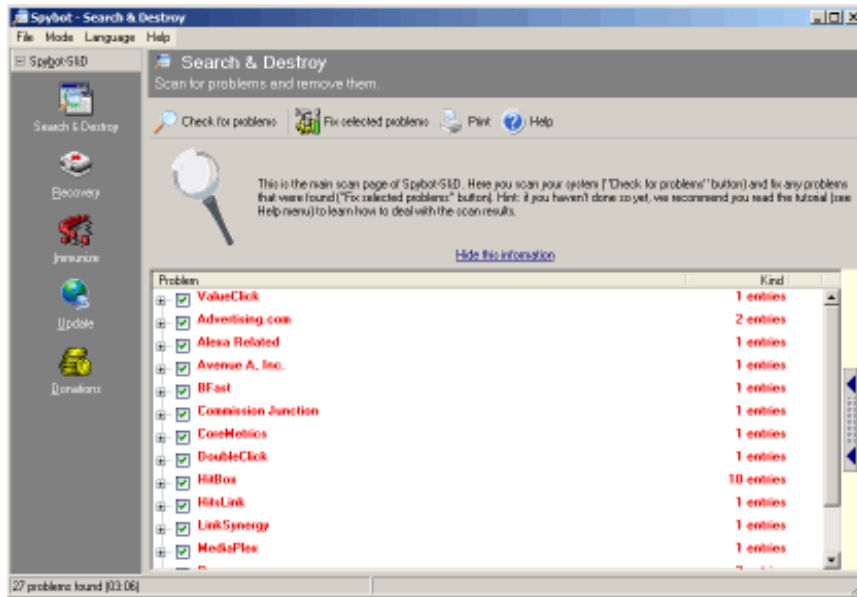
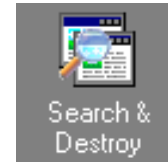


Scroll down using the scroll bar on the right side of the screen. Make sure to check the Enable permanent block of bad addresses in Internet Explorer checkbox and select from the drop down list Block all bad pages silently.



6. Doing a scan

Click the Search & Destroy button in the left side panel of the program.



You will now see the main Search & Destroy Screen. Initially, you will see only an empty list and a toolbar at the top. Click Check for Problems in the toolbar to start scanning.



Lean back and watch the scan progress. Depending on the speed of your computer, this can take several minutes.

7. Interpreting the results

At this point, 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.

For the usage tracks, removal is non-critical, but depends on your personal preferences.

8. 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? I normally put a check in every box.

9. Removing the threats found

It's time to click the Fix selected problems button.



When the program has completed fixing the problems it can be closed. If you get a message stating that some problems can not be fixed until Window is restarted, follow the prompts and it will automatically restart and run again to finish the process.

This program should be run monthly, more often if you are experiencing problems.

Created by: Cam Philbeck, Senior IT Technologist II
University of Tennessee Extension