

## **STEPS TO SPYWARE REPAIR:**

If you follow these easy steps, repairing spyware problems on your Windows PC will be certainly possible. We are going to download three packages first, install them, run them for updates, go to safe mode and run them for repair.

### **Follow these easy steps (the first time only):**

- 1) Download Firefox by going to MOZILLA.COM
- 2) Use Firefox and set up a folder on the desktop to save all downloads called DOWNLOADS
- 3) Using Firefox, go to download.com
- 4) Download ADAWARE, SPYBOT, SPYWAREBLASTER
- 5) Install ADAWARE. close it without running the program afterwards
- 6) Install SPYBOT, close it without running the program afterwards
- 7) Install SPYWAREBLASTER and run (this is the only program that you do not need to run in Safe mode)
- 8) Run ADAWARE for updates only
- 9) Run SPYBOT for updates only
- 10) Go to SAFE MODE
- 11) Run ADAWARE for removal
- 12) Run SPYBOT for removal

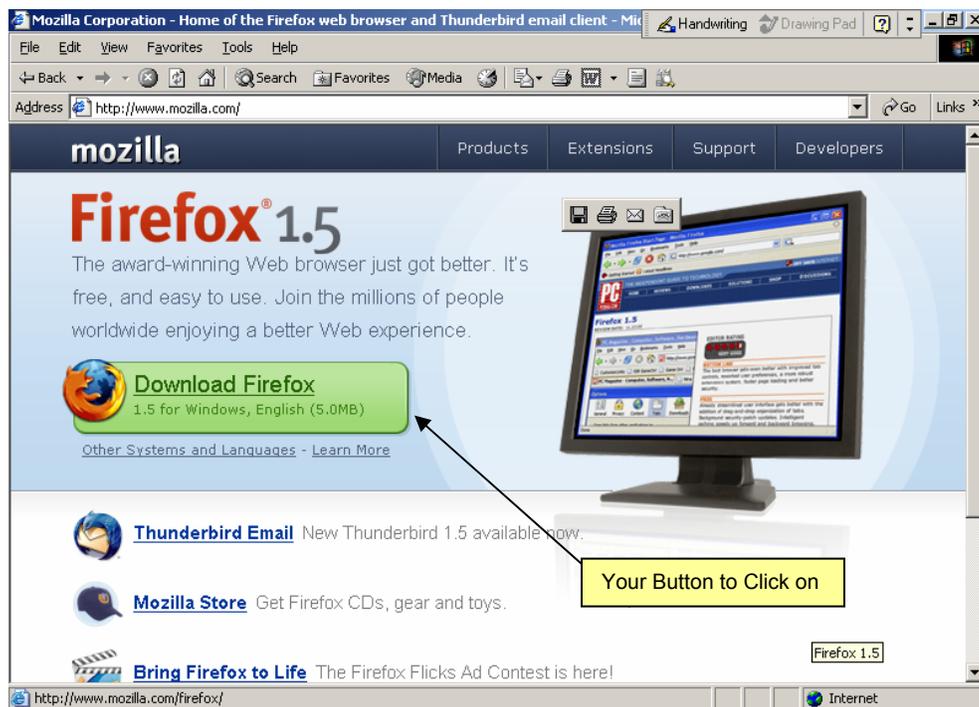
Now, once you have everything installed and you did this once, follow this procedure daily, weekly, bi-weekly, etc..

- 1) Run SPYWAREBLASTER in "normal" Mode
  - 2) Run Ad-aware for updates only (in normal mode)
  - 3) Run Spybot for updates only (in normal mode)
  - 4) Go to Safe mode
  - 5) Run Adaware
  - 6) Run Spybot
- (P.S.) you can run Spywareblaster in Safe mode also if you really want to. It doesn't hurt anything.

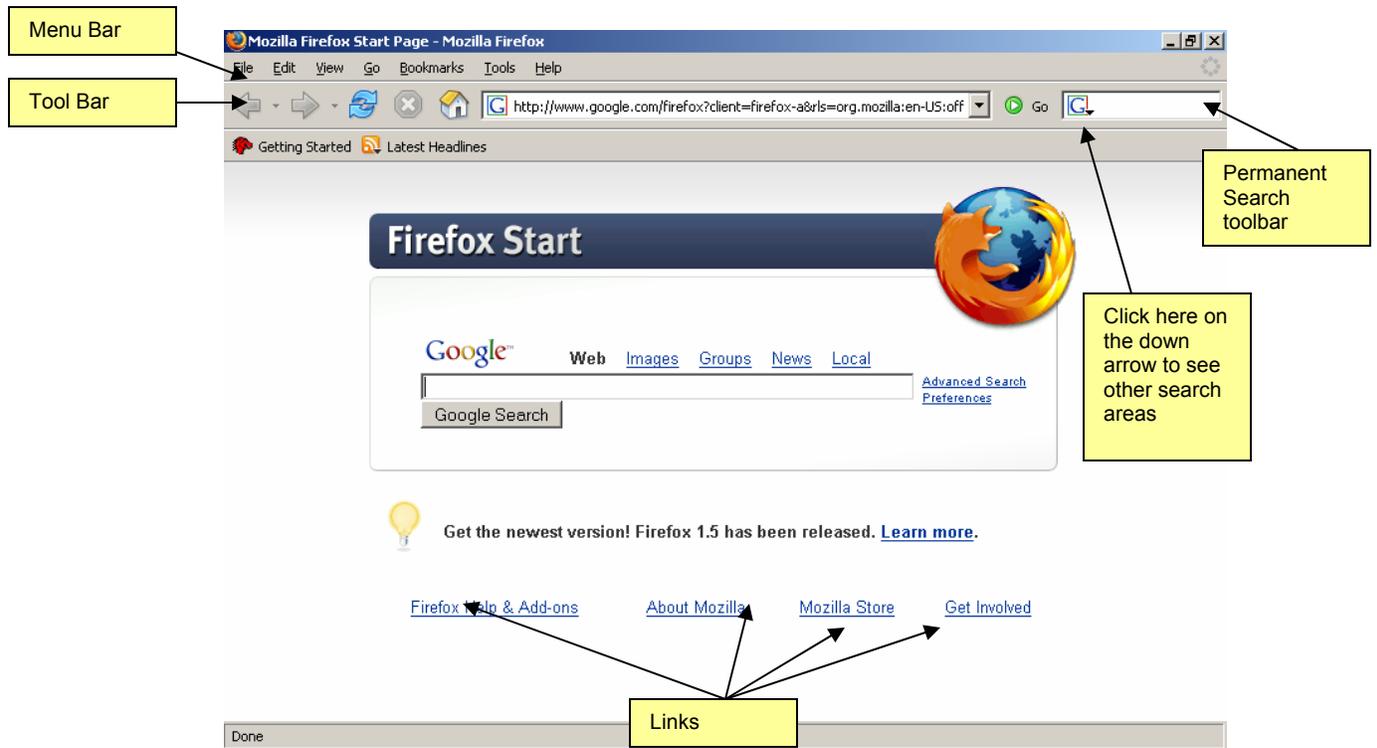
## DOWNLOAD FIREFOX

The first thing that you want to do is stop is stop using IE (if you can). So

- 1) Using Internet Explorer (for the last time maybe)
  - a) Type MOZILLA.COM in the address bar of your web browser. We are going here because the Mozilla Foundation is the maker of FIREFOX, your new web-browser
  - b) Click on the BIG GREEN download button for FIREFOX
  - c) Click on RUN and RUN again
  - d) Watch the percentage's slip away
  - e) Click on NEXT on the FIREFOX SETUP SCREEN
  - f) Click on ACCEPT and NEXT
  - g) Click on STANDARD and then NEXT
  - h) On the SUMMARY SCREEN, click on NEXT
  - i) Keep LAUNCH MOZILLA FIREFOX NOW checked
  - j) Click on FINISH
  - k) On the IMPORT WIZARD screen, click on NEXT
  - l) On the FIEFOX HOME PAGE SELECTION SCREEN, click on NEXT
  - m) Click on FINISH / YES
  - n) Now close down IE



# FIREFOX – PARTS OF THE SCREEN

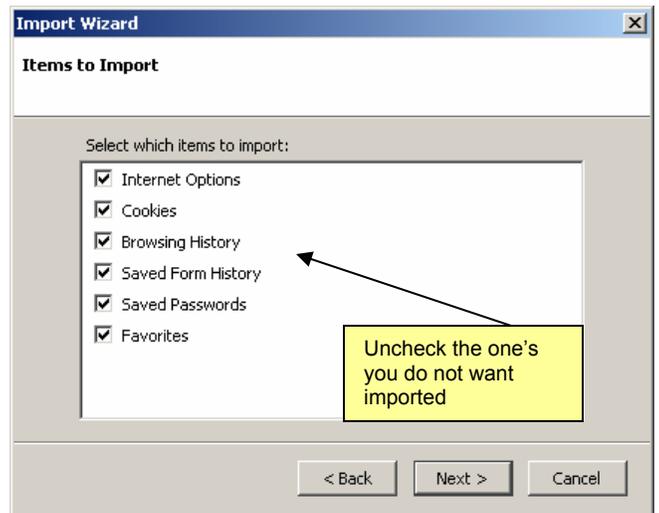
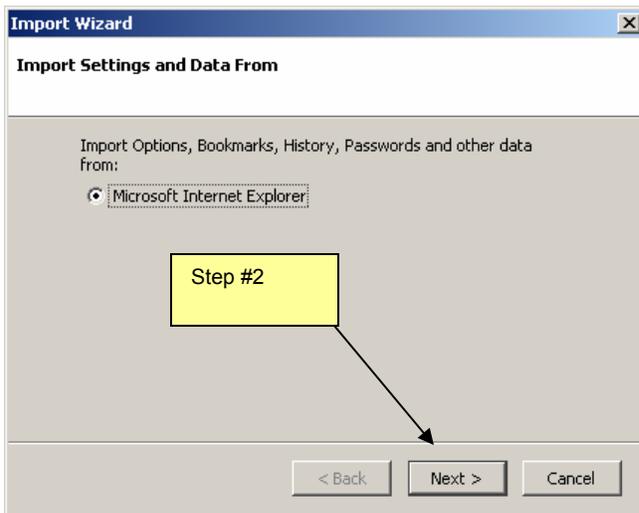


## IMPORTING IE SETTINGS

Remember that the first time you use Firefox; it will bring in all of your IE settings, including Favorites. But if you have several accounts (maybe for the kids) then you will need to do it manually for each of them. Or maybe for some reason you added to your IE list, you will want to update Firefox.

To do so:

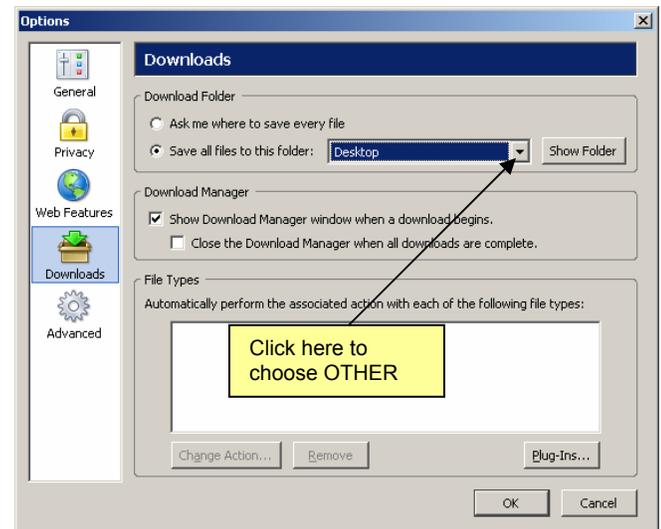
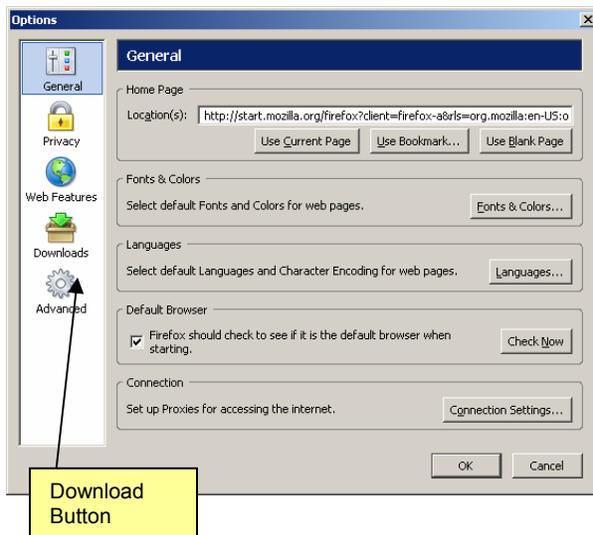
- 1) Click on FILE / IMPORT
- 2) Click on NEXT
- 3) Uncheck the items you do not want imported
- 4) Click on NEXT
- 5) Click on FINISH



## **MAKING A FOLDER TO STORE YOUR DOWNLOADS**

Many people who do not frequently download software from the internet have difficulty telling the difference between the program used to install software, and the software that has already been installed. By default, Firefox saves all downloaded files to your Windows desktop, which in no way helps this situation. To eliminate this confusion, we are going to create a folder to save all the downloads. We will call the folder DOWNLOADS and place it on the desktop (you can, of course, choose any other place you'd like to put your downloads, but this guide will use a Downloads folder on the desktop).

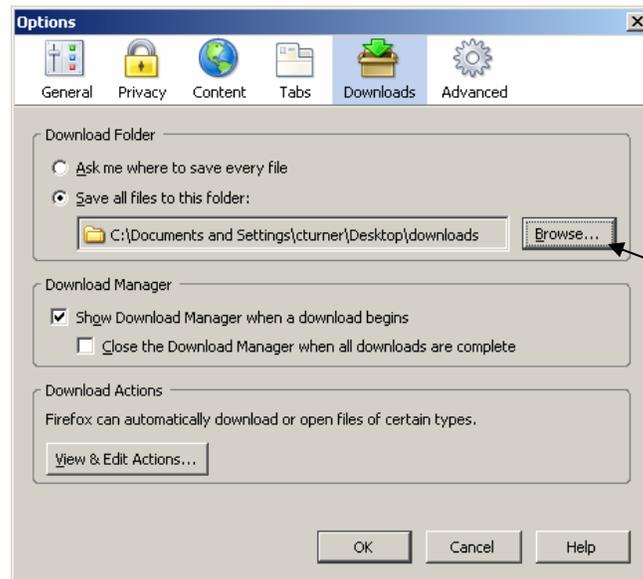
- 1) While in FIREFOX, click on TOOLS / OPTIONS
- 2) Click on the DOWNLOADS button
- 3) Click on the Down arrow key next to SAVE ALL FILES TO THIS FOLDER and choose OTHER
- 4) Click on the DESKTOP folder and then choose NEW FOLDER
- 5) Type in DOWNLOADS
- 6) Click on OK and OK again
- 7) You now have a folder on the desktop called DOWNLOADS and FIREFOX knows to save all downloads into there



Depending on the version of Firefox that you are using, your screens above may be a little bit different. For Step #3, you might need to click on the BROWSE button next to SAVE ALL FILES TO THE FOLDER

Then click on the DESKTOP folder (located at the very top of the list)

Then click on MAKE NEW FOLDER



## DOWNLOADING ADAWARE

Now that you have downloaded FIREFOX, we will be using that as our web-browser. We are going to a web-site called DOWNLOAD.COM. It is an awesome place for downloading software, but it is a very confusing web-site the first couple of times one visits. You see, there are tons of advertisements all over the page. Not to mention that when you look for a program, it will put all of the advertising at the top of the page, ahead of your search results. You MUST scroll down to find what you are looking for. So with that in mind:

- 1) Open up Firefox (or IE if you are not using Firefox. But use Firefox)
- 2) Type in DOWNLOAD.COM in the address bar
- 3) The web-site will load
- 4) In the Search box on the web page, type in ADAWARE and click on GO
- 5) BE CAREFUL! WATCH OUT FOR ALL OF THE ADVERTISING. Normally the top 3-5 items listed are sponsored items unrelated to your search. You must scroll down past the gray bar to see the non-advertising results.
- 6) Once you scroll down past the gray bar and find AD-AWARE SE PERSONAL edition, click on the green DOWNLOAD arrow on the far right
- 7) Because we created the folder in the step above, the file that is being downloaded will go directly into the DOWNLOAD folder on the desktop.

Search results for adaware - Reviews and free downloads at Download.com - Mozilla Firefox

YOUR SEARCH:  All Software

FROM OUR SPONSORS

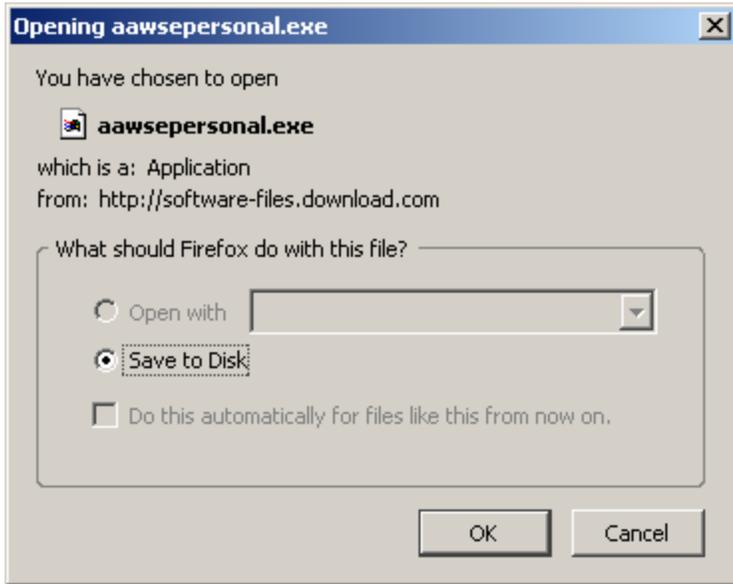
Adware Remover Download  
PC Magazine Editors Choice Winner! Download 5 Star Rated Adware killer  
[www.pctools.com](http://www.pctools.com)

Ad-ware - Free Download  
2006 Leading Spyware Remover. Kill Popups & Viruses in Seconds!  
[www.noadware.net](http://www.noadware.net)

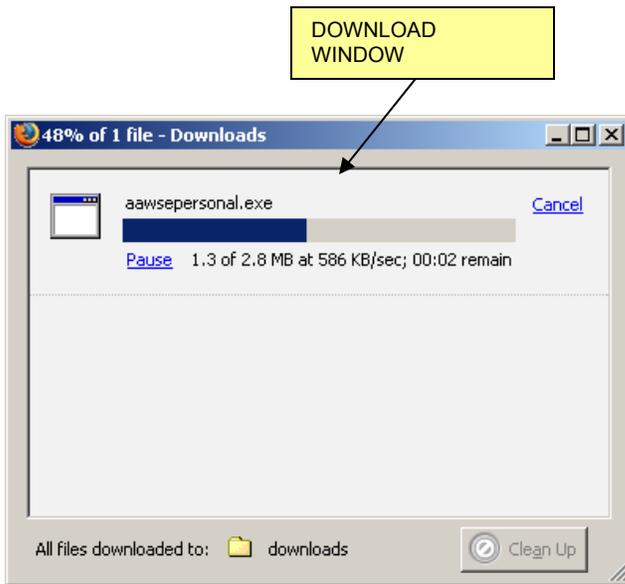
Adware - Free  
Need to Get Rid of Spyware - Fast? Get Your Quick Download - Free!  
[www.adaware.com](http://www.adaware.com)

> More results like this...

Re-sort by: Name   ENET rating [?]   User rating	Date added	Total downloads	
<b>Ad-Aware SE Personal Edition 1.06</b> ★ ★ ★ ★ ★ ONET EDITOR'S RATING ☆ ☆ ☆ ☆ ☆ USER RATING Scan your system for ad-supported software components and remove them. <a href="#">Read full review...</a>	05/27/2005	177,162,191 ♥ Popular	<input checked="" type="checkbox"/> Download <input type="checkbox"/> Buy now
<b>Startup Mechanic 2.6</b> ★ ★ ★ ★ ★ ONET EDITOR'S RATING ☆ ☆ ☆ ☆ ☆ USER RATING Scan and remove data-mining, advertising, and tracking components from your system. <a href="#">Read full review...</a>	12/26/2005	439,506 ♥ Popular	<input checked="" type="checkbox"/> Download



- 8) Click on SAVE TO DISK
- 9) The DOWNLOAD Window will open up and show you what is, and has been downloaded. When it is done. It will say so. You can close this window down now or at any time without affecting your download.

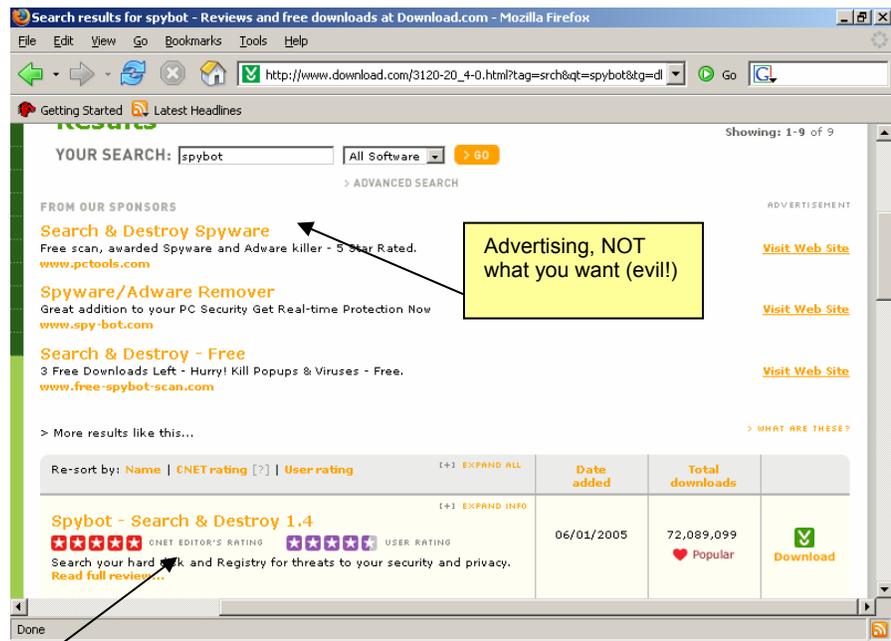


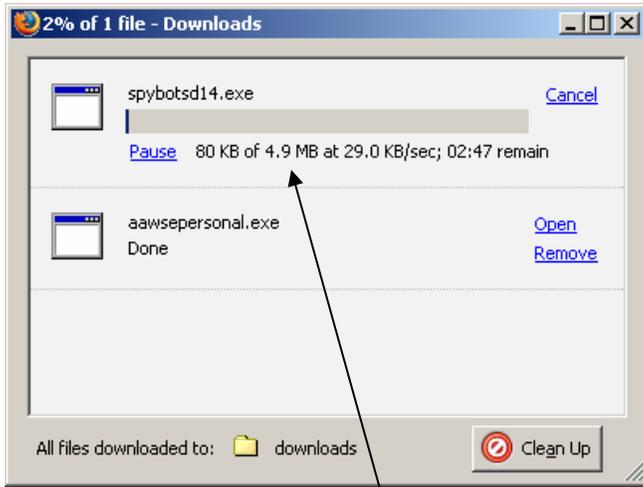
## DOWNLOADING SPYBOT

If you have already downloaded ADAWARE and you have DOWNLOAD.COM open, simply jump to step # 4.

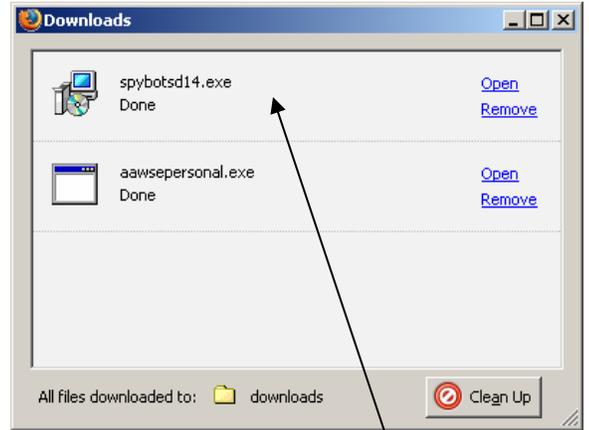
Now that you have downloaded FIREFOX, we will be using that as our web-browser. We are going to a web-site called DOWNLOAD.COM. It is an awesome place for downloading software, but it is a very confusing web-site the first couple of times one visits. You see, there are tons of advertisements all over the page. Not to mention that when you look for a program, it will put all of the advertising at the top of the page, ahead of your search results. You MUST scroll down to find what you are looking for. So with that in mind:

- 1) Open up Firefox (or IE if you are not using Firefox. But use Firefox)
- 2) Type in DOWNLOAD.COM in the address bar
- 3) The web-site will load
- 4) In the Search box on the web page, type in SPYBOT and click on GO
- 5) BE CAREFUL! WATCH OUT FOR ALL OF THE ADVERTISING. Normally the top 3-5 items listed are sponsored items unrelated to your search. You must scroll down past the gray bar to see the non-advertising results.
- 6) Once you scroll down past the gray bar and find SPYBOT - SEARCH AND DESTROY, click on the green DOWNLOAD arrow on the far right
- 7) Because we created the folder in the step above, the file that is being downloaded will go directly into the DOWNLOAD folder on the desktop.





In Process



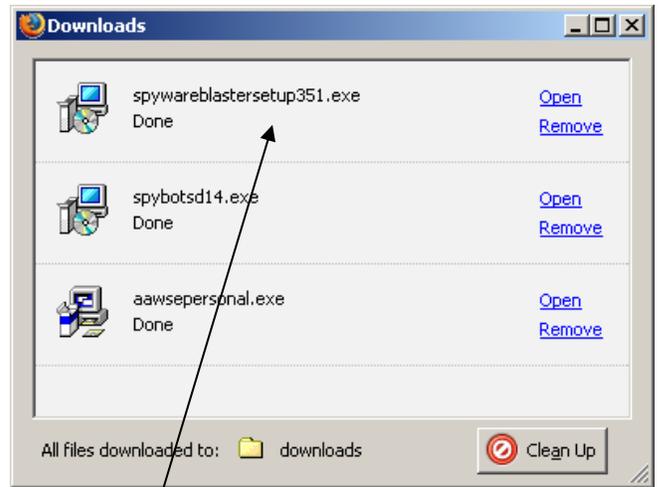
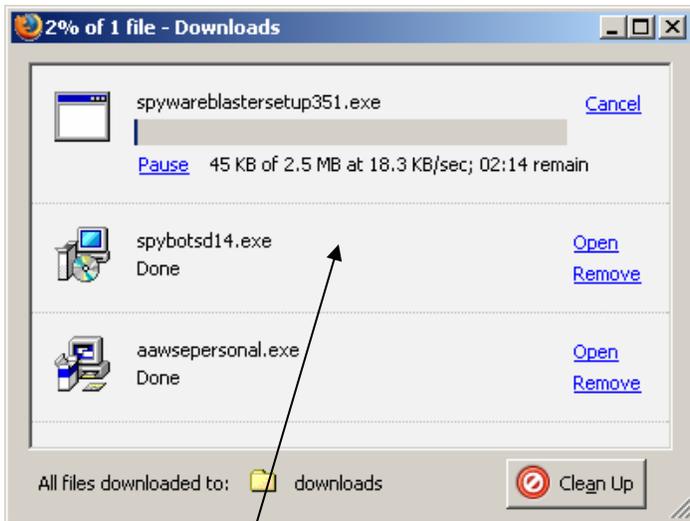
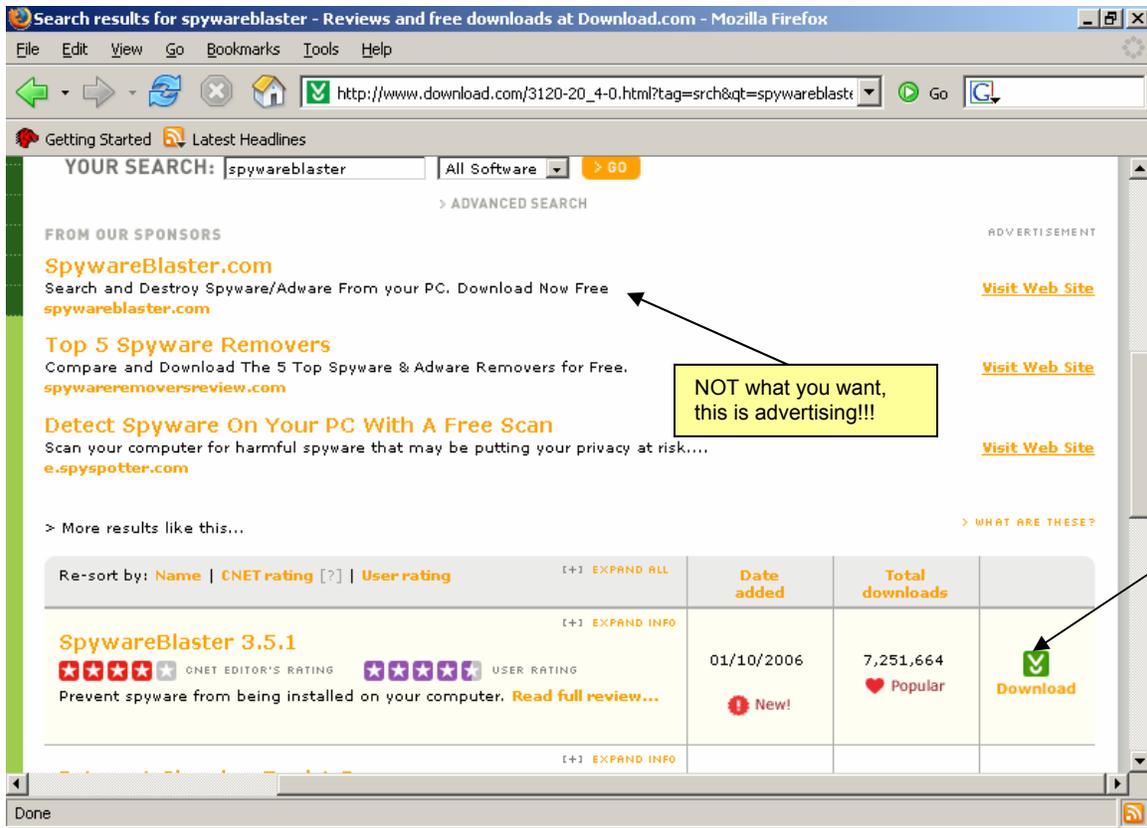
Done

## **DOWNLOADING SPYWAREBLASTER**

If you have already downloaded ADAWARE or SPYBOT and you have DOWNLOAD.COM open, simply jump to step # 4.

Now that you have downloaded FIREFOX, we will be using that as our web-browser. We are going to a web-site called DOWNLOAD.COM. It is an awesome place for downloading software, but it is a very confusing web-site the first couple of times one visits. You see, there are tons of advertisements all over the page. Not to mention that when you look for a program, it will put all of the advertising at the top of the page, ahead of your search results. You MUST scroll down to find what you are looking for. So with that in mind:

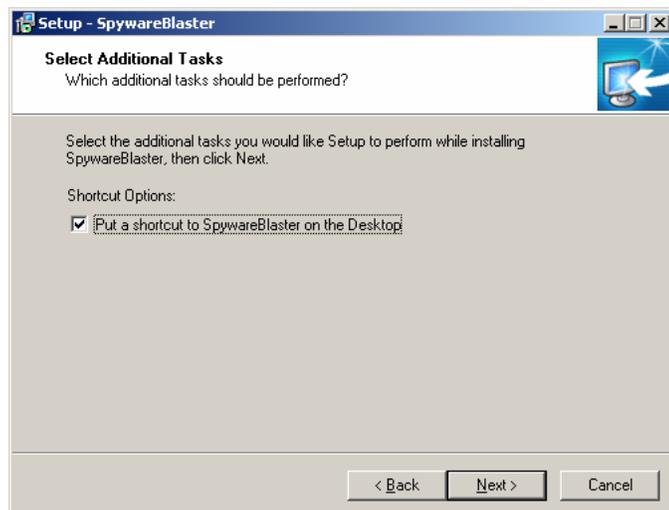
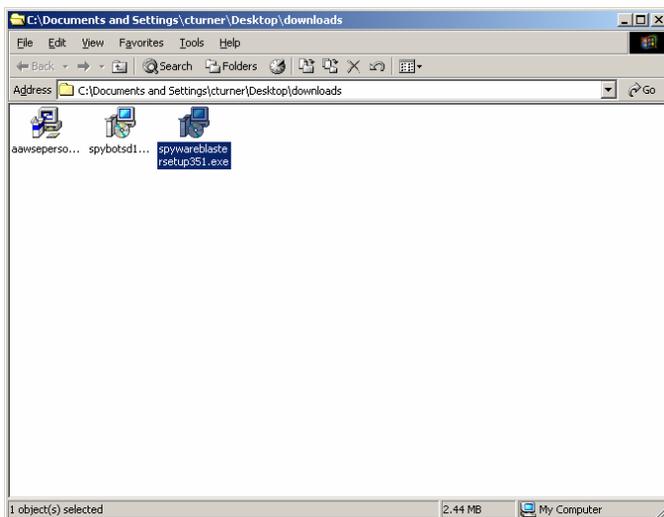
- 1) Open up Firefox (or IE if you are not using Firefox. But use Firefox)
- 2) Type in DOWNLOAD.COM in the address bar
- 3) The web-site will load
- 4) In the Search box on the web page, type in SPYWAREBLASTER and click on GO
- 5) BE CAREFUL! WATCH OUT FOR ALL OF THE ADVERTISING. Normally the top 3-5 items listed are sponsored items unrelated to your search. You must scroll down past the gray bar to see the non-advertising results.
- 6) Once you scroll down past the gray bar and find SPYWAREBLASTER, then click on the green DOWNLOAD arrow on the far right
- 7) Because we created the folder in the step above, the file that is being downloaded will go directly into the DOWNLOAD folder on the desktop.



## **INSTALLING AND RUNNING SPYWARE BLASTER**

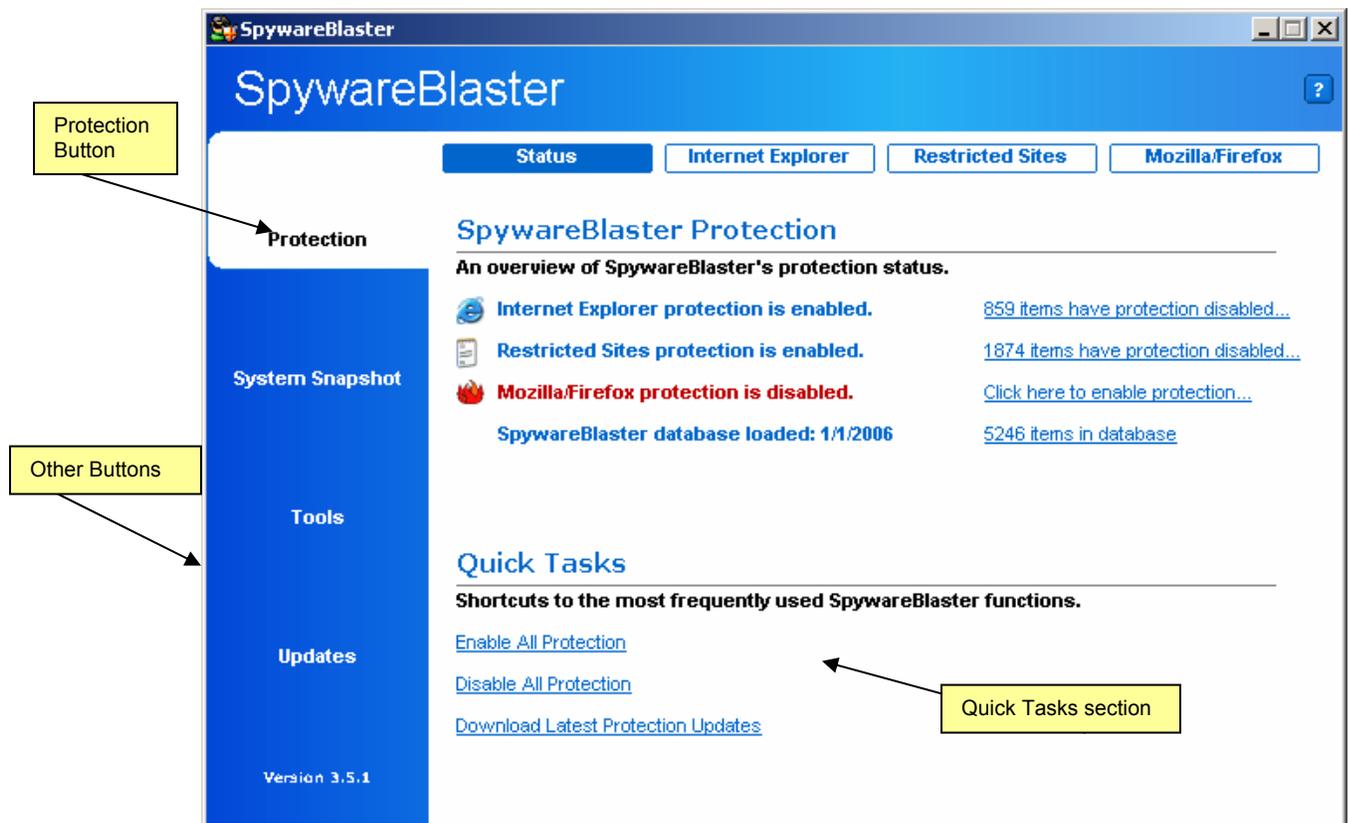
SpywareBlaster is a simple program that prevents your computer from contacting certain known-bad (bad as in “Installs or supports Spyware”) sites on the Internet. It does *not* remove any spyware one might already have. To Install SPYWAREBLASTER:

- 1) Double-click on the downloads folder on your desktop
- 2) Double-click on the icon that says SPYWAREBLASTERSETUPxyz.EXE
- 3) Click on NEXT
- 4) Click on I ACCEPT THE AGREEMENT and then NEXT
- 5) Click on NEXT on the INFORMATION screen
- 6) Click on NEXT on the SELECT DESTINATION LOCATION screen
- 7) Make sure that there is a check for PUT A SHORTCUT TO SPYWARE BLASTER ON THE DESKTOP
- 8) Click on NEXT
- 9) Click on INSTALL
- 10) Keep the box RUN SPYWARE checked and click on FINISH



The first time you run SpywareBlaster, it will run through a series of help screens to explain how to use and update the program. Just follow along and click. (Click NEXT on the GETTING STARTED screen, click NEXT on the KEEP UP TO DATE screen, Click FINISH on the THANK YOU screen). If this is the second time in, you can simply double-click in the icon on the desktop in order for it to run. It will then look like the following:

## PARTS OF THE SCREEN FOR SPYWAREBLASTER



### **TO USE SPYWAREBLASTER:**

- 1) Under QUICK TASKS, click on ENABLE ALL PROTECTION
- 2) Under QUICK TASKS, click on DOWNLOAD LATEST PROTECTION UPDATES
- 3) Click on CHECK FOR UPDATES
- 4) When it is done, on the left hand pane, click on the PROTECTION tab
- 5) Click on ENABLE ALL PROTECTION again under QUICK TASKS
- 6) Close down SPYWAREBLASTER

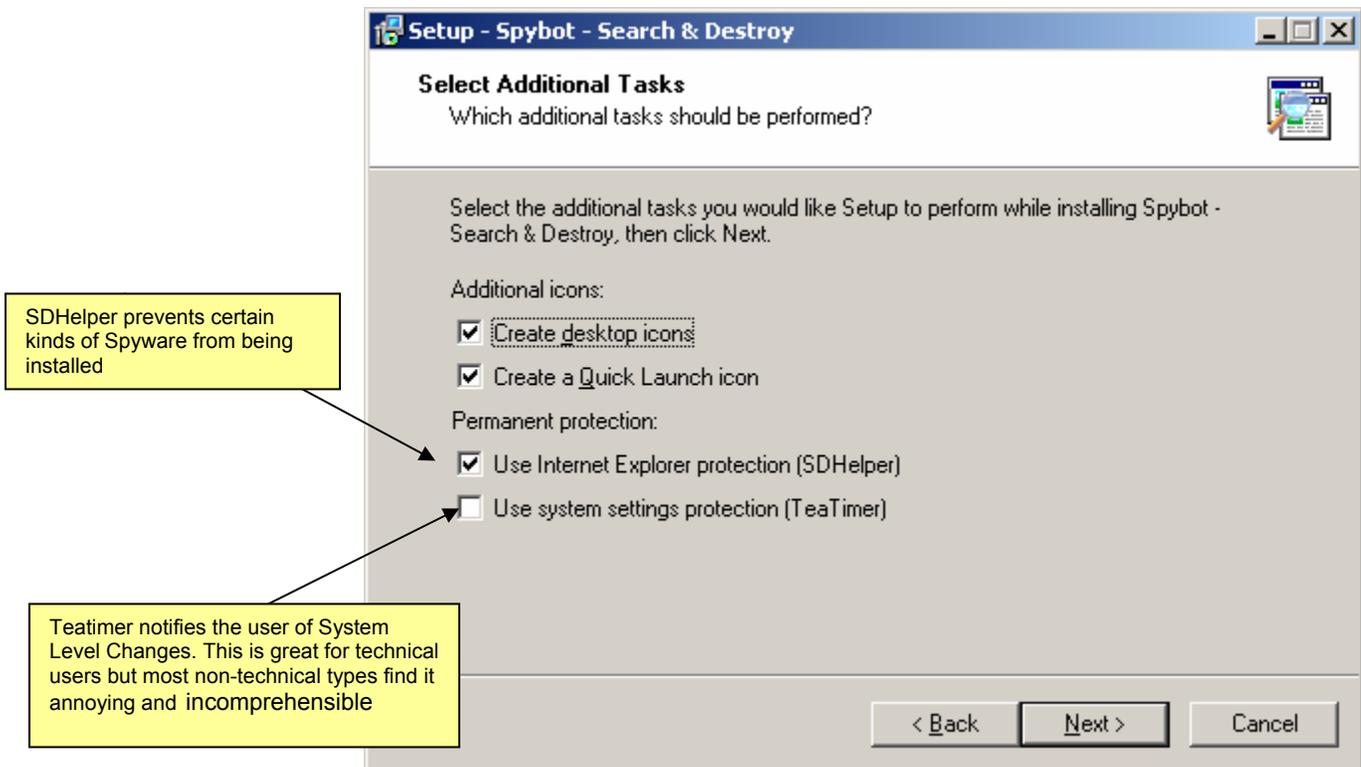
Roughly one time a week, a user should start this program, click “Download Latest Protection Updates”, then follow through by clicking the “Check for Updates Button” in the updates Window. Once updates have been downloaded, click the “Enable All Protection” button.

If the program is being used properly, there should always be zero items with protection disabled in each of the three categories. Every once in a while, a spyware program will add itself to SpywareBlaster’s exceptions list, so care should be taken that *nothing* is excepted from protection. “Enable All Protection” removes items from the exceptions list. A for-pay version of SpywareBlaster can update and add protection automatically. Honestly, that’s OK, but spyware is so pervasive that it’s probably better for a user to regularly monitor his or her computer by manually running and updating these programs.

## INSTALLING SPYBOT

Spybot is a parasite removal program. In order for it to work properly, you need to run it twice. Once in “normal” mode to get the latest updates and then again in SAFE MODE to actually remove the crud it’s supposed to remove. Spybot will not install updates for you. You must check for updates fairly regularly (weekly). So, we have to install it first, then run it. To install it:

- 1) Double-click on the ICON in the DOWNLOADS folder
- 2) Select ENGLISH as the language and click on OK
- 3) Click on NEXT on the WELCOME screen
- 4) Click on I ACCEPT THE AGREEMENT and then NEXT
- 5) Click on NEXT to accept the DESTINATION LOCATION
- 6) On the SELECT COMPONENTS screen, click on NEXT
- 7) On the SELECT START MENU FOLDER screen, click on NEXT
- 8) When you get to the SELECT ADDITIONAL TASKS screen, make sure that TEATIMER is unchecked. Click on NEXT
- 9) Click on INSTALL
- 10) Uncheck RUN SPYBOT and click on FINISH. We are unchecking RUN SPYBOT because we do not want to run it now. If we do, a wizard will come up, step us thru and we will be done. The problem with that is that is the only time you see the wizard, the first time through. So we want to make sure you know how to run it without the wizard.

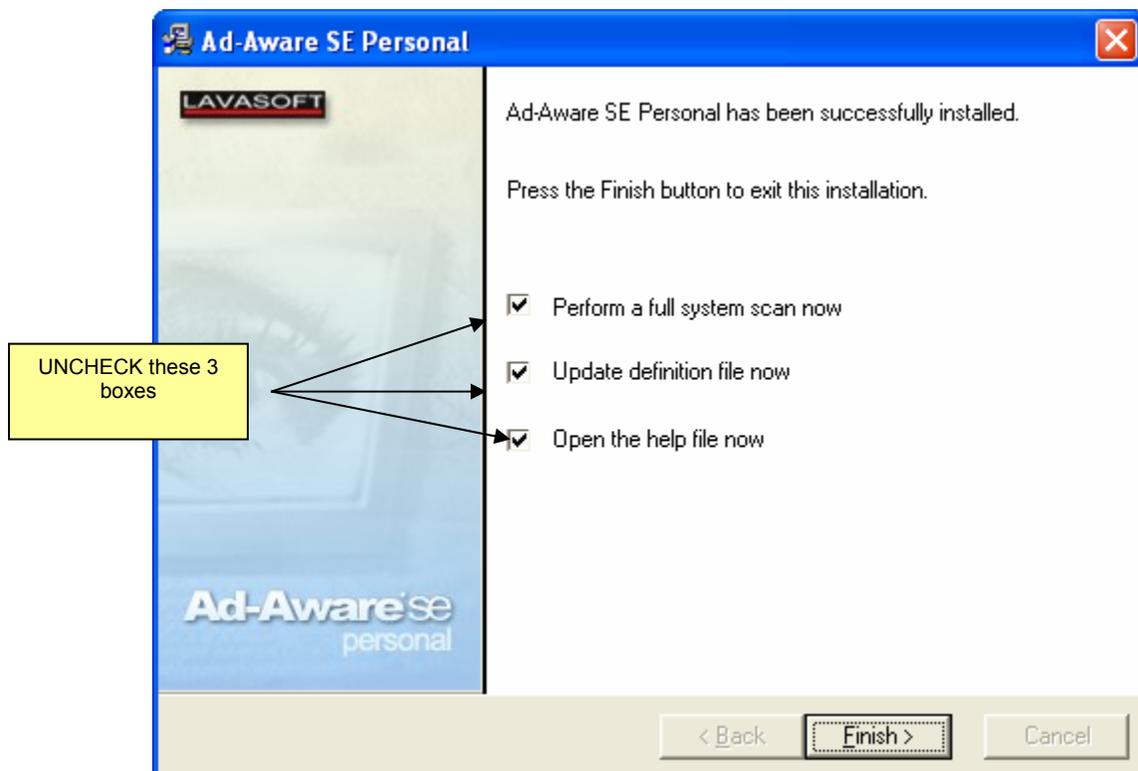


## INSTALLING ADAWARE

Adaware is a program that will remove spyware. I am assuming that you have already downloaded it in the steps above and that you have it in a folder called DOWNLOADS on your desktop.

SO, to install it:

- 1) Double-click on the DOWNLOADS folder on your desktop
- 2) Double-click on the AAWPERSONALxxxx.EXE file
- 3) Click on NEXT
- 4) Click in the box to accept the license and click on NEXT
- 5) Click on NEXT on the DESTINATION FOLDER screen
- 6) Click on NEXT on the INSTALL TO ALL USERS MENU screen
- 7) Click on NEXT to STAR INSTALLATION
- 8) When you get to a screen with a bunch of check marks ... STOP
- 9) Uncheck all three boxes and click on FINISH. We are doing this because once again the program will do this all for you, using a wizard, but you will never see the wizard again. We need to make sure that you know how to run the program without the wizard. Therefore, we are stopping at this point!



## RUNNING ADAWARE – FOR PURPOSES OF UPDATES ONLY

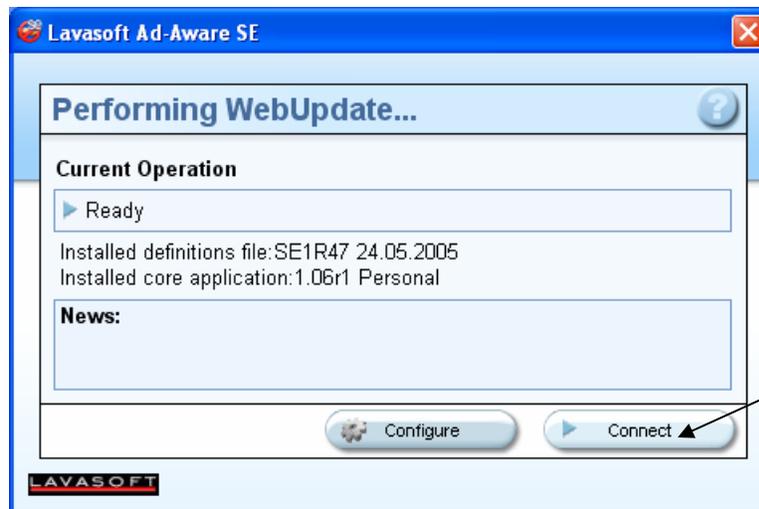
Ad-aware needs to be run in regular mode while you are connected to the network so that you can check for updates to the program. Once we are done running it, we will run it again in Safe mode to remove all of the spyware.

So, to check for updates (I am assuming that you followed the directions above and installed the program with a shortcut on the desktop)

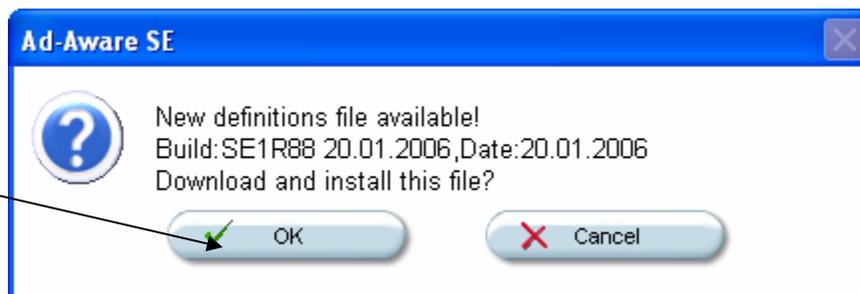
- 1) Double-click on the AD-AWARE icon on your desktop
- 2) If your updates are old, it will say so and ask you if you want to check for updates. Always say OK.. Click on CONNECT.. Click on OK. If your updates are not old, then it will take you directly to the main screen and you can close down
- 3) When you get to the main screen, close the program down.



Screen you will get if the definitions are old



Click on CONNECT to go to the Internet to check for updates



Click on OK to download the file so that you are up to date

## AD-AWARE MAIN SCREEN



By the way, if this is not the first time in, then this is how you check for updates.

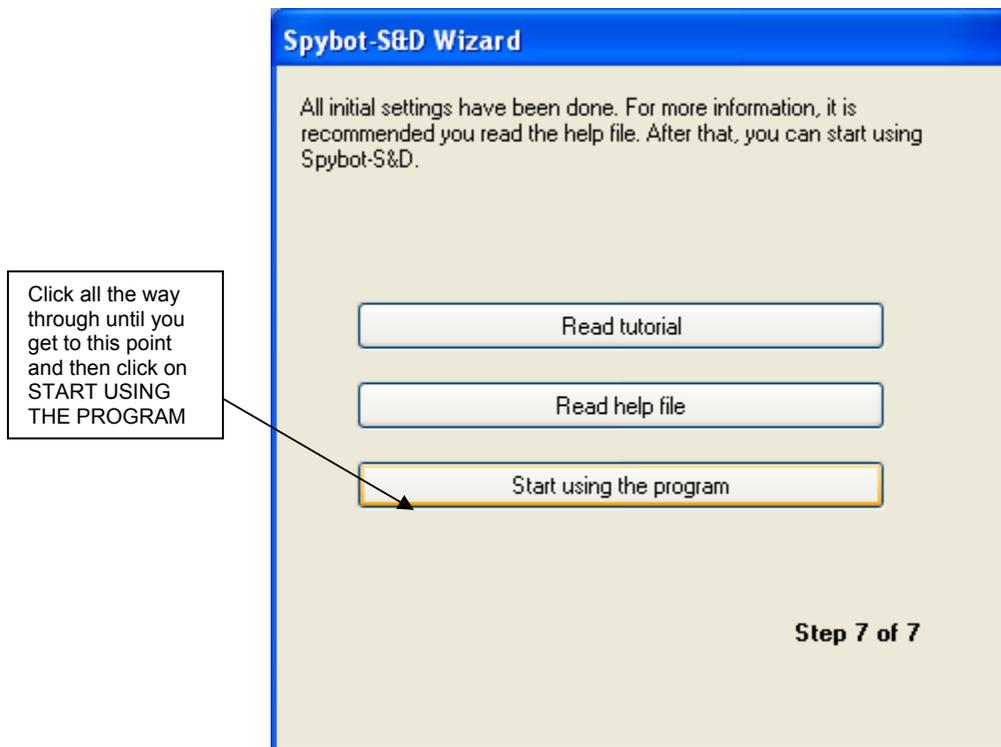
- 1) Click on CHECK FOR UPDATES NOW
- 2) Click on CONNECT
- 3) Click on FINISH

The updates install very quickly if you have a fast internet connection. Dialup users will have time for a couple games of Solitaire at this point.

## **RUNNING SPYBOT FOR PURPOSES OF UPDATES ONLY – IN NORMAL MODE**

Now let's run Spybot (for purposes of getting the updates only!). I am assuming that you downloaded the program with the steps above and there is a shortcut on your desktop. I am also assuming that this is the first time you've run the program.

- 1) Double-click on the SPYBOT icon on your desktop
- 2) If there is a legal message, click on OK
- 3) It will ask you to create a registry backup. Create the backup by clicking the button and then NEXT
- 4) Continue to click NEXT all the way through until you get to a window with a START USING THE PROGRAM button. We do this because the only time that you will see the wizard is the first time that the program runs. I want to make sure that you know how to use the program without the wizard, hence all the clicking!



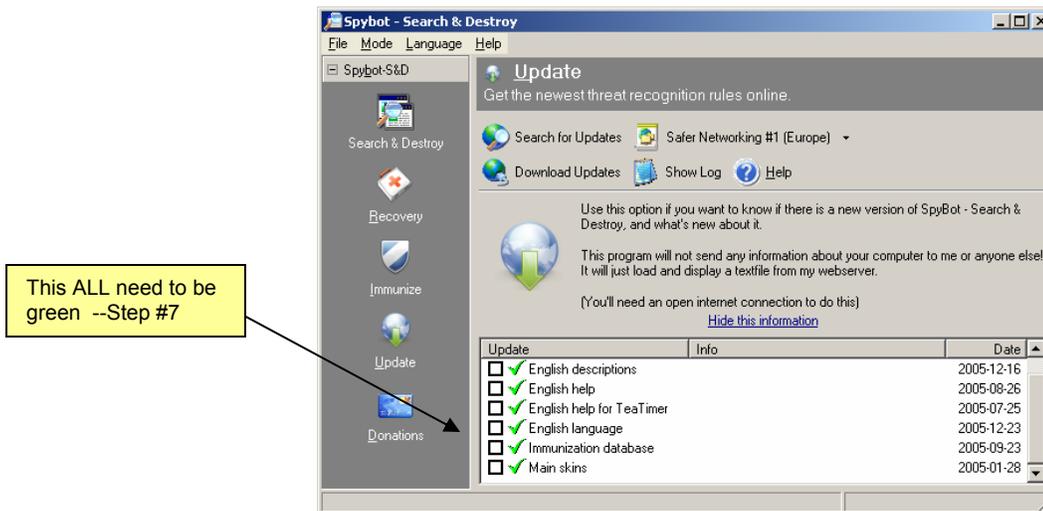
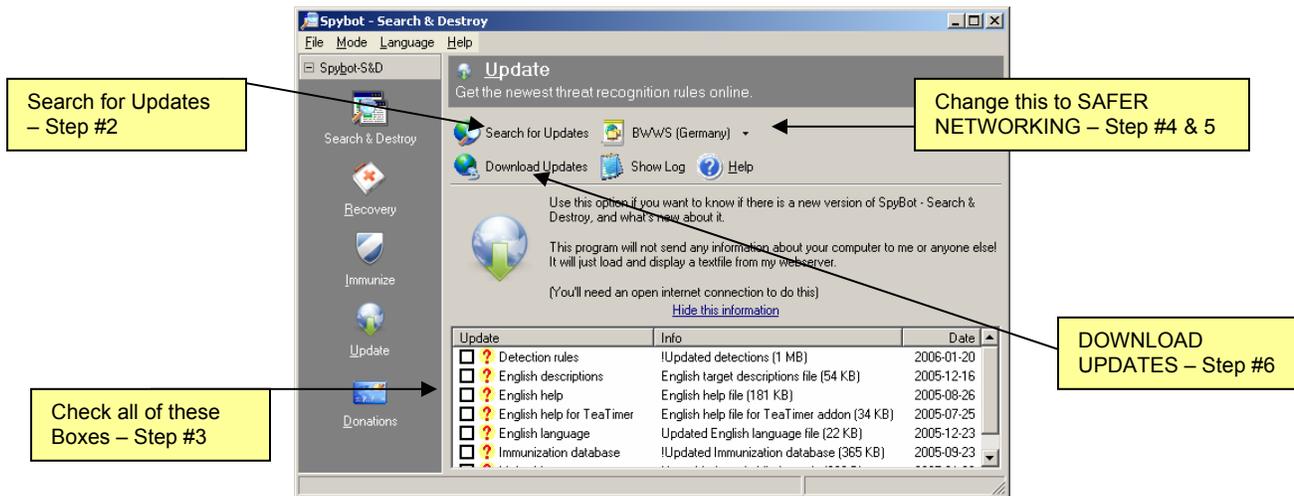
Once you click on START USING THE PROGRAM the following screen will appear:

## PARTS OF THE SPYBOT SCREEN



## TO RUN THE PROGRAM FOR UPDATES ONLY

- 1) Click on SEARCH FOR UPDATES (in the center of the screen)
- 2) Click on SEARCH FOR UPDATES (at the top of the screen)
- 3) Check ALL of the boxes (the ones that have the red and yellow question mark)
- 4) Look at the button next to SEARCH FOR UPDATES and click on the down arrow key next to it.
- 5) Choose SAFER NETWORKING (either one) .. DO NOT choose the site in AUSTRALIA (unless you're in Australia, in which case it's probably the best choice)
- 6) Click DOWNLOAD UPDATES
- 7) All of the question marks should have turned to green check marks. If not, DO IT AGAIN
- 8) Close the Program down



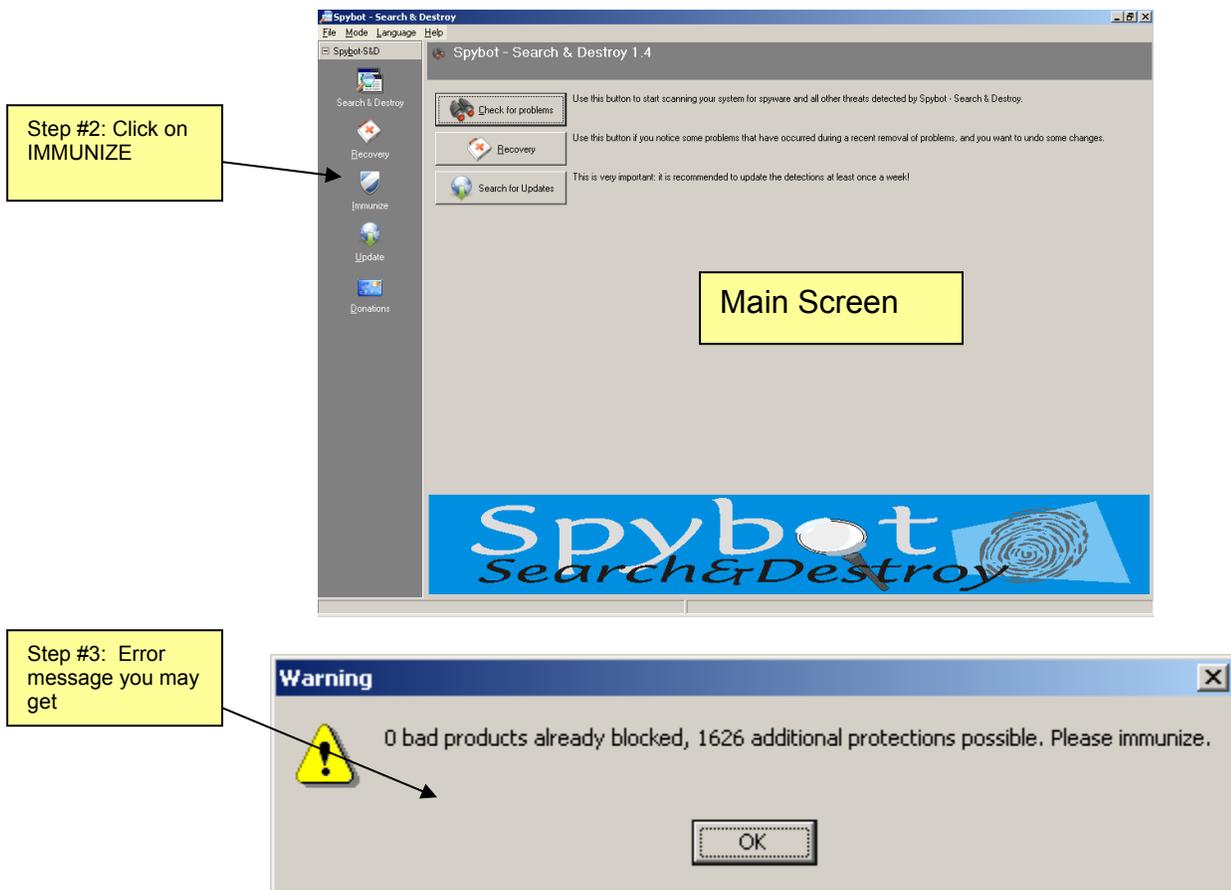
## **GETTING TO SAFE MODE**

Now that you have all of the programs downloaded and installed and updated, you need to run ADAWARE and SPYBOT in safe mode so that they can do their job. Why safe mode? Because Spyware programs are generally configured to start up with Windows and to run the entire time Windows is running. As long as the programs are running, they are much less likely to be detected or successfully removed. In safe mode, most programs, even important ones configured to start up with the computer, such as Antivirus programs, don't start up. Safe mode is the bare minimum of software needed for Windows to operate, and it's supposed to be a clean environment for running maintenance of all sorts.

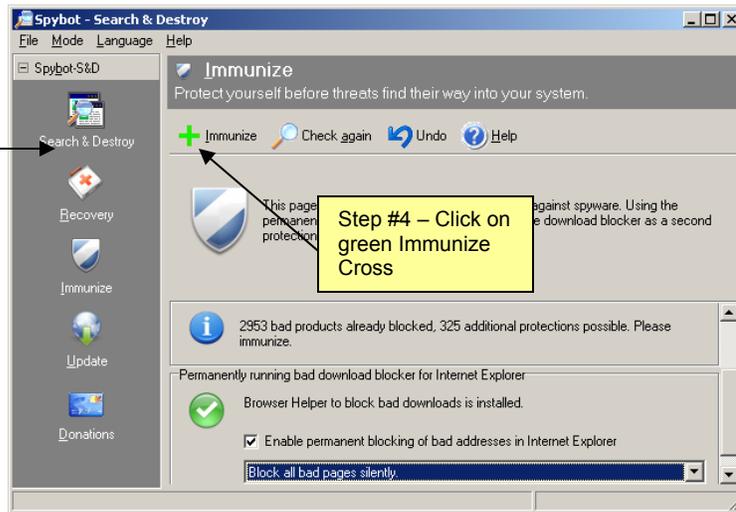
- 1) Shut down all programs that you are working in and save all of your data
- 2) Restart your computer
- 3) As your Computer begins to start back up (when the screen turns black), begin repeatedly tapping the F8 key (located at the top of your keyboard) constantly.
- 4) If you catch it, your computer will soon come to a black screen with choices, one which is RUN IN SAFE MODE. If you did not catch it, turn off your computer and try again.
- 5) Using your arrow keys on the keyboard, Choose SAFE MODE and wait a minute or five
- 6) Answer YES to SAFE MODE. If you say no, your system will go into RESTORE mode, which really will do you no good!
- 7) Your system will eventually come up to a black screen, with Larger letters and Icons than you are probably used to seeing.
- 8) You should see both AD-AWARE and SPYBOT on the desktop somewhere.

## RUNNING SPYBOT IN SAFE MODE

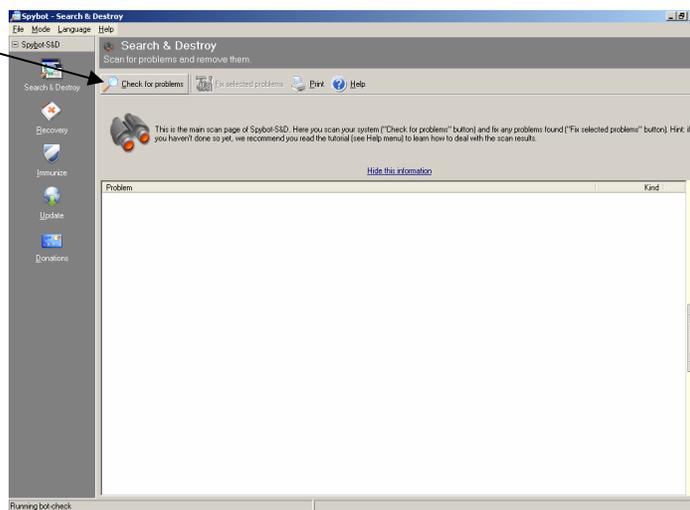
- 1) Double-click on SPYBOT. Since we are in SAFE mode, we cannot check for updates, even if we wanted to
- 2) Click in the left pane and choose IMMUNIZE (The shield).
- 3) Click on OK when it gives you the warning message
- 4) Click on the GREEN Cross that says IMMUNIZE (towards the top). If you maximize the screen, then you will be able to see what it is doing.
- 5) Once it is done, on the left pane, click on SEARCH AND DESTROY
- 6) Click on the magnifying glass CHECK FOR PROBLEMS (towards the top)
- 7) If you watch the bottom status line, it will tell you where it is checking for all of the bad stuff. This should take about 3-10 minutes.
- 8) Click on FIX SELETED PROBLEMS
- 9) Click on YES when it asks you "Do you want to remove selected problems"
- 10)When it is done, all of the boxes should now have GREEN check marks next to them
- 11)Close the program down



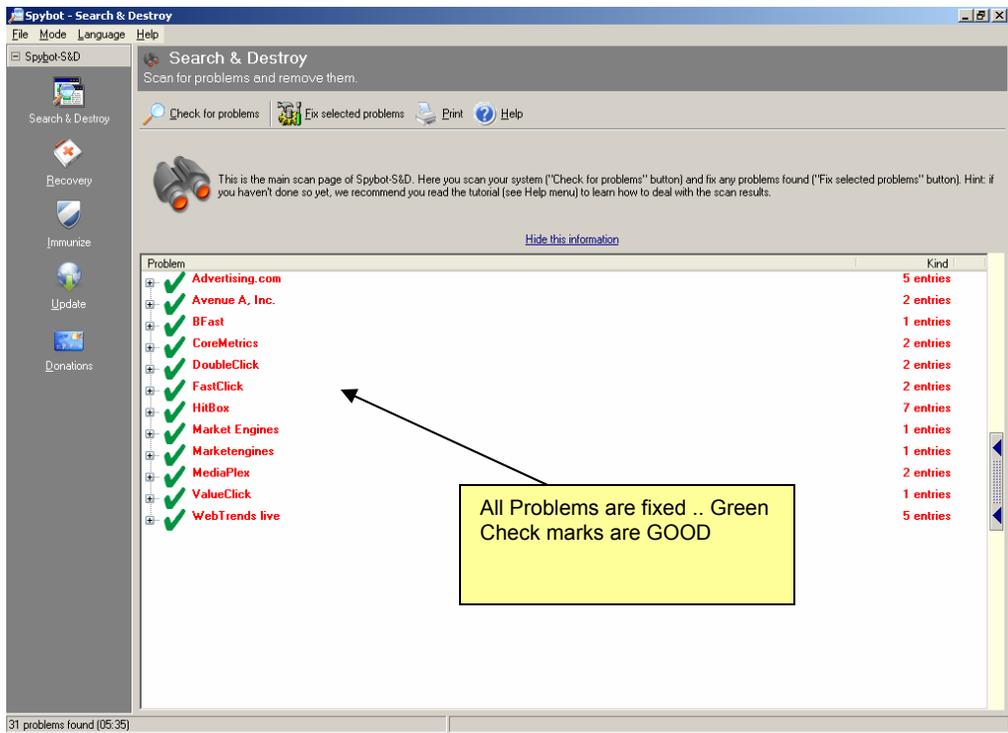
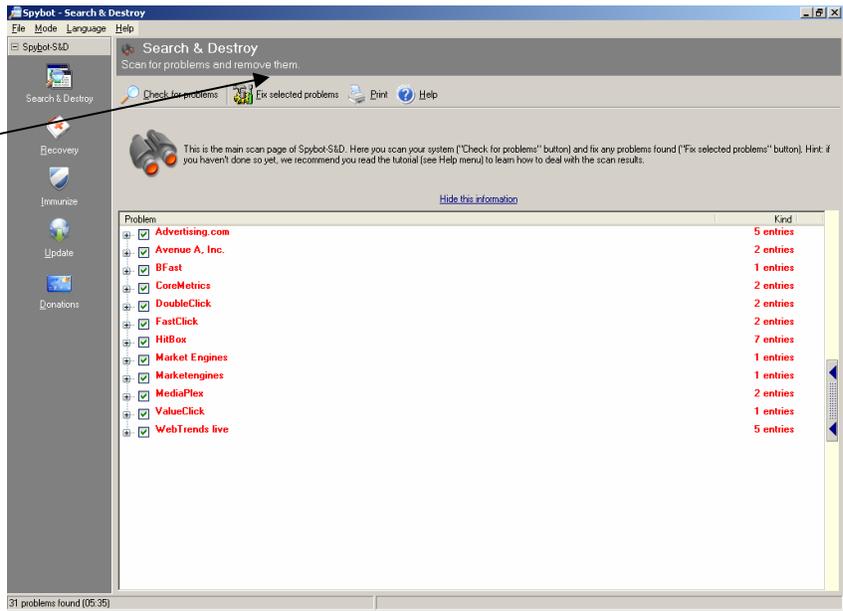
Step #5 – Click on SEARCH AND DESTROY



Step #6 – Click on CHECK FOR PROBLEMS



Step #8 – Click on FIX  
SELECTED PROBLEMS



All Problems are fixed .. Green  
Check marks are GOOD

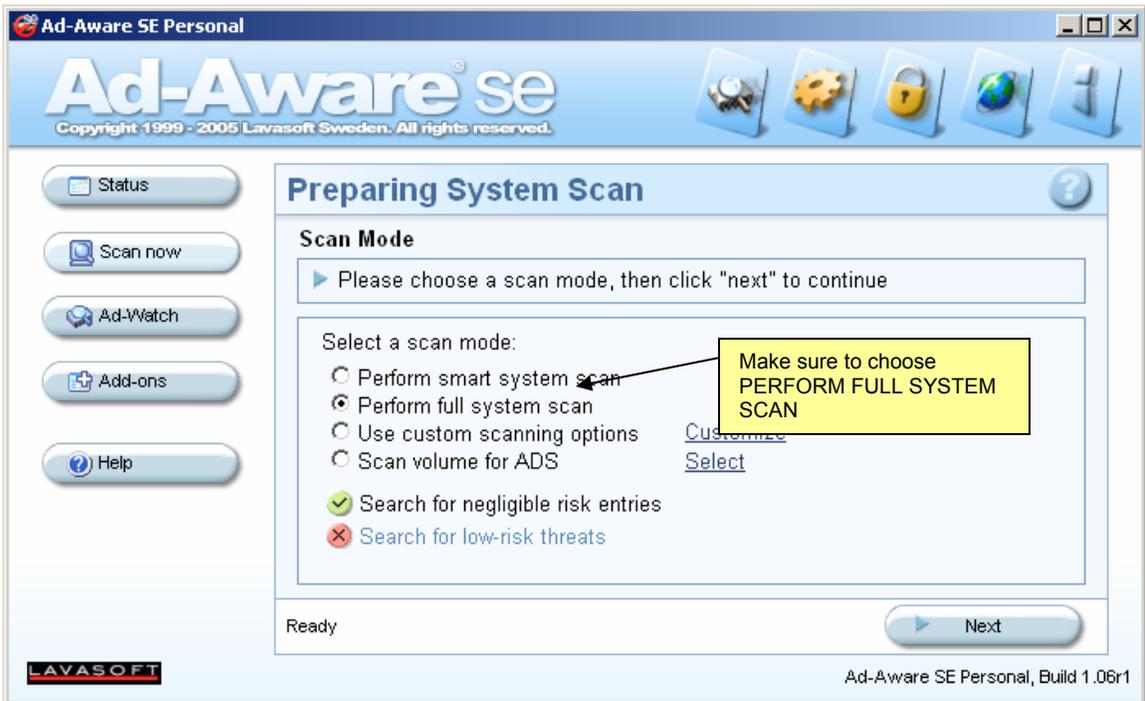
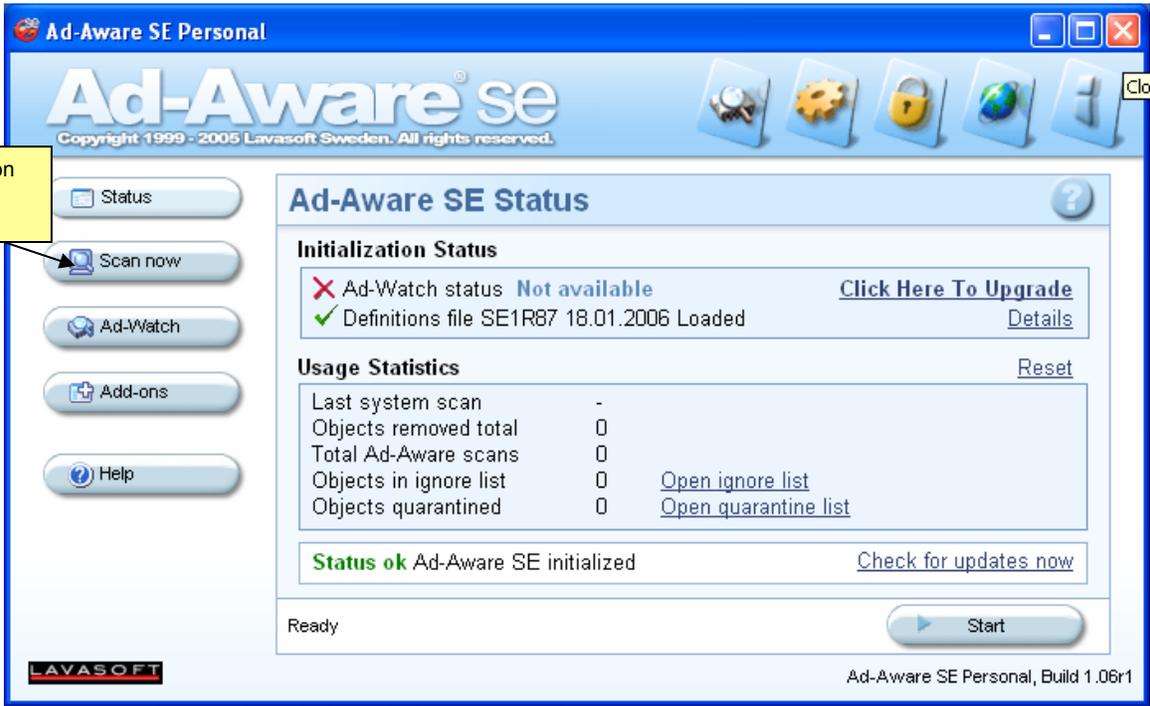
It is not uncommon for Spybot to say that it cannot remove a particular software package until Windows is restarted. That is fine. The software will still be removed. It is also not uncommon for Spybot to continuously flag “DSO Exploit” as a problem on your computer. The DSO Exploit refers to a security problem with Internet Explorer that may or may not actually be a problem on your computer. If you regularly install Windows Updates, it is not an issue on your PC.

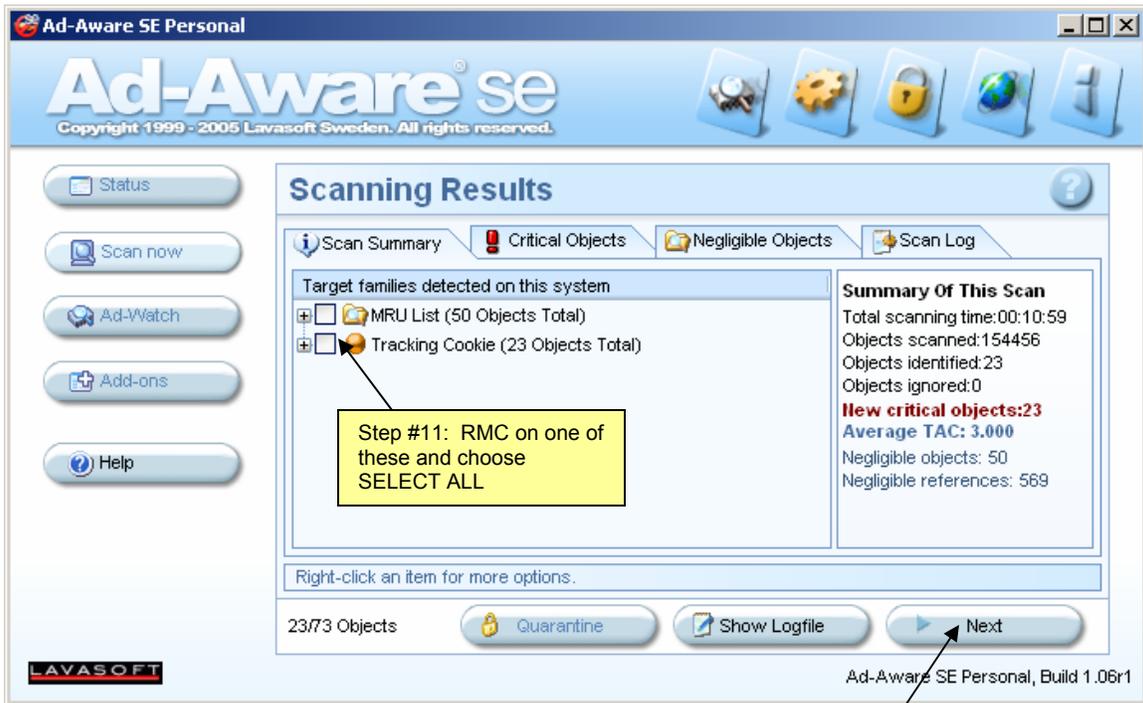
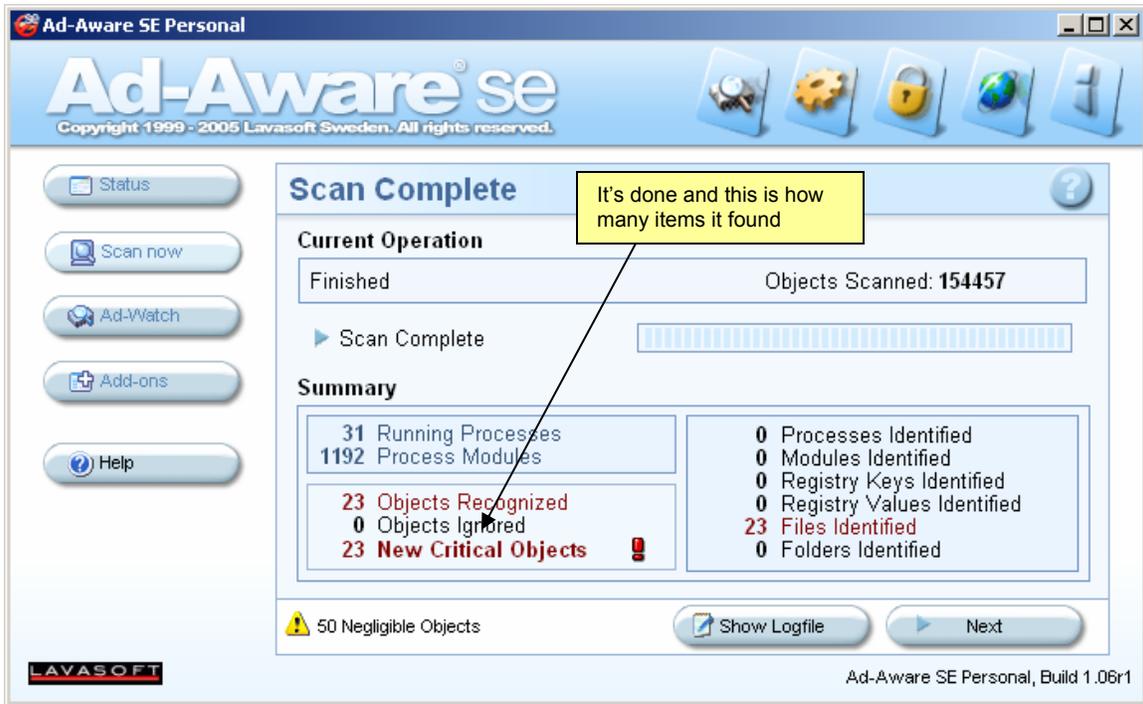
## **RUNNING AD-AWARE IN SAFE MODE**

Now that you are in safe mode (if not, follow the directions above)

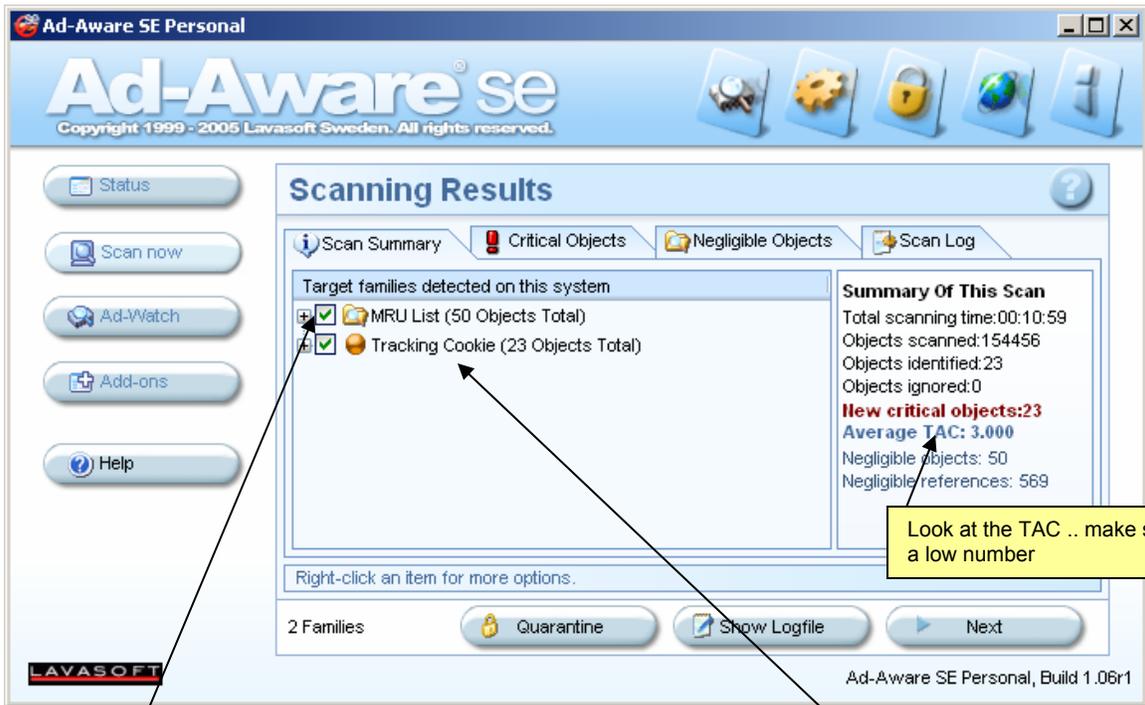
- 1) Double-click on the AD-AWARE icon on your desktop (or in START / PROGRAMS / LAVA SOFT)
- 2) The program will begin to run
- 3) The updates should be up to date because you followed direction and checked for updates before getting into safe mode! Because you have already installed its updates, you can immediately choose to proceed to a scan
- 4) Click on SCAN NOW in the left pane
- 5) Click on PERFORM FULL SYSTEM SCAN
- 6) Click on NEXT
- 7) Begin to WAIT.. and WAIT .... And WAIT. Eventually Ad-aware will finish and tell you what it found (xyz Critical Objects found), with a little red exclamation point next to it.
- 8) Click on NEXT
- 9) Click on SCAN SUMMARY. Notice the TAC (\*\*see below)
- 10) RMC on one of the boxes and choose SELECT ALL
- 11) Click on NEXT and then it will say that xxx number of objects are being removed .. please continue .. YES
- 12) Make sure that there is nothing in the IGNORE LIST. If so, open it up and remove anything on that list.
- 13) Close the program down

\*\*\* TAC - This is the threat assessment count. It is a rating from 1-10. High TAC ratings mean you have or had something scary on your computer.





Step #12: Click on NEXT



MRU: This is the MOST RECENTLY USED. These are normally not a big problem.

COOKIES: These are also normally not bad

Look at the TAC .. make sure it is a low number

Frequently Asked Questions:

1. *Are there any other programs that are effective for removing spyware?*

Of course there are. Adaware, Spyware Blaster and Spybot Search and Destroy all have for-pay automatically updating, real-time-scanning versions. Microsoft makes Microsoft AntiSpyware, which is presently in beta-test and may be made available for free to Windows Users (the beta version is a free download available at <http://www.microsoft.com/athome/security/spyware/software/default.msp>).

Even the best Antispyware programs will not prevent all infections. Even continuous real-time scanning with the commercial versions of these programs *will not stop all infections*.

A *substantial* number of programs available on the internet that claim to remove spyware either only remove spyware made by certain companies, while leaving purposefully spyware made by others, or actively download and install *more* spyware to inflate the purported usefulness of the software. There is a list of known bad anti-spyware programs at [http://www.spywarewarrior.com/rogue\\_anti-spyware.htm#products](http://www.spywarewarrior.com/rogue_anti-spyware.htm#products).

As a rule of thumb, the best and most effective tools are free.

Furthermore, it is the opinion of this document's author that Anti-Spyware/Privacy Guard/Firewall programs from major PC Utility software makers like Symantec (Norton Internet Security), and McAfee (Internet Security Suite) do far more harm than good when installed on an average home user's PC, since they are:

1. Difficult to install and configure properly
2. Give a false sense of security
3. Are insufficiently diligent at removing spyware – these programs are made by big companies that might be sued by small firms for mislabeling a program as spyware; lots of things Adaware or Spybot say are spyware are given a pass by Symantec and McAfee... with predictable consequences.

2. *Does installing Firewall software help?*

Kind of. A little bit. First of all, Windows XP, if it's been updated to Service Pack 2, comes with a firewall that doesn't need much in the way of configuration. That's great, because firewalls are tough for Computer Professionals to set up properly, let alone the average home user. Home users with broadband access might be surprised to know that a large percentage of Cable and DSL access devices *also* have a firewall built in.

Firewalls create a barrier between your "internal" computer or network and the rest of the internet. But if you choose to let something in, say, by installing a

game that includes a spyware installer, or by visiting the wrong web page with Internet Explorer, you've given the bad stuff a key to the front door. Your firewall might as well be tissue paper at that point.

Firewall programs on your PC also verify whether the programs running on your computer should be allowed to connect to the internet. Everyone who has had a firewall program has installed has probably seen a message like "Generic Host Process for Win32 has asked for permission to access the internet. Allow or Deny?"

And if you are a savvy computer user, you can look up what "Generic Host Process" is with Google and then choose whether to let that program do what it wants to do. This smart user can in that way prevent spyware from connecting to the internet and doing some of the obnoxious things that spyware does.

If you aren't quite so up on things, you'll probably settle on either allowing or denying everything. If you allow everything, you might as well not even have the firewall. If you deny everything, sooner or later you'll deny something important, like the Windows Update Background service, from working. Whoops.

Firewalls *do* protect against worms. A worm can be described as a virus that seeks to spread itself through an active network (internet) connection. Worms are so common that a freshly installed Windows XP computer with no firewall software that is plugged directly into a cable modem (that also doesn't have a firewall built in) will on average be infected with a worm within 15 minutes of being connected. You do need a firewall.

#### 4. *Why doesn't my Anti-Virus software pick this stuff up if it's so bad?*

Spyware does not meet the crucial minimum functionality of a virus – it's not self-replicating. It might've been installed from a Trojan that your Antivirus software should have caught. It might change crucial network settings, tell your computer to dial up to the internet through a server in Antigua, or reinstall itself despite your best efforts to remove it, but it's *not* a virus. By some twisted logic, it might be said that the spyware was installed on your computer in a legitimate fashion. Installing software, watching certain movie files or visiting certain web pages are all actions that might all cause spyware to be installed. In each case, there's probably some legalese somewhere that says "By accessing this content you agree to let us install horrible things on your computer."

Furthermore, the big Antivirus companies sell Anti-spyware software as well. They want you to buy *that* too.

#### 5. *Is there any way to not get Spyware?*

To be completely safe, no. Apple Macintosh computers at present do not have spyware problems, but that's mostly because they are far less common than PCs and because they don't use the Windows operating system. If Macs were more common there would be Spyware on them, too.

Using Firefox at the moment is a big help in preventing infection, but that has more to do with the fact that many fewer people use it than Internet Explorer. Firefox has a better track record of being updated to fix security issues, and it was designed with security in mind, but there are spyware programs that can affect Firefox, and supposedly Spyware authors have started writing software which might some day be able to infect Firefox. At the moment it's a better choice.

Choosing not to use Peer-to-Peer software downloading services and instant messaging programs also helps quite a bit. IM-addicted persons can probably get by with web sites that replicate IM software functionality, like [aimexpress.com](http://aimexpress.com) or [meebo.com](http://meebo.com).

These simple steps will prevent many malignant software installations.

- A. Stop using Internet Explorer (or the AOL Browser) to browse the web.
- B. Do not download *anything* from a non-trusted source...
- C. most especially silly games, icons, sounds, windows wallpapers, gambling software, peer to peer filesharing programs... if you really want those things, use google to find out whether the one you want is safe or not. If there's no information, assume that it's not safe.
- D. Do not follow web links that have been E-mailed to you.
- E. Do not open attachments in E-mail.

Because Internet Explorer is so insecure, and the entry point for many of these problematic software installations, I (and the Department of Homeland Security) recommend switching to a different web browser. I suggest downloading and installing the Firefox browser from Mozilla.org.

#### 6. *Why is Internet Explorer so bad?*

IE was not built with security in mind, kind of like having a house with a thick steel door that does not lock. Internet Explorer is a part of Windows, so technologies that were made to allow the web browser built into Windows to do neat tricks and present nifty interactive content also allow it to receive instructions like "Download this program, install it automatically and don't tell anyone".

Unfortunately, there's no way to completely turn internet explorer off or to disable all the features that spyware programmers use to install their evil on your PC. All you can do is choose not to use Internet Explorer unless you have to.

#### 7. *Why is Firefox better than Internet Explorer?*

Lots of reasons. Sticking to the spyware-related ones, Firefox is not part of the operating system, and therefore doesn't have hooks into some of the sensitive parts of Windows that IE does. Also, it's not possible to craft a web page to make Firefox install something on a PC without the user's explicit approval. Firefox can and usually is updated within minutes of a security flaw being found (Microsoft releases security updates on the second Tuesday of every month). Finally, Firefox lacks support for the major technologies Spyware makers use to infect PCs running IE.

#### 8. *Why is Spyware made?*

Spyware is profitable. Legitimate companies sometimes pay for the types of data that might be collected on a spyware-infected PC. Less legitimate companies might use spyware to drive traffic to an advertiser, to overlay one banner ad on top of another, or to read your personal information and credit card numbers from

the text boxes as you're ordering something on-line (because it's reading the information from a keyboard, the fact that it's encrypted on the page doesn't matter).