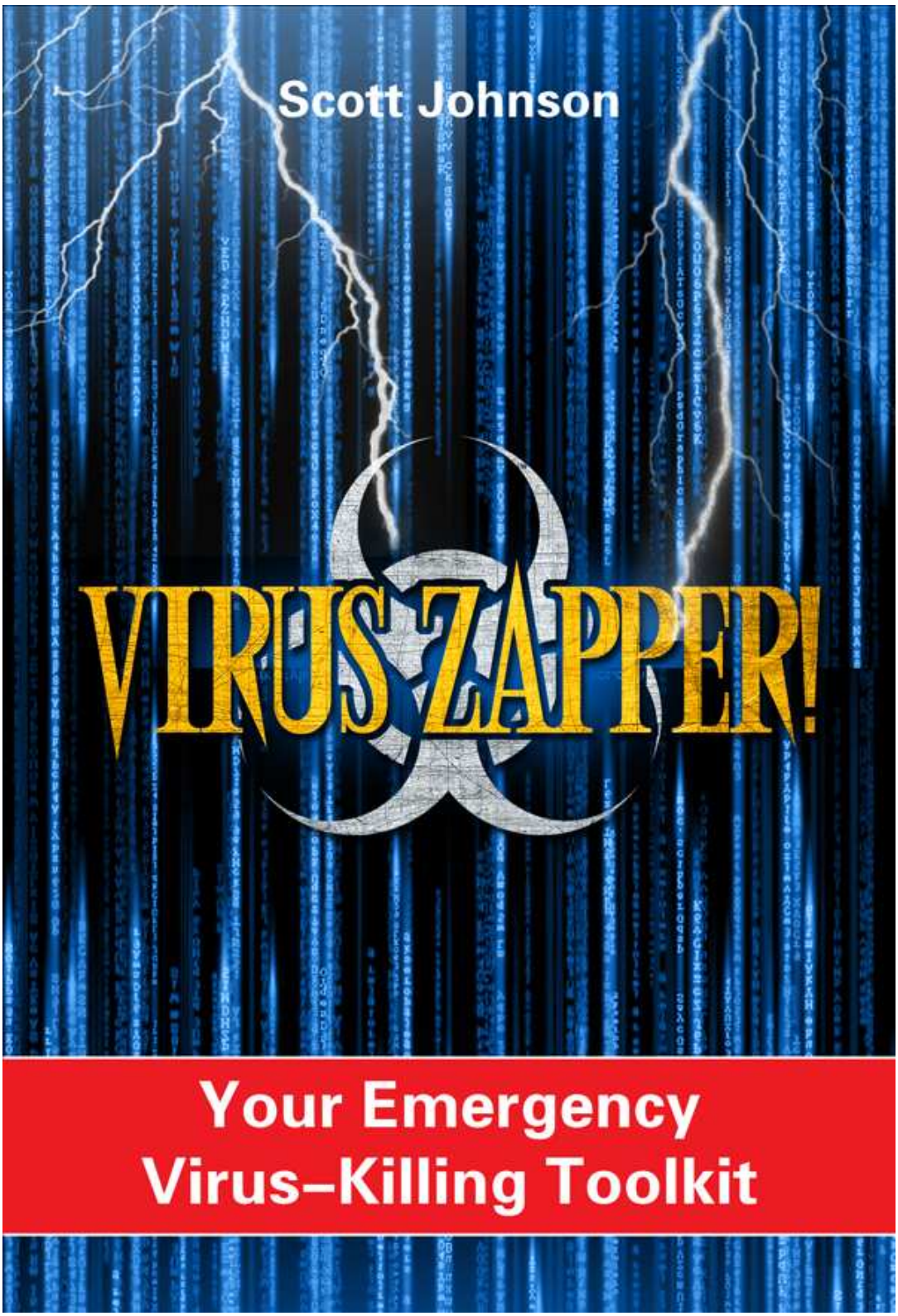
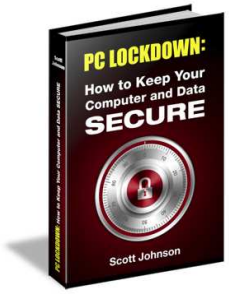


www.ComputerTutorFlorida.com

Disclaimer and Legal Notices: This report is for informational purposes only and the author, his agents, heirs, and assignees do not accept any responsibility for any liabilities, actual or alleged, resulting from the use of this information. While every reasonable attempt has been made to verify the information contained in this eBook, the author and affiliates cannot assume any responsibilities for errors, inaccuracies or omissions, including omissions in transmission or reproduction. Any references to people, events, organizations, or business entities are for educational and illustrative purposes only, and no intent to falsely characterize, recommend, disparage, or injure is intended and should be so construed. Any results stated or implied are consistent with general results, but this means results can and will vary.

You're invited!



If you are concerned about keeping your computer and your data free from virus and spyware infection, and you want to keep up with the latest security procedures that the average person needs to do, you should be on my list. I send out a free email newsletter every Monday morning with tips and tricks on how to use your computer more easily and effectively – including lots of information about privacy and security. By being on my list, you will also get my computer security guide: ***PC Lockdown: How to Keep Your Computer and Data SECURE***. You can sign up at my site: http://ComputerTutorFlorida.com

Introduction

This guide is written for a specific situation: your computer seems to have acquired a virus or some type of spyware, and you need to know what to do to get things back to normal. You might have warnings coming up on your screen, or pop-up messages telling you that your hard drive is about to die, or other dire alerts.

I perform computer repairs such as this all the time. The procedures that I am about to describe are the steps that I would take if the computer were sitting right here in front of me. The things you need to do are really dependent on what exactly is happening, but there are lots of ways to defeat this problem and get things back to the way they were.

When you see something like this come up on your computer, there are 3 possibilities about what is going on:

1. A hoax – you have no problem, even though it looks like you do.
2. Spyware – your computer has acquired some program or toolbar that is causing problems or "alerts" or worse.
3. Virus – your computer is actually infected with a virus.

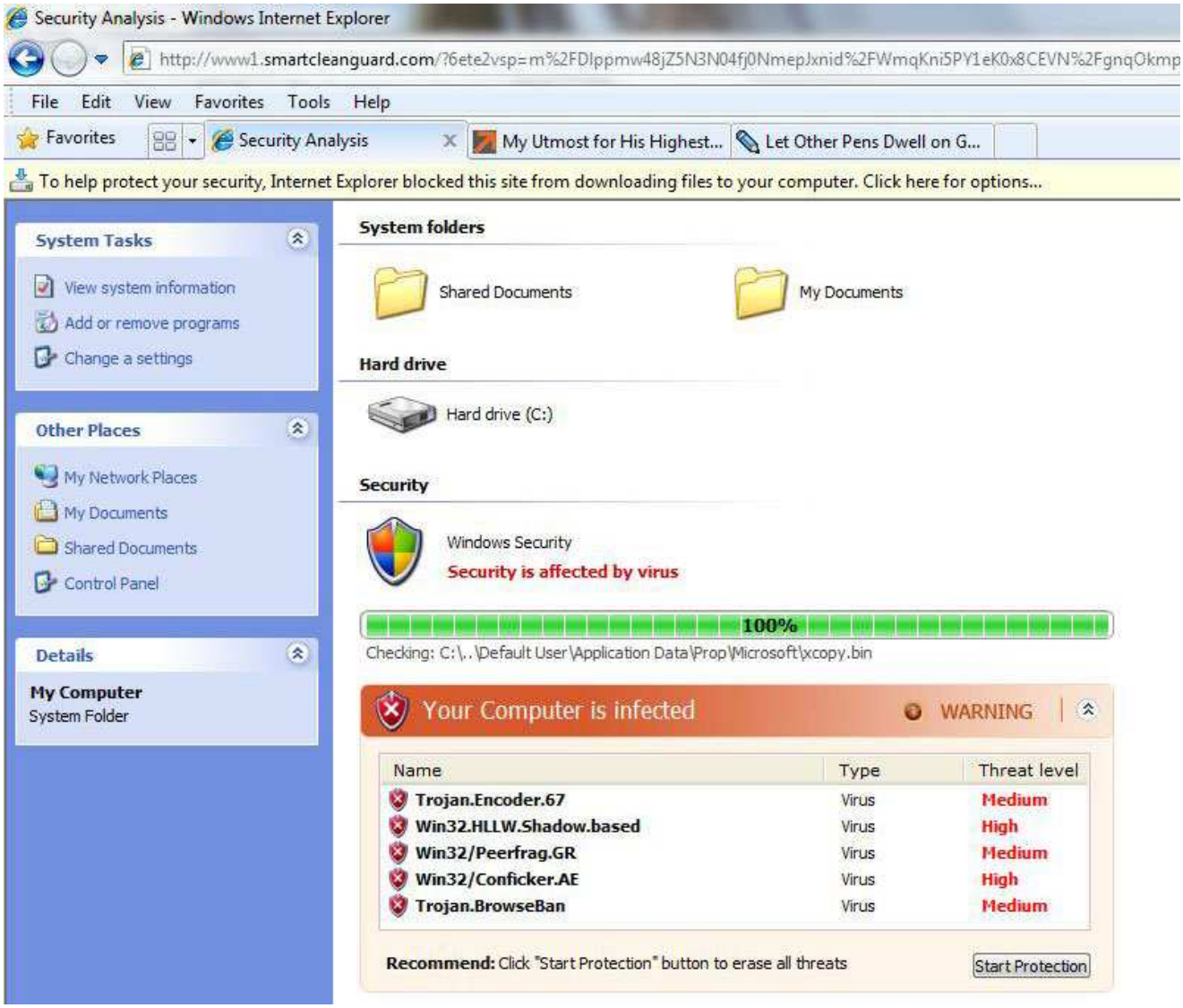
Fortunately, if you are running a good antivirus program and a good antispyware program, there's a good chance that you are okay. If you are not sure about how to secure your computer, I highly recommend my free guide: ***PC Lockdown: How to Keep Your Computer and Data SECURE***. You can get it here: http://computertutorflorida.com/?p=3006

The action you should take is dependent on what is happening. We'll take them step by step in the following pages.

FIRST: take a deep breath.
This is not the end of the world.
I fix these things all the time and we'll get through it.

Step 1: Determine if you are merely seeing a web page

You might not be seeing a warning window on your screen. You might just be looking at a website that is designed to LOOK like a warning. Here is an example:



That looks pretty serious, right? Warnings, threats, infections…but it is all a FAKE. This is nothing more than a web page. This web page was created by some scammer who wants to infect your computer with his malicious software. It's pretty clever, because it is designed to look exactly like Windows Explorer, a folder you see on your Windows computer all the time.

This type of web page is created with the idea of getting 2 things to happen:

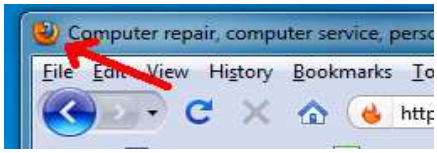
1. It wants to generate a feeling of panic in the user. That's why all of the warnings and alerts are there. It wants you to feel like "I need to fix this problem, NOW, before anything worse can happen!"

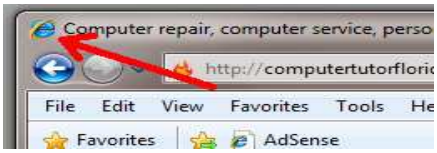
2. When you are all worked up and stressed about what to do, it wants you to see what could be the solution – the little button in the bottom right corner that says "Start protection". It even says that clicking on that button will "erase all threats".

Unfortunately, many people will see this and go ahead and click that button. But that is when the real problems start. At that point you will be downloading and installing software on your computer, and it's not good. **So don't click it**.

How do you know if you are just looking at a web page instead of a real warning? You need to identify the computer window where it appears.

In the top left corner of the window there is an icon to tell you what program you are using to view that window. If you see the Firefox icon or the Internet Explorer icon in the top left, that means you are viewing a web page.





If you determine that you are only viewing a web page and not an actual warning window, the solution is simple: just click the Back button and don't go to that web page again.

To double check, after you leave that web page, do a scan with Malwarebytes and with Microsoft Security Essentials to make sure your computer is still clean.

Step 2: System Restore

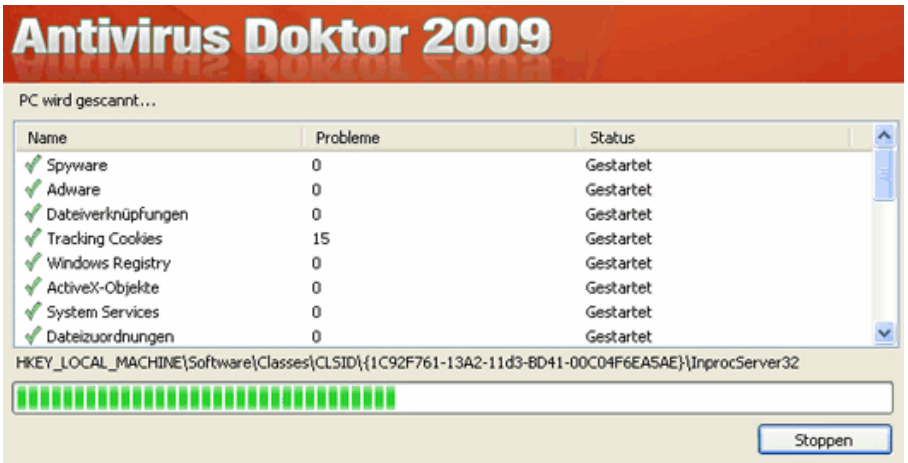
If you are not just viewing a fake web page, you could see "warnings" popping up on your screen telling you that you are infected. These can be in various forms:

- An alert in the System Tray in the lower right corner of the screen (or several alerts)
- A pop-up that appears right in the middle of your screen warning that you have lots of viruses/threats/infections and you need to take action
- Your background wallpaper might even change to a virus warning

When this happens, it is most commonly what is called a "rogue antivirus". In other words, it is a malicious program **acting** like an antivirus program. It is supposedly "doing its job" and alerting you to all of dozens or hundreds of threats that it has discovered on your computer.

In most cases, a rogue antivirus will refuse to be ignored. If you close the window, it will just reopen again in a few seconds. In fact, there could be multiple windows opening at the same time, and some or all of them block what you are trying to do, so you have to keep closing them. They are hoping that you get tired of closing them and finally just click on the "solution" button (that could say "Fix problems", "remove threats" or something else). **Don't click any buttons on these programs**.

Here are what some of them look like:



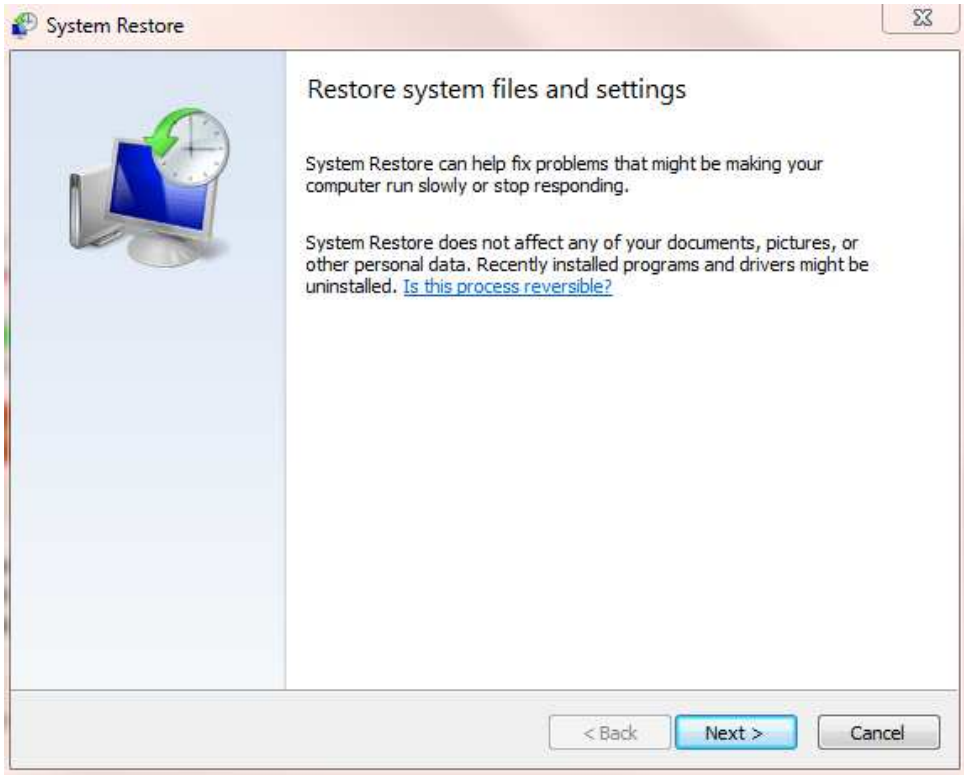
Sometimes they are easy to spot because of misspelled words or incorrect grammar. But if something like this pops up on your computer and you have never seen it before, it should make you suspicious anyway.

The first thing I recommend trying is System Restore. This means you will be taking your computer back to the state it was in before this problem popped up. If you suddenly noticed the popup warnings today when you were using your computer, you can probably safely assume that if you took it back to "yesterday", you should be okay. If you started seeing them a couple of days ago, you might want to take it back to a week earlier just to be safe. I try to take it back just far enough to be sure that it was before the problem started showing up.

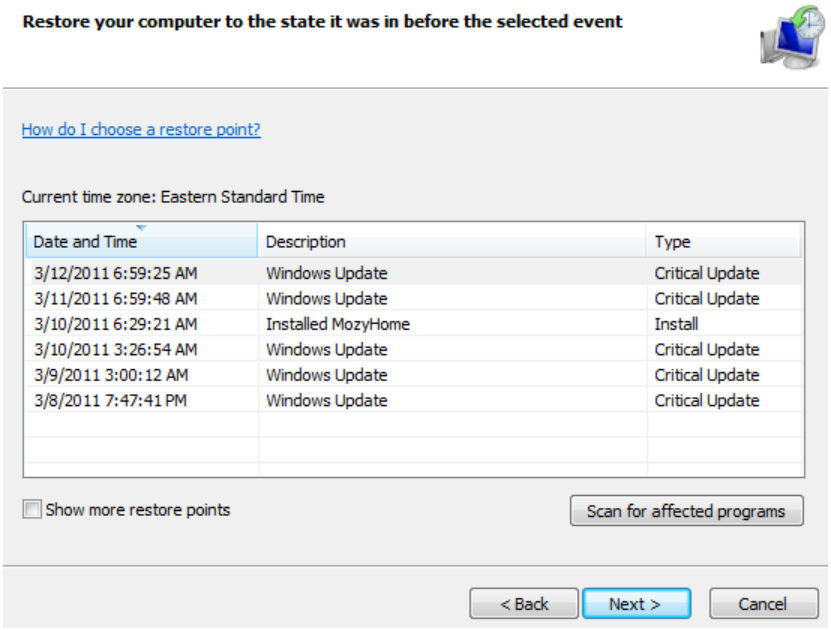
The procedure for System Restore is different depending on whether you are using Windows XP, Windows Vista, or Windows 7. We'll go through each one step by step.

System Restore for Windows 7:

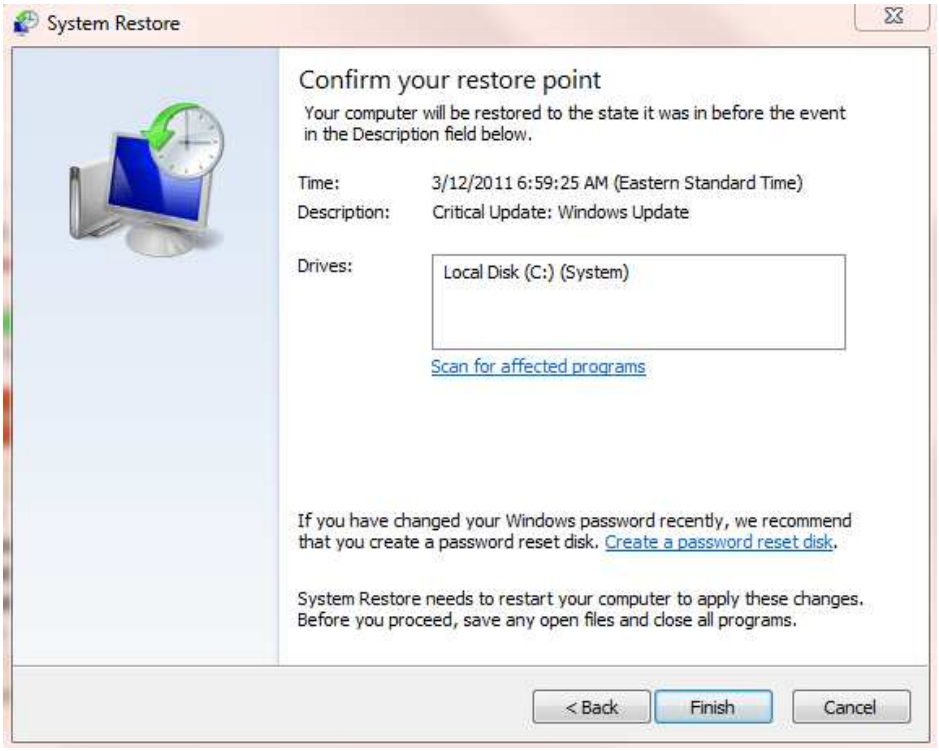
1. If you are using a laptop, make sure it is plugged into an outlet rather than running on battery. Click the MS logo in the bottom corner.
2. Click on All Programs
3. Click on Accessories
4. Click on System Tools
5. Click on System Restore
6. System Restore will open, and you will see a window that looks explains what System Restore will do. Just click Next.



7. On the next screen, you will see a list of dates, called “Restore Points”. The initial list will only go back a few days. If you need to go back to an earlier date than what is restored, check the box that says “Show more restore points”. Otherwise, choose a date and click Next:



8. The next window will confirm the Restore Point you chose. If that is correct, click Finish:



9. Your computer will go through the System Restore process, including doing a restart. Just let it complete this process (it shouldn't take more than about 10 or 15 minutes).

System Restore for Windows Vista:

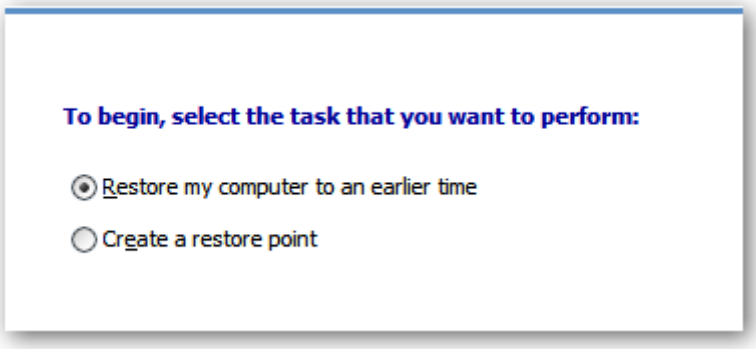
If your computer has Windows Vista for its operating system, you can essentially follow the instructions listed above for Windows 7. The actual screenshots might appear slightly different, but the overall procedure is just about identical.

System Restore for Windows XP:

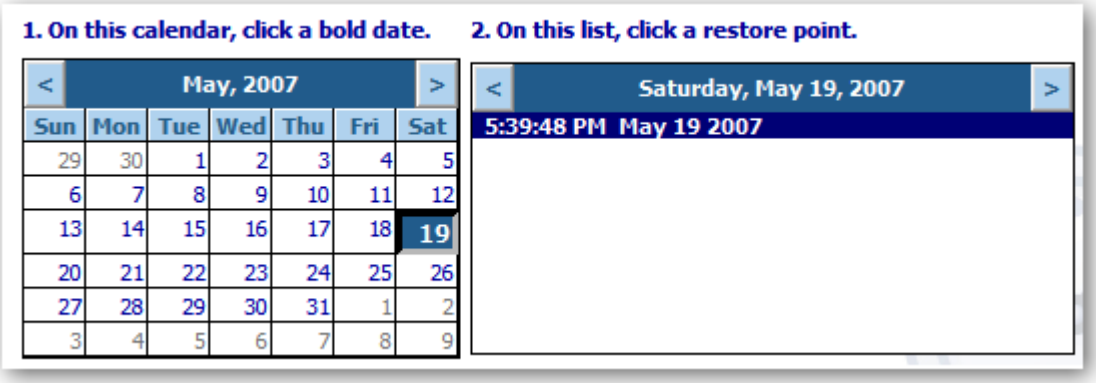
1. If you are using a laptop, make sure it is plugged into an outlet rather than running on battery. Click the MS logo in the bottom corner.
2. Click on All Programs
3. Click on Accessories
4. Click on System Tools

5. Click on System Restore

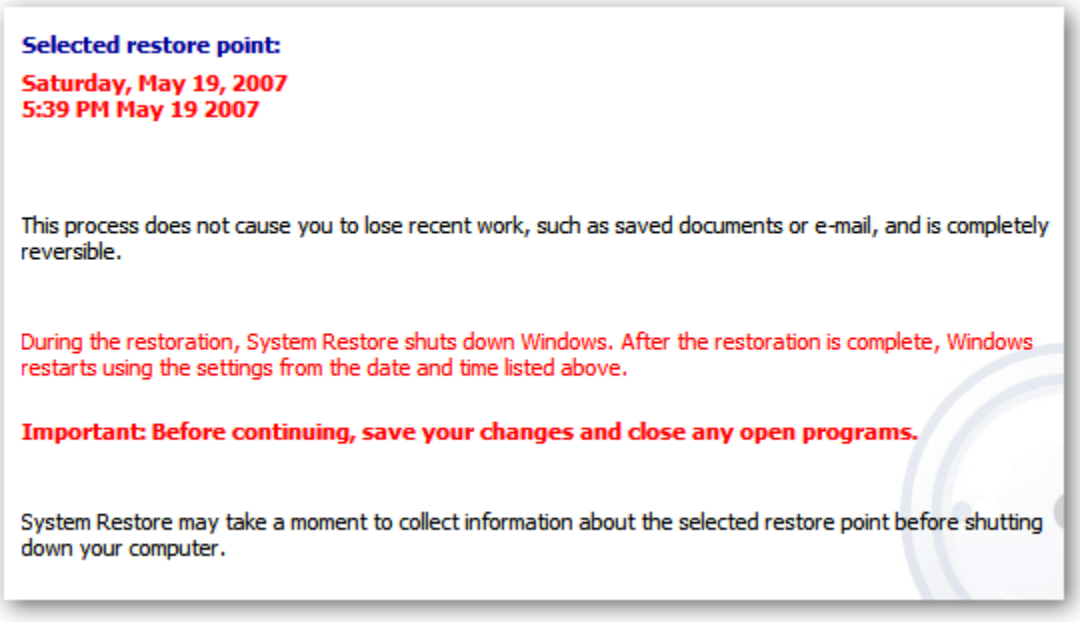
6. You will be given an option to either restore the computer to an earlier time, or to create a new restore point. You want to "restore my computer to an earlier time":



7. On the next screen, you will get a calendar that shows the dates of the current month. Some of those dates will be clickable, and some might not be. The ones that are clickable are the dates for which you have eligible restore points. If you need to go back earlier, you can choose the left arrow and go to the previous month. Otherwise, choose a date:



8. Now you will get one more screen, which will confirm your chosen restore point and explain what is about to happen:



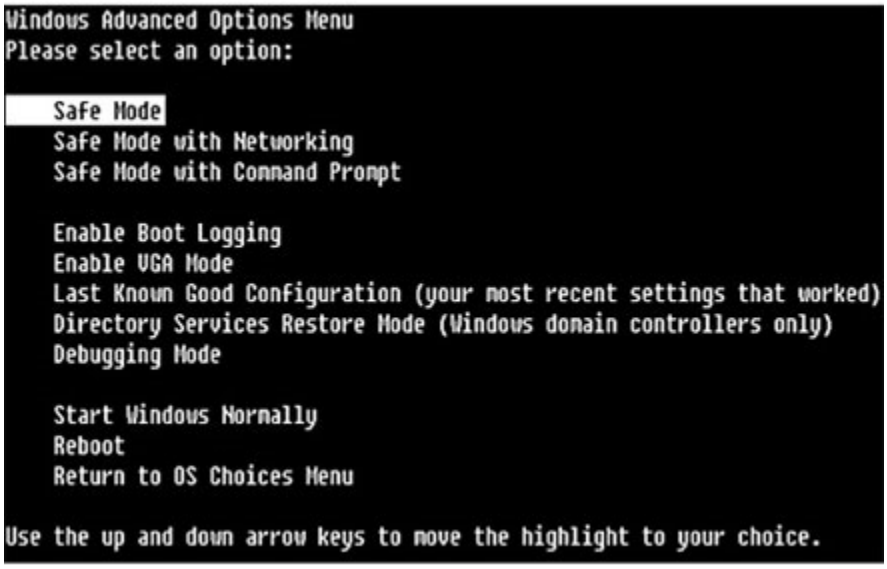
9. Go ahead with the restore process, and then just wait for it to complete. It will include a restart.

So now you have run System Restore and taken your computer back to an earlier point in time. In many cases, this will solve the problem and you won't see those pop-ups on your screen any more. Problem solved!

What if you can't run System Restore?

Some rogue antivirus programs are smart enough that they will prevent you from running System Restore (clever, huh?). In that case, you will need to run System Restore from Safe Mode. Here's how:

1. Turn off your computer and wait 10 seconds.
2. Turn on the computer, and as soon as you hit the Power button, start tapping the F8 key on your keyboard.
3. As the computer boots up, before it gets to the point of loading Windows, you will get a black screen that has some options. Use the arrow keys on your keyboard to move the selection up or down. When "Safe Mode" is highlighted, hit Enter:



The computer will continue to boot up, but things will look a little different. Your desktop icons will probably be larger, and they might not be in the same places as they were before.

However, in general, you can still use the computer the way you normally would. So, follow the instructions for System Restore for your version of Windows as listed above. The only difference now is that you are doing it in Safe Mode, which greatly increases your chances of success. The computer will go through the same restart process (except when it reboots this time it won't go back into Safe Mode – it will be in regular Windows mode).

Hopefully when the computer reboots and you get back to your desktop, you won't see those popups any more. Problem solved!

If System Restore didn't help, you could try running it again but take it back to an even earlier date. Otherwise, let's move on to the next section and try another option for fixing this problem.

Step 3: Run Malwarebytes

Malwarebytes is a great little tool for getting rid of spyware. I have used it for a long time and it does an excellent job. If you have been getting my newsletter for any length of time, you probably already have Malwarebytes installed on your computer (in fact, I recommend getting the paid version of Malwarebytes – http://bit.ly/jANr2).

If you don't have Malwarebytes, you can at least go and get the free version at www.malwarebytes.org. Download it, then double click on the file and install it.

With Malwarebytes installed, double click to run it and do a Quick Scan. This shouldn't usually take very long, maybe 20-30 minutes at the most. When it gets done, it will tell you if it found any threats. Whatever it finds, go ahead and have it remove them.

Then do a FULL scan with Malwarebytes (you can just run it on drive C when given the option). This one will take longer. It depends on how many files you have on your computer, but it could even go as long as an hour or two. Again, whatever it finds as a threat, allow it to remove. You might have to restart the computer as part of the removal process.

Removing whatever Malwarebytes finds will often solve the problem. Done!

What if you have Malwarebytes installed, but you can't run it?

That's a possibility. Some of the spyware programs assume that you will try to run Malwarebytes so they disable it ahead of time. Then when you try to run it, it won't run.

When that happens, you have a couple of options:

1. Start up the computer in Safe Mode, and run Malwarebytes from Safe Mode.
2. Change the Malwarebytes file name. Believe it or not, this sometimes works. The spyware program is set to not allow a program called "Malwarebytes.exe" to run, but if you just change the file name to "malwarebytes1.exe" it will be able to run. Note: you cannot just change the name of the desktop shortcut. You have to change the name of the actual file. You can find that by going to Computer – C Drive – Program Files (or Program Files x86) – Malwarebytes Anti-Malware. In that

folder, look for a file with the Malwarebytes logo. Called MBAM. It might be displayed as just "mbam", or it might say "mbam.exe". When you find it, do a right-click on the file name and choose "Rename". Then change the name by adding something to it. If the ".exe" was displayed to start with, be sure to leave it there. Once the file name has been changed, double click on the newly-named file to run it. You might be surprised to see Malwarebytes start up and run fine! When that happens, go ahead with the Quick scan and follow that with the Full scan, based on the instructions listed above about removing whatever threats are found.

What if Malwarebytes still won't run?

That happens sometimes. Don't worry, we still have options and a very good chance of fixing this. If Malwarebytes won't run after all of the above has been tried, it's time to move on to the next step.

Step 5: Super Antispyware

Super AntiSpyware is another great tool in my toolbox to fight and defeat spyware and viruses. In a lot of ways, it is pretty similar to Malwarebytes. There is a free version and a paid version. However, Super AntiSpyware offers something else called a "Portable Version" (I'll cover that in a few minutes). In any event, your next step to solving your problem is to run Super AntiSpyware.

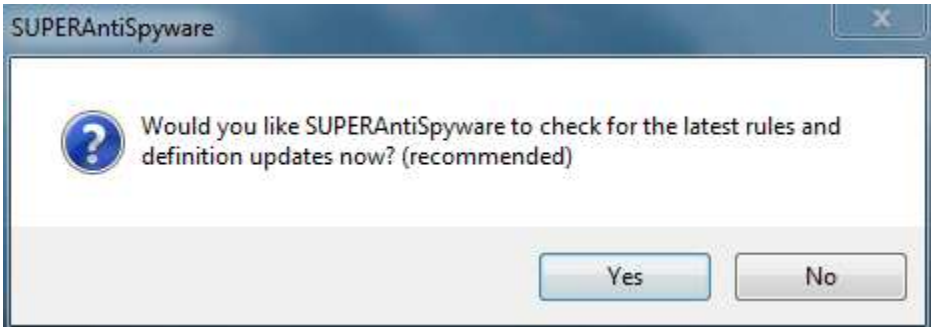
You can get the free version (which is all you need at the moment) at www.superantispyware.com. Click on the big red button that says "Free Edition download". The download will begin. Then, double click on the downloaded file to install the program.

During the installation, you will be prompted to ender a Product Registration code. This is only if you purchased the Professional version. If you leave it blank, the Free version will be installed:

Just continue to click “Next” to complete the installation, then click “Finished”.

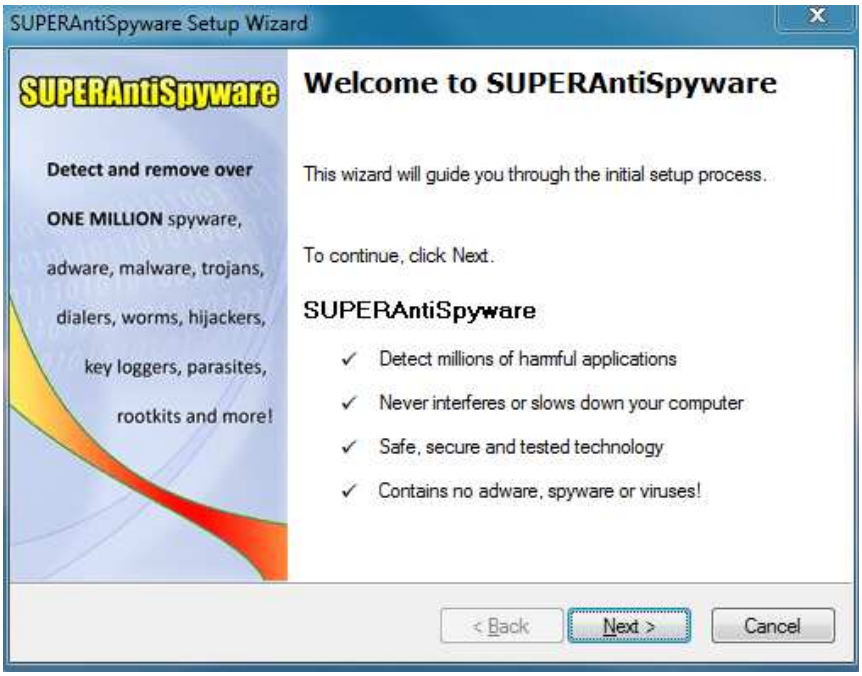
Next, choose the default language you prefer.

Now SuperAntiSpyware will want to check for updated definitions. Click Yes:



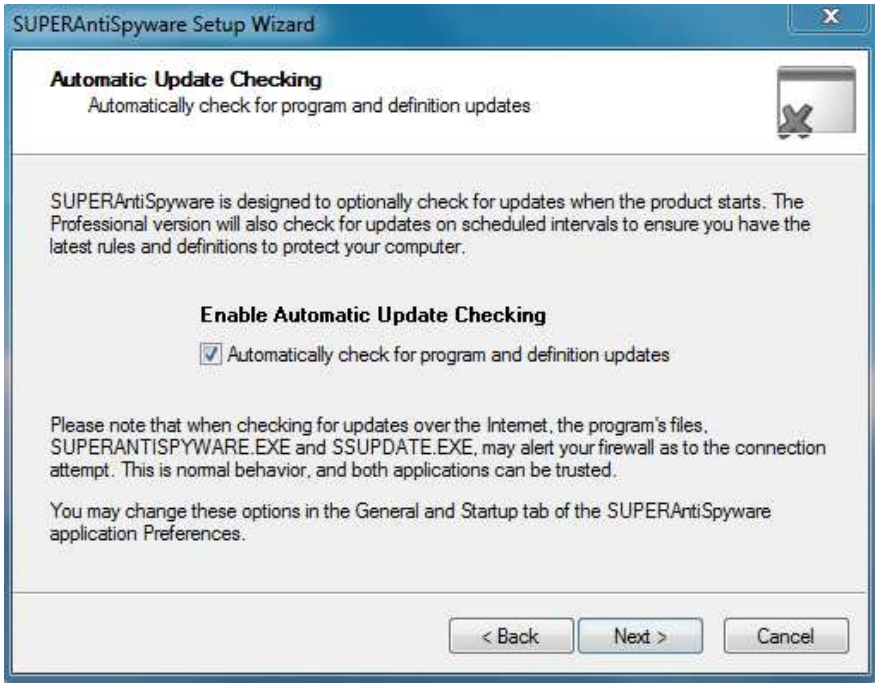
The program will update itself with the latest information:

When that’s done, it’s time to get down to business. Click Next:

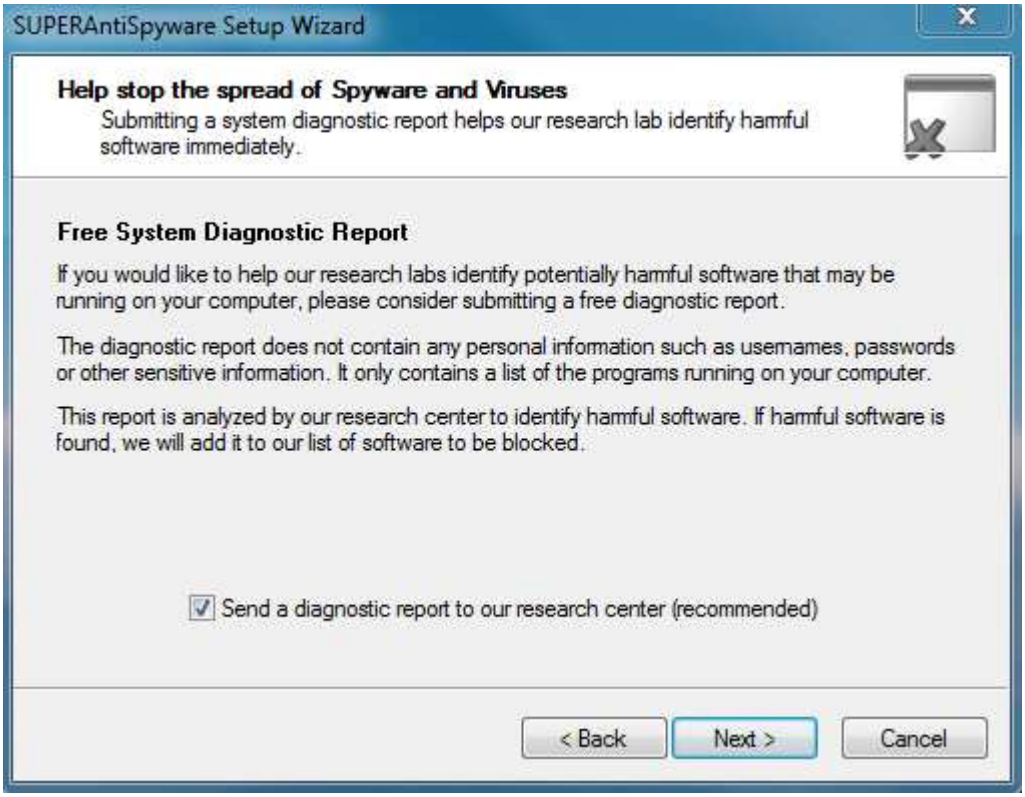


It's up to you if you want to submit your email address to them for notification about future updates. You can click Next without doing so:

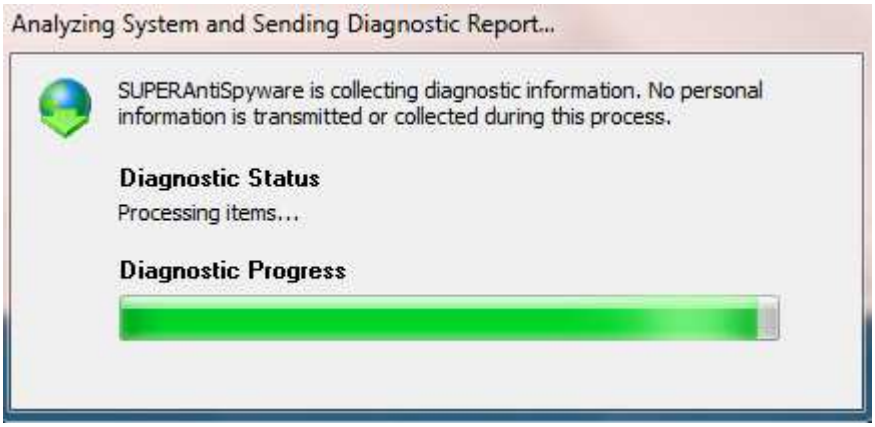
I do recommend you leave the box checked on the next screen, for Automatic Update Checking. This stuff changes all the time, and the program has to be updated with the changes in order to remain as effective as possible. So leave that checked and click Next:



I also like to opt to send a diagnostic report when something is found. After all, they are giving you the program for free; why not help them out a bit with a little report (it's totally anonymous anyway). So leave that checked and click Next:



Now the program will run the free System Diagnostic Report and you will see the progress bar as it works (just takes a minute):

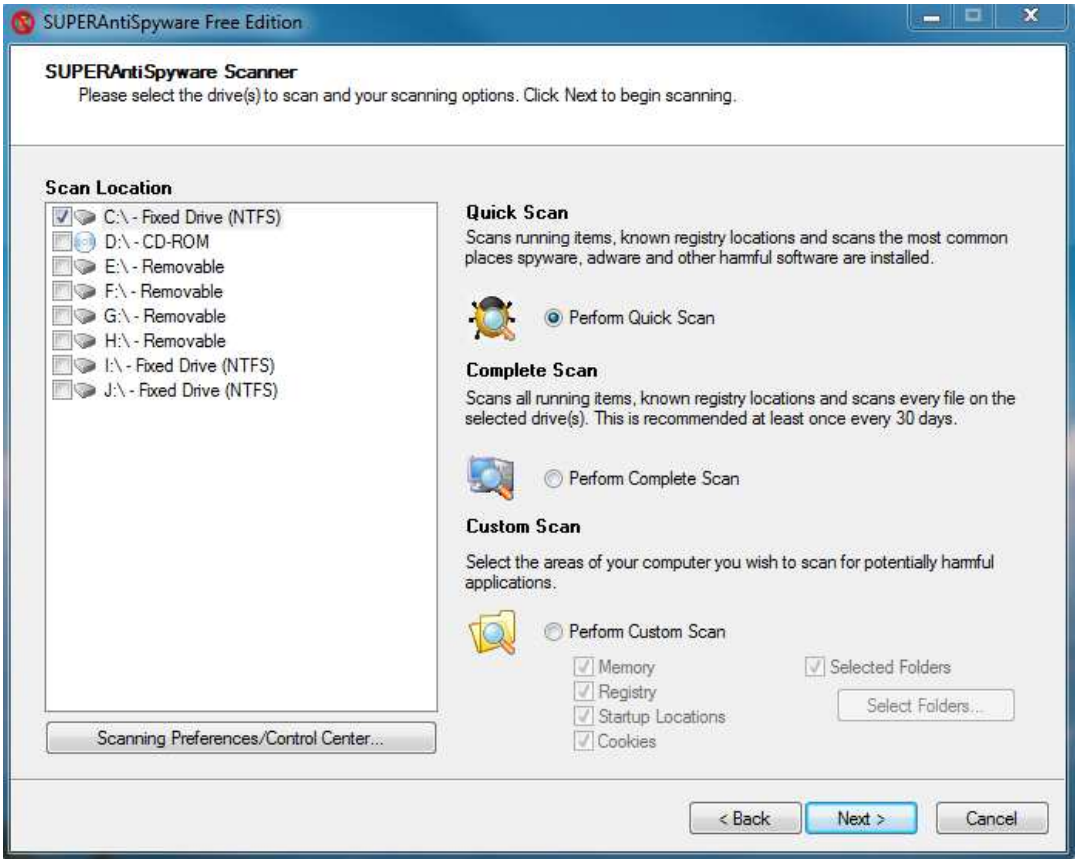


At this point, the Setup portion is complete. Click Finish.

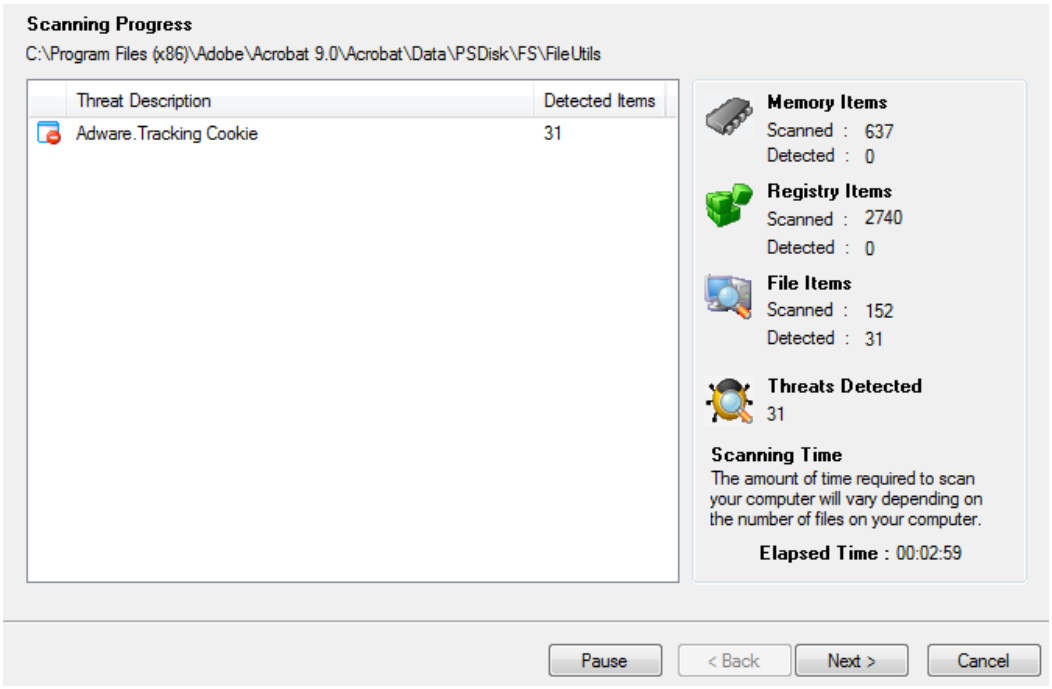
The next thing you will see is an option to protect your home page. One type of spyware is called a "browser hijacker". It will change your home page to a different website, such as a casino site or a porn site. SuperAntiSpyware can protect against that, which is good. Click on "Protect home page".

Now we are at the main menu. You can see there are a few options, but the only one you want to bother with right now is the button that says "Scan your computer".

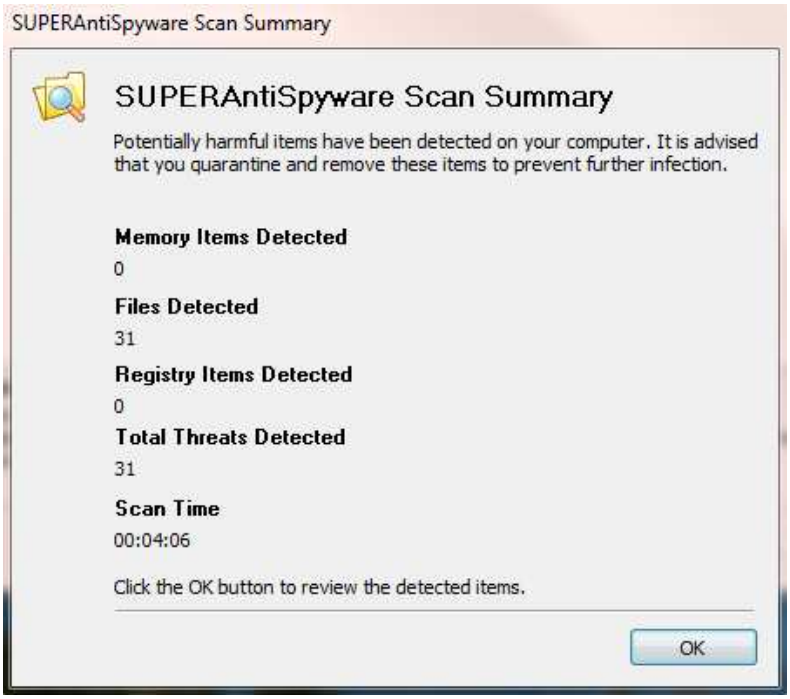
The next screen will present you with a few options. For Scan Location, just check drive C (assuming that is your main hard drive). In most cases you don't need to scan the other drives. Also, check the button that says "Perform Quick Scan". We'll start with the Quick Scan like we did with Malwarebytes. Click Next.



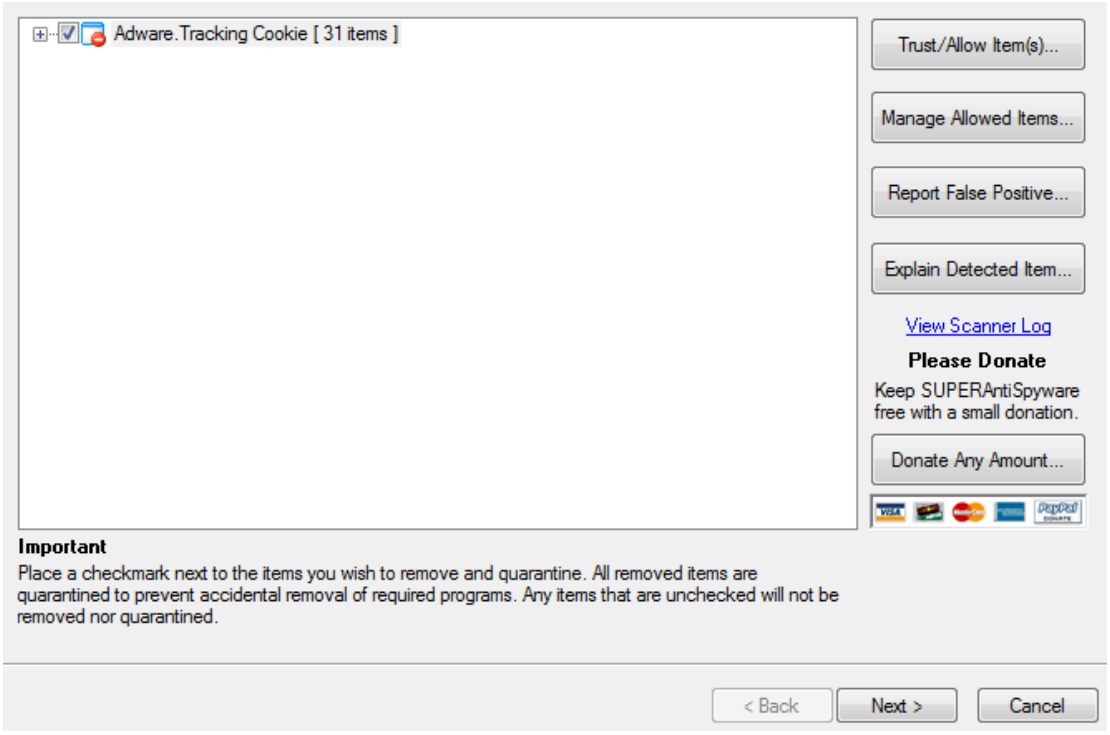
You can watch as the program scans the files in your computer. When the scan is complete, click Next. Just like with Malwarebytes, it's good to allow it to remove whatever it finds.



Here is what the Summary screen looks like when finished:



When you click OK, you will see a list of what was found, along with a checkmark next to each item. Leave the checkmarks there and click Next:



The items will be quarantined and removed. When you click Finish, you will be taken back to the main SuperAntiSpyware menu.

It would be a good idea to do a computer restart now. When the computer reboots back to the desktop, there's a good chance your problem is solved. However, at this point, I recommend going back and repeating Step 3 – run Malwarebytes again. Malwarebytes will often find threats that SuperAntiSpyware does not find, and vice versa. Double team the problem to have the best chance of solving it.

What if you can't run SuperAntiSpyware?

In some cases, the malicious software will prevent you from running SuperAntiSpyware. In that case, restart the computer in Safe Mode and try running it again.

What if you can't even install SuperAntiSpyware?

With this program, we have another option. On the SuperAntiSpyware website you might remember seeing an option called "Portable version". This is a version that doesn't require installation. You can run it from a USB flash drive.

You might need to get this version from another (uninfected) computer. Go to the SuperAntiSpyware website (www.superantispyware.com) and click on the button that says "Portable Version download":

The next screen will list nice, step-by-step instructions for you to follow in order to run the SuperAntiSpyware from a flash drive. I will copy the instructions here anyway, so you have them as part of this guide:

1. Download the Scanner

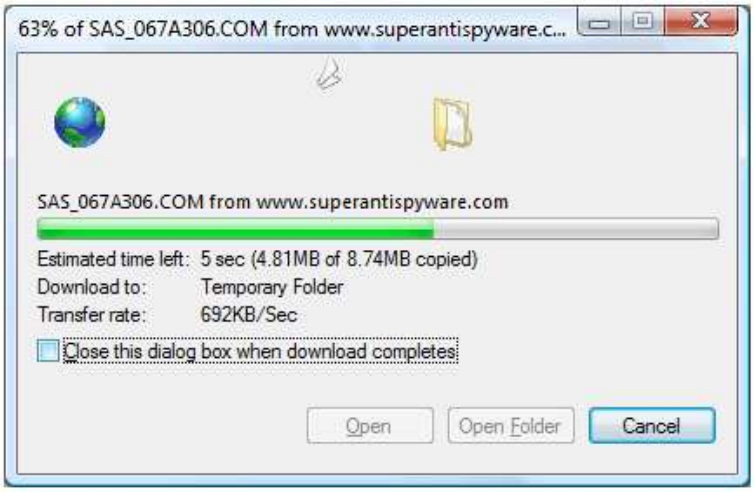
Click the button to the right to start the scanner download process.

2. Download the Scanner

Click Click the **SAVE** button when prompted. If you are using a browser other than Internet Explorer then prompt may be different.

3. Wait for the Scanner to Download

The scanner will download in just a few seconds.



4. Copy the Scanner to a USB/CD or other media to use on the infected system.

Copy the scanner to the media of your choice so you can run it on the infected system.

Please note : The scanner is saved under a random filename so that malware infections won't block the scanner.

After running the scan from the flash drive, restart the computer. Has the problem been solved? Great! Now go back to step 3 and see if you can run a Malwarebytes scan as well, to be doubly sure your computer is no longer infected.

Step 6: Microsoft Security Essentials

Microsoft Security Essentials is the antivirus program that I use and recommend. It's free, and it's easy to install and use. You can get it at www.microsoft.com/security_essentials.

Install the program, then allow it to get the latest updates (it will do this automatically as one of the last steps of the installation process). Then, MSE will do a scan of your computer to find any viruses that may be lurking there. Just like with the other programs we have used, whatever threats or viruses are found, have the program remove them.

If necessary, you can also try running Microsoft Security Essentials in Safe Mode.

What's next?

Chances are really good that your virus or spyware problem is now solved. **Good job!**

Here are a few tips that may help you avoid running into this again:

- If you install a program on your computer, watch for the **toolbars** that are sometimes installed by default. UN-check them so that they don't get installed. They can bring spyware with them.
- Keep your web browser(s) and your Windows installation updated.
- Don't visit "bad neighborhoods" on the web – sites that offer free screensavers, free streaming of movies that aren't even released on DVD yet, free music by major artists, etc. Getting stuff from those sites is asking for trouble!

I hope this guide has been helpful. And I hope you don't need to use it again! If you are in need of assistance that is beyond the scope of this guide, feel free to contact me through my website and arrange for some professional assistance.

Scott