OOOPS I answered wrong to a bogus virus alert! (Spring 2008)

So how did this get on my PC

Unfortunately, due to the nature of computer virus infections, antivirus and antispyware programs will not be lagging behind when new threats appear. It is also true that the balance between security and the ability for operating systems to deliver a workable solution leaves the user ultimately in charge. That is to say that a user answering a pop-up in the wrong manner will bypass security settings, PC firewalls, antivirus, and antispyware programs. The same line of logic can be applied to corporate firewalls and spam filters. Since security software has become more effective at e-mail security, most PC's are compromised by careless and reckless Internet use.

The ultimate lure is social in nature. Regardless of weather through e-mail, social programs, or word of mouth, "cool" video's, pictures, and sites draw visitors. Unfortunately, a number of these sites contain viruses and spyware. The latest more successful of these launch a popup that announces that your PC is infected with one or more viruses. One of these popup windows looks very much like a Microsoft warning. It then urges that the user remove the infection. As soon as the user agrees, the spyware is installed. It is often a Trojan or worm that then links back to a web page and disables security measures on the PC. This can even include disabling the Task Manager (Ctrl+Alt+Del), thus hindering the user's ability to stop destructive programs that are running. The infection then proceeds to allow or even invite other malware to infect the PC, sort of a malware kegger going on. Some of the software will even add some of the virus locations to Antivirus exception lists.

The most likely sites to infect your PC are pornographic in nature, often of the nude celebrity variety. Next are sites that install cute cursors, funky wall paper, and the like. In any event, none of these sites are a necessary browser destination to conduct daily business or to store and maintain important information.

How can one protect oneself?

Since PC's contain sensitive information and personal property (i.e. pictures, accounting and contact information, etc.) it is important that users treat PC's that are used for work, banking, and important information storage with the proper respect. A compromised PC can easily send sensitive information to a web connected server and be used for fraudulent purposes. It is not sufficient to rely on security programs and devices alone. It is imperative for users to be vigilant and not agree to any popup windows they did not request. Close any suspicious windows as soon as they appear. It would be best to avoid any suspicious websites. "*McAfee Site Advisor*" is a product that allows you to judge a web site before you go to it. If you end up at a site that is dangerous and get advised thereof, leave the site immediately and delete all Internet files. Keep your security software and operating system up to date. Back up your data. So which is the best product? The major three are Norton Security Suite, McAfee, and Microsoft Live One Care. As noted above, they are not all perfect. For the home user, Microsoft One Care is product that forces the user to update their operating system, clean and maintain their file system, backup information, and provides good malware protection. But it does not fix everything either but allows you to regain some control of your computer.

So how to get rid of the infection.

This assumes that you have unwittingly launched a very nasty Smitfraud program that is falsely reporting "worm.win32.netbooster" as the infection. If you have not done so, regain some control over your PC. If you cannot properly access the Internet, launch the Task Manager (Ctrl+Alt+Del), or Manage your Computer ([Start], right click [My Computer], choose [Manage]), you will need to install an anti-malware program from a disk. The recent winner in that department was One Care. Once One Care removes the infection that prevents you from properly accessing the web etc. please follow these steps. DO NOT BUY THE ANTISPYWARE PROGRAM THAT IS BEING ADVERTISED ON YOUR WALLPAPER AND IN THE POPUPS. The malware is actually trying to entice you to do so. Follow these steps:

1. Download and install the Smitfraudfix tool from http://siri.urz.free.fr/Fix/SmitfraudFix.exe
2. Update your antivirus software definitions.
3. Start the PC in Safe Mode
4. For Windows Xp, restart your computer and start pressing the F8 key on your keyboard.
5. On a computer that is configured for booting to multiple operating systems, you can press the F8 key when the Boot Menu appears.
6. Select an option when the **Windows Advanced Options** menu appears, and then press ENTER.
7. When the **Boot** menu appears again, and the words "Safe Mode" appear in blue at the bottom, select the installation that you want to start, and then press ENTER.

8. Run Smitfraudfix first after you start your operating system is in safe mode. Follow the instructions carefully for Smitfraudfix.
9. Run bitdefender and allow it to quarantine any suspect file it finds
10. Reboot in normal mode. Run your antivirus software and allow it to quarantine whatever it finds.
11. Run the Bit Defender online scan (no download necessary)at http://www.bitdefender.com/scan8/ie.html and allow it to quarantine whatever it finds.
12. If the problem does not disappear, you may have to download and run RogueRemover at http://www.malwarebytes.org/rogueremover.php . Select "Scan" and follow the steps indicated.
13. If you do not have a current antispyware program, http://www.superantispyware.com has an antispyware program that is free.
14. YOU SHOULD REALLY NOT RUN MULTIPLE ANTISPYWARE OR ANTIVIRUS PROGRAMS! Once the infection has been removed, the additional programs should be uninstalled.
15. Continue to follow-up with Live OneCare if you desire. You should also keep anti-virus software up-to-date and scan regularly.
16. Hopefully it will be working well again after the infection is removed. Be sure to restore the settings which the Smitfraud program altered. Smitfraud apps are quite nasty, and it may take a while to remove all traces.

So far we do not have a better or easier way to remove this type of infection. If you have sensitive information or conducted online banking from the previously infected PC, check that the information has not been compromised. Check bank and credit card statement for any irregularities.