

Who HiJacked My Computer?!?!?!?



Richard W. Schierer
March 2010

If you surf or work on the internet or receive

internet email (and who doesn't these days), then you run the risk of having your computer infected by a rouge antivirus programs. Several of my clients have been infected in one way or another by pop-ups claiming that files on your PC are infected, click here to download antivirus program. If you click NO, the pop-ups continue. Internet Explorer might be disabled, you can't access Windows Update site, nor run your present antivirus, and when you access troubleshooting utilities, they respond back with cryptic messages.

Left to the novice or uninformed user, they fall for the gimmick and install the rouge antivirus program that asks for your credit card number and states it will only charge you \$39.99 (better check that charge when it comes). Once the program is installed it continues to drive you crazy with the pop-ups making the computer impossible to use. Usually once the rouge program is installed, it is nearly impossible for the untrained to remove. Some think they find the program and uninstall it only to reboot and find the program has returned it those irritating pop-ups!

To give you an idea of what a trained professional has to do to 'try to' return the PC to working condition, I have included a How-To from this website

<http://ezinearticles.com/?Remove-Sysguard->

[--How-to-Conduct-a-Sysguard.exe-Removal-Procedure&id=2242313](http://ezinearticles.com/?Remove-Sysguard-)

Here is the article in full:

Need to remove Sysguard? You aren't the only one, I can promise you of that. This virus has been taking the internet by storm lately. If you feel you may be infected, I would highly recommend you conduct a Sysguard removal as soon as possible. The last thing you want to do is allow this virus to fester on your computer.

Sysguard.exe is a process found in quite a few different rouge antivirus programs. A rogue antivirus program is essentially a fake malware remover. How it works is first it sneaks on your computer typically as a trojan. This could have been from visiting a malicious website, installing infected software, or using a P2P network to download files. Once on your system it will infect the Windows registry and begin to create pop up add with "Warning!" or "DANGER" type messages.

Clicking on these pop up ads will probably start the fake malware scan. After the scan the virus will attempt to frighten you into installing the software. If you are not already aware, THIS IS A TRAP. Do not give these folks your credit card number.

In fact leaving the virus on your system can make you a victim of identity fraud. Viruses like Sysguard have the capability to use spyware and keyloggers to record sensitive information on your computer.

Conduct a Sysguard.exe Removal

- Remove all Sysguard related processes (any malicious EXE files)
 - Remove any associated DLL files (Dynamic Link Library)
 - Remove any dangerous .lnk files associated with the virus
 - Go into the registry, locate and remove dangerous files in following directories
HKEY_LOCAL_MACHINE
HKEY_CURRENT_USER
- Remember that you must remove all remnants of the malware before you reboot. Otherwise*

the virus will simply generate the next time you boot up. These removal instructions are geared towards computer experts who know how to properly identify dangerous files. Deleting the wrong registry files can serous damage if you don't know what you are doing. Fortunately there is a way to remove Sysguard if you a not a computer expert. With the right removal tool you can eliminate the virus in minutes. I have found one in particular that also offers real time protection to fight future threats.

>>>>

I would not recommend the un-initiated to try these steps as one wrong move and you may make your PC inoperable! (Not that it was running so well before this!)

Sometimes these steps don't work. And it is easier to backup your data to an external source and then wipe the PC and reinstall the Operating System (XP/Vista) and all the applications.

This is a fairly lengthy process, usually taking 2-3 days (minimal) with the PC being removed off-site.

Bottom line is, be careful of what emails you open (even from friends and known associates) or websites you visit.



Richard W. Schierer

makemytechnologysimple.com

631-375-4512