Scareware Contamination?

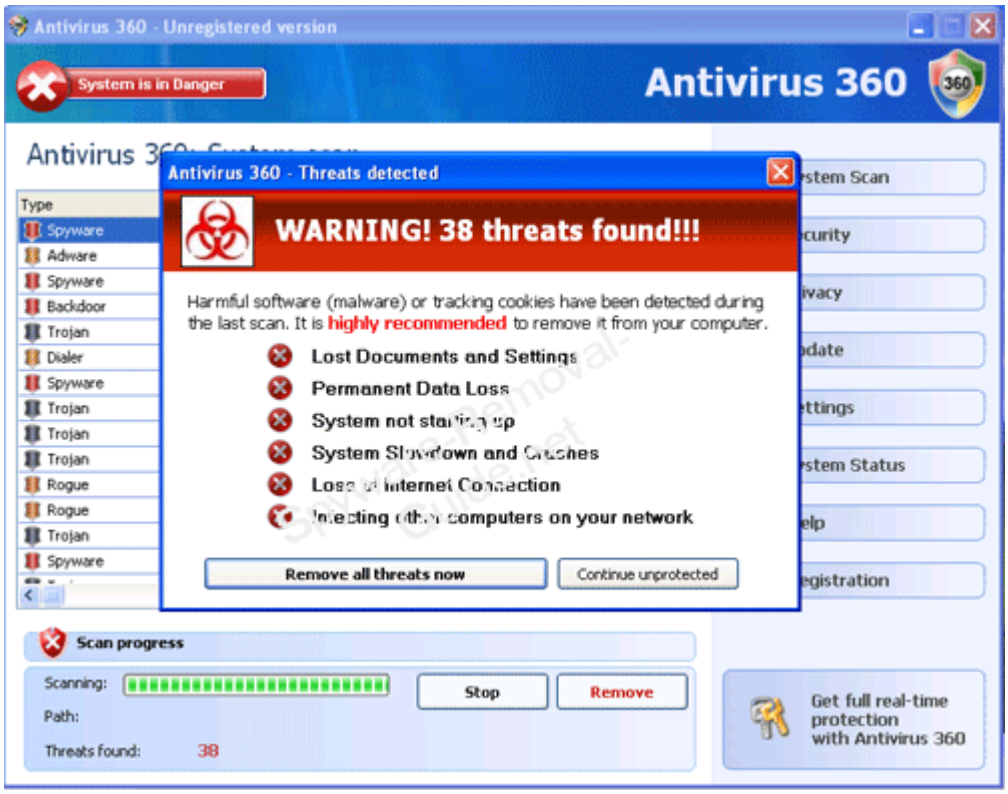
What is a computer virus? "*Computer viruses are small software programs that are designed to spread from one computer to another and to interfere with computer operation. A virus might corrupt or delete data on your computer, use your e-mail program to spread itself to other computers, or even erase everything on your hard disk".*

What is spyware? "*Spyware is a general term used to describe software that performs certain behaviors such as advertising, collecting personal information, or changing the configuration of your computer, generally without appropriately obtaining your consent first*."

What is Rogue Adware/Scareware? These programs fall into two categories:

1. They claim to remove spyware, but actually install it (and usually charge you for their product!)
2. They've stolen their code from another vendor (most notably, from Spybot S&D. This is somewhat funny, as Spybot S&D is no longer, in my opinion, a very effective product). These are some of the most annoying programs since they will constantly pop up warnings about your "infection" encouraging you to purchase their protection, while they are actually what you need to be protected from! Often you will find you cannot even surf the internet at all since they will constantly re-route you to their website, hoping you will give them your credit card information.

Although your problem could actually be caused by viruses or spyware, we are seeing a predominant number of computers infected with rogue adware or scareware. If you see pop ups that look similar to these images, you probably are infected with a rogue adware or scareware program yourself:



The name displayed by the program might be different (i.e., Antivirus 2007, Antivirus 2008, Antivirus XP,

Antivirus 360, etc.) but they are all pretty much the same infection. They all look very legitimate and will appear to actually be scanning your system while displaying the results of dozens or even hundreds of infections. If you see this type of pop up on your computer, don't panic. It doesn't matter what button you click or what you may have already done. No matter what you do, your computer is already infected. This happens because you do not have adequate protection software installed, it has not been updated daily or you ignored or did not notice the warnings the program displayed. Since there are several hundred new viruses and spyware programs introduced every month, keeping your protection up to date is critical! And you must also download and install all Microsoft Critical Updates every day.

Once the malware is installed and running on your system, it will usually prevent you from installing any new anti-malware software, updating any anti-malware program you already have installed, or navigating to any website where you can perform an online scan. **No matter what it may tell you, NEVER EVER GIVE THEM YOUR CREDIT CARD NUMBER! The program will try to take you to a website to "activate the program". You will be asked to enter your credit card information to activate or register the program. If you do this, you will be charged anywhere from $75 to $150 and nothing else will happen to your computer! You will continue to be infected and your computer will still be unusable even after you have paid the required activation fee! The companies who are distributing this software are making upwards of $20,000 a day from people who give them the credit card information. If you have done this yourself, contact your credit card company immediately and try to get the charges reversed.**

Virus / Spyware / Adware Removal Process

If your infection is caused by a simple virus that has been around for a long time, it can probably be removed quickly and relatively effectively. I say relatively since there is never any guarantee that any virus/spyware/adware has been completely removed from your system. ANYONE who tells you differently is absolutely wrong! There are simply too many malware programs and variations in existence for any one removal program to be 100% effective. Years ago when these programs were not so prevalent or powerful, we could eliminate 99% of them within a couple of hours using 3 or 4 utility programs. Now that process takes 6 or 7 utility programs and 4 to 6 hours and is almost never totally effective! And we must constantly purchase new utility programs to keep up with the crooks! If you are using free programs such as Spybot S&D or similar programs, you simply do not have adequate protection. We strongly recommend you purchase AVG from Grisoft.

No matter how long we work to remove the malware from your system, we cannot give you any level of assurance that your system is totally clean and free of all malware unless you allow us to backup your data, totally erase and reformat your hard disk drive and reinstall your operating system and all your programs. We generally charge for 1.5 to 2 hours for this entire process and not only will your malware problem be totally eliminated, your computer will run better than it did when it was brand new, guaranteed! And the process can be completed overnight in most cases so your computer will not be out of service for more than a couple of hours. Keep in mind, you must have the original disks for any special programs you are using (i.e., Microsoft Word, Outlook, Excel, Quickbooks, etc.) since only data files can be restored. And if your computer is not a Dell, you might need to have the system recovery CD's that came with your computer (unless the recovery program is stored on a hidden partition on your hard disk drive). If your computer is a Dell, we will not need any CD's from you at all.

How do you prevent this from happening again?

1. Do not allow any file sharing programs such as Limewire, Bittorrent, etc. to be installed or used on your computer.
2. Never download or install any type of free program on your computer unless you are absolutely certain it is from a legitimate company such as Microsoft.
3. Never download or install any free screensavers or desktop backgrounds unless you are absolutely

certain it is from a legitimate company such as Microsoft.

4. Never allow anyone to use your computer to browse websites that are potentially hazardous, i.e. porn sites, etc.
5. If you suspect a scareware program such as that pictured above has been launched on your computer, DO NOT CLICK ON ANYTHING! Turn your computer off immediately, start it back up and run a full scan immediately. If you click on anything being displayed by that program, you will be contaminated automatically.
6. Do not run your computer using an account that has administrative privileges, even if you are the only one who uses it! Setting up users with limited privileges will prevent any type of program from installing unless you specifically want it to. To install programs, etc. you simply log on as the administrator. When finished, log back on as a limited user to prevent unwanted programs from being installed.
7. Never allow children or teenagers to use your computer!
8. Learn to actually USE the antivirus/antimalware program you have installed on your computer. None of the programs will provide adequate protection without your help!
9. Don't open any emails that look suspicious, no matter who they are from! Even your mother could have an infected computer at her home that is sending out infected emails using her email address.
10. Never forward an email until after you have deleted all the visible email addresses it contains!
11. Never send an email to more than one person unless all the recipients are listed in the **bcc** section! (List your own email address in the "To:" section)
12. Use an alternative browser such as Firefox.