



A Public Service Announcement By

Reich Consulting

breich@reich-consulting.net / <http://www.reich-consulting.net/>

Internet Users: Beware of Fake Antivirus Programs

In the past month I've personally cleaned more than a dozen computers infected with a new strain of virus that sneaks onto your computer by disguising itself as an antivirus program. According to Microsoft **994,061 computers were infected in the month of November alone**. If you use the Internet, your chances of coming in contact with this threat are very, very high.

The virus begins as a pop-up window claiming that your computer is infected with a virus. It displays the results of a virus scan claiming that your computer is infected with viruses that it doesn't actually have. You will be prompted to download software to clean them, but when you do your computer will become infected with one of the most malicious viruses that I've seen in the past 13 years.

Identifying a Fake Antivirus Scan

The good news is that this type of Trojan application depends on you—the user—to install it, and so in this case an ounce of prevention is worth a pound of cure. By knowing what to look for, you can avoid becoming a victim of this scam.

Make sure you have antivirus installed and know what it looks like. Install a legitimate antivirus application such as *AVG*, *Trend Micro*, *Norton*, or *McAfee* and familiarize yourself with the “look and feel” of the program. Every application has a unique icon at the top of its program window that it uses to identify itself, and by knowing what it looks like, you can determine when a virus warning is legitimate or a ploy to infect your PC.

Be suspicious of virus detection warnings. Most of these fake antivirus programs are a variant on a single virus called “Win32 / FakeSecScan”. Each variant looks a bit different from the rest, but they all behave the same way and are easy to spot.

Some of the fake programs you may come in contact with are *XP Antivirus 2009*, *Spyware Preventer*, and *System Antivirus 2008*. If you are surfing the Internet and a message pops up telling you that your computer is infected with viruses and spyware, **approach it with suspicion!** Look at the title bar on the window: are the title and icon the same as the antivirus application you already have installed on your computer? (You do have antivirus installed, don't you?)

A program cannot scan your computer for viruses unless you have already installed it. Make sure that the program title and icon are the same as the antivirus application you already have installed. If it is not your antivirus application close the window and leave the website that you are viewing. Avoiding infection is that simple.

What to do if Your Computer is Already Infected

Because this virus infects your computer at a variety of points including your Startup Programs, registry, and hardware drivers, it can be very difficult to clean. And after the virus is removed it can leave a path of destruction behind it rendering your computer almost useless. If your computer is already infected with a variant of the “Win32/ FakeSecSen” virus, you may need to enlist the help of a professional to remove it.



General Computing Tips

1. Keep Your Software Updated.

Configure your PC to automatically install updates when they are available using Windows Update. This will keep your software free from known bugs and security holes that can be exploited by viruses and hackers.

2. Install Antivirus Software and Keep it Current.

Purchase or download a quality antivirus application such as AVG, Trend Micro, Norton, or McAfee and keep it current. Don't ignore it when it wants to do an update or perform a scan. Out of date protection is as good as no protection at all!

3. Install Antispyware Software and Keep it Current.

Antispyware software like Windows Defender and Ad Aware protect you from unwanted advertisements, toolbars, and pop-ups windows. Use these free tools and keep them updated.

4. Use A Firewall.

A firewall is a program that prevents unwanted connections to and from your computer. If you run Windows XP or Vista you already have one installed. Don't disable the firewall for convenience sake. It's there to keep your computer protected from threats!

5. Use Your Computer Responsibly.

Getting your computer professionally repaired is expensive. You can avoid the fees and hassle by following the guidelines above and by staying aware of the things that you download and install from the Internet.