

Dear PCS Customer:

There is a big family of fake antivirus applications reaping havoc across the internet. We first started seeing them in July 2008. Many of the programs have names that closely resemble the names of legitimate antivirus programs. This is done on purpose to trick you into thinking that these programs are trustworthy.

Programs you might see causing problems on your computer are (updated 8/13/2010):

- Advanced Virus Remover
- AntiMalware Doctor
- AntiVir Solution Pro
- Antivirus 2008 (also 2009, 2010, and 7)
- Antivirus Pro 2010
- Antivirus Soft
- Antivirus Suite
- Antivirus XP
- Antivirus XP 2008 (2009 and 2010)
- AVSecuritySuite
- AVSuite
- AV7
- Cleanup Antivirus or Clean Up Antivirus
- Control Center
- Control Components
- Cyber Security
- Defense Center
- Digital Protection
- GreenAV
- Internet Security 2009 (2010)
- Live Antispy
- Malware Defense
- Malware Wiped
- MS Antispyware 2009 (2010)
- PaladinAntivirus
- PC Antispyware 2010
- Personal Antivirus
- Personal Security
- Privacy Center
- RegFix Pro
- SecurityEssentials2010
- Security Guard
- SecurityMasterAV
- Security Tool
- Smart Security
- Spyware Locker
- SpywareMaster
- System Antivirus
- System Guard 2009 (2010)
- System Security 2009 (2010)
- Total PC Defender 2010
- Ultimate Antivirus 2008 (2009 and 2010)
- Ultimate Defender
- User Protection
- Virus Heat
- VirusRemover2008 (2009 and 2010)
- Vista Antivirus 2008 (2009 and 2010)
- XP AntiMalware 2010
- XP Antivirus
- XP Security
- XP Smart Security 2010
- Your Protection
- Windows Antivirus 2008 (also 2009 and 2010)
- WinAntivirus Pro 2007 (2008, 2009, 2010)
- WinPCAntivirus
- Windows Protection Suite
- Windows PC Defender
- Windows Police Pro
- Windows Antivirus Pro
- Wireshark Antivirus

And there are new ones cropping up every day. We are finding new names constantly as we clean computer systems. According to some industry sources, there are over 15,000 new malware programs produced every day! So, as you can see, it's very hard to keep up.

### **What are these programs?**

These programs are rogue Antispyware programs. Their goal is to steal your money. They are spread through trojan viruses and other malware in the form of fake security alerts and warnings. They can be caught from malicious web sites. They usually warn that you are infected with malware or are being attacked in some manner. When you click on these warning or web sites, they will automatically download and install their programs on your computer. In some cases, the program is installed without any intervention at all from you.

Once these programs are installed, they will scan your system and start displaying fake security warnings. They will say that your computer is infected with multiple instances of malware and spyware. They try to create a panic about your computer. Warnings persistently pop up on your desktop alerting you of infections (the number goes up as time goes on) and you may be informed that your credit card information has been hacked or worse. The rogue software offers you to clean your system if you purchase the full licensed version. The software that you are supplied is just more malware.

Other tactics that these programs use is to change your desktop background to a message stating you are infected. There may also be pop-ups and fake alerts stating your computer is being attacked, and a fake Internet Explorer page that states Google has found your computer to be infected. All of these are further scare tactics and should be ignored.

### **Possible symptoms after infection:**

- The infections will hide the C: Drive icon located in the “My Computer” window. **Tip:** To be able to see your C: Drive, open a browser and type “C:\” or “My Computer”.
- “VIRUS ALERT!” may appear in the system tray (lower right hand corner of your desktop). It may change your desktop background to a red hazard alert or a blue background with a yellow alert in the center.
- The Screensaver may change to either the ‘Blue Screen of Death’ or bugs crawling on the screen.
- The Start Menu does not list some or all of the following: ‘Programs’, ‘My Documents’, ‘My Computer’, ‘My Recent Documents’, ‘Search’, ‘Help’, ‘Control Panel’ or ‘Run’.
- They may disable the Task Manager, Control Panel, Registry, Display Properties change desktop background, lock homepage, download unwanted files, steal passwords and credit card information, overwrite admin privileges and more.
- You will see Pop ups of random rogue anti-spyware programs. The pop-ups displayed are for rogue anti-spyware programs like the names mentioned above.
- Windows explorer may close by itself or display an “Illegal Operation of System” page.
- Your computer performs sluggishly or crashes.
- You may not be able to access the internet or certain websites.
- Your antivirus software may stop working and you may not be able to install any antivirus software or other cleaning tools.

**Possible images or screen shots (there are many variations) you may see on your system:**



**How to get rid of this problem:**

If you have any trace of these rogue Antispyware malware programs on your system, it is recommended that you take immediate steps towards removal. The first step towards the removal of these programs is to determine if your system is actually infected. For this, you can use any good quality anti-spyware, many of which are freely available on our website at [www.pcscomputer.net](http://www.pcscomputer.net).

Antivirus 2008, XP Antivirus and its variants are persistent, hard-to-remove applications that hide their files to escape detection from legitimate security software. Because these infections are so persistent and hard to remove, it will be a difficult, laborious process to attempt to remove them yourselves. Sometimes the hard drive has to be physically removed from the computer and scanned by another computer in order to clean it up. If you bring your system to PCS we will help you with this cleanup process. Depending on the number of users on your system and the aggressiveness of the infection, this process can take several days.

**How to Avoid These Infections and more....**

If you want to keep spyware (including adware, popups, and hijackers) off of your computer, the most important thing to keep in mind is this: **NOTHING IS FREE. EVERYTHING COMES WITH A PRICE.** The price of most of the “free” stuff found on the internet is the extra junk that gets installed on your computer without your knowledge. This junk is what we commonly refer to as spyware. Here are some specific things to be aware of:

- Do not participate in any of the so-called “free music” or “free video” systems.
- When using the internet, do not click on links or buttons for anything advertised as free. This includes free screen savers, free virus scanners/removers, free spyware scanners/removers, and free weather programs.
- If you do get a popup that asks if you want to install or download something, do not click anything inside the popup window. Click the “X” in the top right corner instead.
- If you get a popup or see anything on your computer screen that claims your computer has some type of terrible infection, do not click anything inside the popup window. Click the “X” in the top right corner instead.
- Some websites distribute rogue anti-spyware programs like Antivirus XP 2008 to its visitors. Visit only those websites that you trust.
- Do not use pirated software. Use only genuine software.
- Instant Messaging programs are good carrier of spyware and other malware. Avoid IM to share files.
- Set your e-mail program so that it does not automatically display messages on your screen. You should have to click on a message to open it and read it. Do not open messages from anyone you don’t know. Delete them without even viewing them.
- Do not click on any links or buttons that say you have just won a prize or that you may be eligible to receive a prize.
- Be careful about sharing files on MySpace, FaceBook, and other such sites.

We hope this information has been helpful. We look forward to continuing to help you with all your computer needs.

Sincerely,

The Staff at PCS