

Total Computer Solutions

“YOUR BUSINESS COMPUTER SPECIALISTS”

Legit or Bogus? How to Spot A Rogue Anti-Virus Program

Have you seen an advertisement or pop-up offering a free PC scan, or telling you that your computer is infected and at risk? If so, you’ve seen first-hand a harmful trojan disguised as an anti-virus (AV) program.

These types of rogue AV scams are on the rise. They appear legitimate, but clicking on these pop-ups is the number one way unsuspecting users get infected. Most of these pop-ups have legitimate sounding virus names and ask you to pay for the program. They will almost always have a notice indicating you need to “click here” to install the program to disinfect your PC. Once you click on that link - and sometimes ANY link in the pop-up - you’re infected.

According to Roger Thompson, chief research officer of security firm AVG, "It looks like an AV program, except it's making up stories of what's actually on your computer. It doesn't offer an uninstall option and it generally burrows deep, like a rootkit. It's generally very difficult to remove."

To take it a step further, if you accept the offer and enter your credit card information, the hackers have your personal data and can use it at will.

Here are many of the questions our customers have asked lately about these pop-ups:

I have anti-virus software, won't that protect me?

A good anti-virus program is essential to protecting your computer. However, some AV programs only protect you against virus infections. They will not protect you against malware.

A good AV program will give you good virus protection as well as malware protection.

What can a rogue anti-virus program do?

An infection can do almost anything to a computer, from stealing information to destroying your valuable data. Some malware will collect your password information and use it to access your financial accounts.

Some infections will let your computer be used as a “bot,” which lets attackers use it to

share illegal files, attack other systems on the Internet, or spread infections to your friends and family.

How do I protect myself?

Here are some basic tips to keep yourself from being a victim of a rogue anti-virus program.

1. Keep your computer updated with the latest security patches for your operating system and web browser.
2. Never click on pop-ups that you come across on a website. Even if the advertisement looks legitimate, chances are it isn't.
3. Check to make sure your Internet firewall and antivirus are updated every time you use your computer.
4. Turn off any Active-X and scripting from foreign websites. (In Internet Explorer these controls are found by going to the TOOLS menu, INTERNET OPTIONS, SECURITY tab and clicking the CUSTOM LEVEL... button.) Many of the infections come from these types of scripts. Depending on your current settings, your system may ask you if you want to run the script. If this was triggered by a pop-up, always chose no.
5. Keep a good backup. Some infections can be so severe that you will need to restore files for your PC to be disinfected and repaired properly.
6. Scan your computer on a regular basis. Most antivirus programs will do this automatically. AVG is a very good program that will scan every day, and can be set to run at night so, even if you have a slow computer, it doesn't slow down your work.

What if I get a popup on my screen while I am on the internet?

If you happen to get a pop-up on your screen as described above, we recommend you press and release the power switch (do not hold it in). This should close all programs and shut down your computer. This is one of the safest ways to keep the malware from loading on your computer.

NOTE: If possible, you should save any open documents before pressing the power switch to shut down the computer.