

How to Avoid Downloading A Fake Anti-Virus

This is a scam which is growing very fast, and one you really should be aware of. Fake anti-virus and anti-spyware software is being used by scammers and identity thieves in many cunning ways.

Scammers, identity thieves, and hackers have grown more sophisticated. Today, some cyber-criminals are selling or giving away software that supposedly fights viruses, spyware, and malware.

In fact, their "rogue software" often doesn't work, or will actually infect your computer with the dangerous programs it is supposed to protect against!

I'm going to tell you how to distinguish between useless or even malicious security software and the real deal. And I'll also explain why you need to be cautious about closing or deleting these alerts, even when you know they're fake.



*Not long ago, in a land not so far away, a colleague was conducting Internet research when **pop!** A yellow triangle appeared on her screen, warning that her computer had been “**infected**” by dangerous spyware. The alert looked real. She thought it was from her ever vigilant already installed anti-virus.*

Still, she was skeptical. Using her mouse, she closed the alert by pressing the "x" in the window's upper right-hand corner. --That was her first and last mistake!

Pop-up ads began sprouting everywhere, her screen froze, and none of her programs were accessible, even after rebooting. Basically, her computer had been disabled, and she spent hours trying to get it to work before finally calling IT.

Welcome to the world of fake anti-virus, anti-spyware programs.

Despite what happened to our colleague, it's not that common to encounter hackers who simply want to harm your computer with fake anti-virus programs.

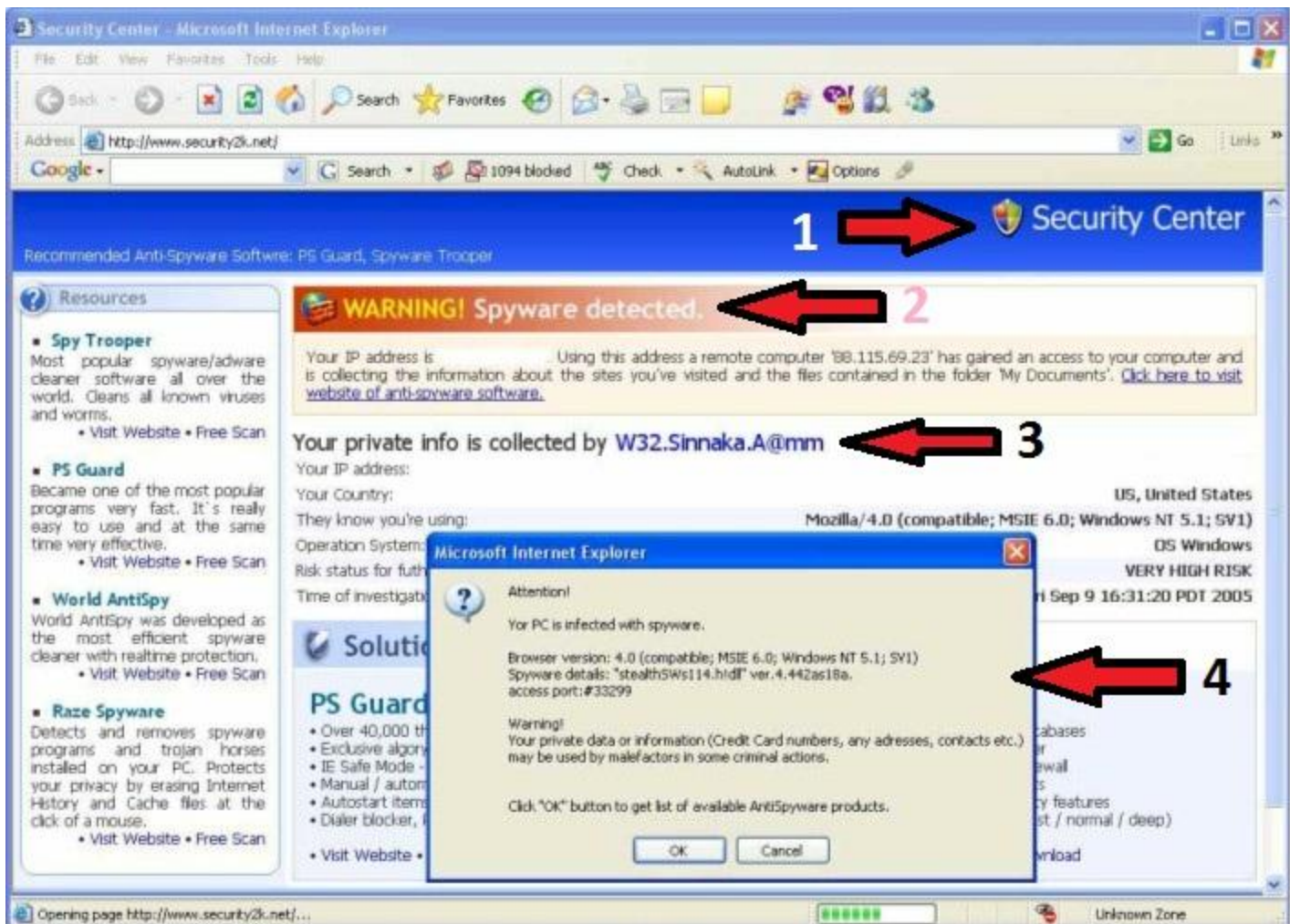
In most cases, you'll confront scammers who want to scare you into buying "rogue" security software by making you think your computer is infected. ("Rogue" means software of unknown or questionable origin, or doubtful value.)

In fact, fake "virus alerts" often mimic ones displayed by brand-name products (**Figure 1, 2**). For example: "Your Computer Has Been Infected!" (That's what some pop-ups and phony alerts will say, hoping you'll download fake anti-virus software.) Sometimes, as you see in the photo below scammers will add a lot of information to confuse you and make it look completely official (**Figure 3**). To the untrained eye it is very convincing, and the prospect of being infected by rogue software or viruses is very scary, which is why most people will click that supposed life saving "SCAN NOW" or "YES" button (**Figure 4**).

Don't be fooled!

Just one click anywhere on these screens is dangerous and in all likelihood will download their malicious software on to your system, causing you, and the technician you will end up taking it to, hours of grief.

Your best defense is Alt+F4. Press and hold down the Alt button and tap F4 until your computer comes up and asks you if you would like to restart. Using this method to avoid any "ghost clicks" (an accidental click) on this fake pop-up is the safest and most effective way to avoid a trip to your local IT department.



Meanwhile, ID thieves will use the fake software to gather your personal and financial information for their own ID theft scams or for sale to others.

Fake virus alerts are usually generated by a Trojan, a program that takes control of your computer after you open an email attachment, click on a pop-up advertisement, or visit a particular website.

If you run programs that provide file-sharing information (ie. Limewire, Bearshare, Torrents) your computer might be remotely accessed by scammers, hackers, and identity thieves.

What to look for:

- Rogue anti-virus/spyware programs often generate more "alerts" than the software made by reputable companies.
- You may be bombarded with pop-ups, even when you're not online.
- High-pressure sales copy will try to convince you to buy RIGHT NOW!
- If you've been infected, your computer may dramatically slow down.
- Other signs of infection include: new desktop icons; new wallpaper, or having your default homepage redirected to another site.

Tips for avoiding malicious software:

1. Keep your computer updated with the latest anti-virus and anti-spyware software, and you can also use a firewall.
2. Never open an email attachment unless you are **POSITIVE** about the source.
3. Do **NOT** click on any pop-up that advertises anti-virus or anti-spyware software, especially a program promising to provide every feature known to mankind. (Also remember: the fakes often mimic well-known brands such as Grisoft AVG, Norton, Microsoft and McAfee.)
4. If a virus alert appears on your screen, do **NOT** touch it. Don't use your mouse to eliminate or scan for viruses, and **DON'T** use your mouse to close the window. Instead, use the technique we discussed earlier. Alt+F4
5. Do not download freeware or shareware unless you know it's from a reputable source. Unfortunately, many freeware and shareware programs often come bundled with spyware, adware or fake anti-virus programs.
6. Avoid questionable websites. Some sites may automatically download malicious software onto your computer.
7. Reset your current security settings to a higher level.
8. Although fake software may closely resemble the real thing, it's rarely an exact match. Look for suspicious discrepancies.

If your computer is infected by rogue software, stop work immediately. Don't keep using the computer. This may further damage your machine and provide identity thieves with more information about you.

For further information please contact your local IT department.