



State of West Virginia Cyber Security Tip

ALERT

West Virginia Office of Information Security and Controls – [Jim Richards](#), WV Chief Information Security Officer

WATCH OUT FOR FAKE VIRUS ALERTS

Rogue security software, also known as "scareware," is software that appears to be beneficial from a security perspective (i.e. free virus scan) but provides limited or no security, generates erroneous or misleading alerts, or attempts to lure users into participating in fraudulent transactions.

How does rogue security software get on my computer?

Rogue security software designers create legitimate looking pop-up windows that advertise security update software. These windows might appear on your screen while you surf the web.

The "updates" or "alerts" in the pop-up windows call for you to take some sort of action, such as clicking to install the software, accept recommended updates, or remove unwanted viruses or spyware. When you click, the rogue security software downloads to your computer.

Rogue security software might also appear in the list of search results when you are searching for trustworthy antispyware software, so it is important to protect your computer.

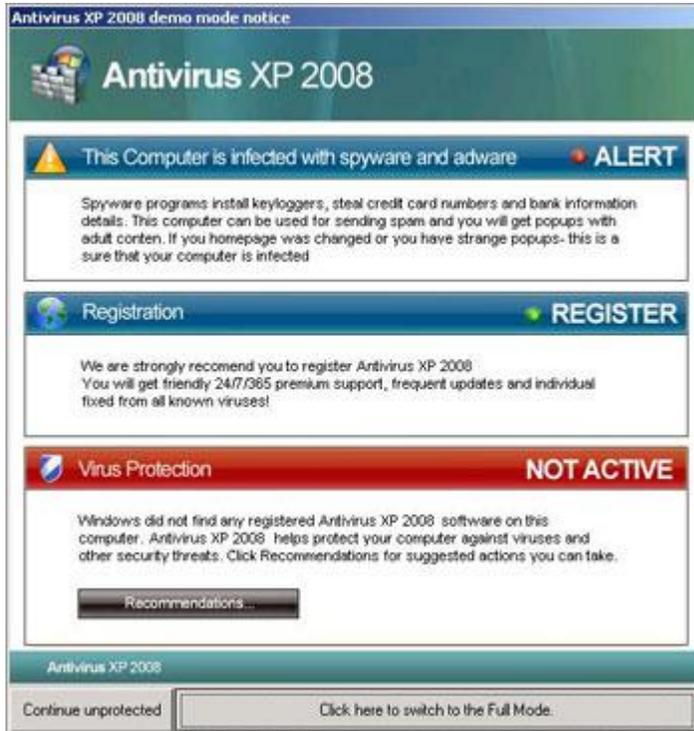
What does rogue security software do?

Rogue security software might report a virus, even though your computer is actually clean. The software might also fail to report viruses when your computer is infected. Inversely, sometimes, when you download rogue security software, it will install a virus or other malicious software on your computer so that the software has something to detect.

- Some rogue security software might also:
- Lure you into a fraudulent transaction (for example, upgrading to a non-existent paid version of a program).
- Use social engineering to steal your personal information.
- Install malware that can go undetected as it steals your data.
- Launch pop-up windows with false or misleading alerts.
- Slow your computer or corrupt files.
- Disable Windows updates or disable updates to legitimate antivirus software.
- Prevent you from visiting antivirus vendor websites.

Rogue security software might also attempt to spoof the Microsoft security update process. Here's an example of rogue security software that's disguised as a Microsoft alert but that doesn't come from Microsoft.

FAKE: Below is an example of a warning from a rogue security program known as AntivirusXP.



LEGITIMATE: Below is the legitimate Microsoft Windows Security Center:



When in doubt, contact your Service Desk or Technical Assistance BEFORE clicking.

Brought to you by:

DIVISION OF
THE OFFICE OF TECHNOLOGY

OFFICE OF INFORMATION SECURITY
AND CONTROLS