

Microsoft | Security Blog



Scareware: Don't Let Scammers Scare You



Tim Rains - Microsoft 15 May 2012 1:01 PM

2

Scareware, also known as fake anti-virus software, has become one of the most common methods computer hackers use to swindle your money. If you have had a security alert icon pop up on your computer, you may have been the victim of scareware.

In a recent [TV interview](#), I discuss how scareware programs usually look and feel just like legitimate security programs. The scareware will claim to have detected a large number of nonexistent threats on your computer and then urge you to pay for the "full version" of the software to remove the threats. In the second half of 2011 alone, Microsoft detected scareware approximately 52 million times in the United States.

Here are some tell-tale signs that may indicate a scareware infection:

- Your computer is running much slower than usual
- When you try to surf the internet to legitimate anti-virus websites, you can't get to them
- You are seeing a lot of pop-up windows with false or misleading alerts
- The anti-virus software you recently downloaded is trying to lure you into upgrading to a paid version of the program

The criminals behind these scareware scams go to great lengths to make their software look legitimate. However, scareware is designed to steal your credit card information and identity along with any and all information on your computer. Steps to protect from scareware:

- Install a firewall and keep it turned on – Windows has a built in firewall you can use for free
- Use automatic updating to keep your operating system and software up to date – you can turn this on in the Windows control panel
- Install antivirus from a company that you know and trust and keep it up to date. One option is to use [Microsoft Security Essentials](#) that you can get for free from Microsoft.com
- Use caution when you click links in email or on social networking websites

For more info about security threats and trends, please read our [Security Intelligence Report \(SIR\)](#).

Tim Rains
Director, Trustworthy Computing

Comments



Ed 15 May 2012 8:07 PM #

I don't think a firewall will block malware/scareware from coming onto a computer as most novices love to click on links or get very nervous when they think there is a problem with their computer.

The scareware/malware writers aren't too smart either when the fake alert screens pop up with dozens upon dozens of "issues" with their computer [you have to ask how did all these get onto my computer when there was none detected days ago]. A few "issues" would be more normal.



Victor 30 May 2012 5:14 AM #

Users should be advised that when presented with such a pop-up, they use Task Manager to close the running session. Most of the pop-ups buttons, including the "Close" button inside the pop-up, only lead to one result, infection.