

PROTECT YOUR COMPUTER Don't be Scared by 'Scareware'

07/09/10



We've all seen them—pop-up messages telling you your computer is infected with a virus. To get rid of it, all you have to do is order the antivirus software being advertised.

Before you click, though, know this: few Internet security companies use ads to tell you about a virus on your computer. Most of these pop-ups are scams, and it's one of the fastest-growing types of Internet fraud today.

These scams have a name. They're called "scareware" because they try to frighten you into purchasing fake antivirus software with a seemingly genuine security warning. But if you do try to buy this program, it will either do nothing...or it could compromise your computer by installing malicious software onto your system. And in some instances, you don't even have to click on the pop-up box...the software downloads automatically.

Cyber criminals often use notorious botnets—networks of compromised computers under their control—to push out their software. They'll also masquerade as legitimate Internet security companies and buy ads on other websites—called "malvertising"—but when consumers click on the ads to purchase the products, they are redirected to websites controlled by the bad guys.



Many of these criminals operate outside the U.S., making investigations difficult and complex for the FBI and its partners. But we've had successes—just this past May, for example, [three people were charged in Illinois](#) in connection with a scheme that caused Internet users in more than 60 countries, including the U.S., to buy more than \$100 million worth of bogus scareware software.

Two of the defendants, including an American, are accused of running an overseas company that claimed to sell antivirus and computer performance/repair software over the Internet. A third man operated the company's Cincinnati call center, which was responsible for technical and billing support to its customers (but in reality deflected complaints from consumers who realized the software didn't work).

According to the indictment, proceeds from the sales of the software (which was typically purchased by credit card) were deposited into bank accounts controlled by the defendants and others throughout the world and then quickly transferred to accounts in Europe.

In addition to the consumers victimized by the scam, a number of legitimate companies tricked into selling ad space on their websites for the bogus software were allegedly defrauded of about \$85,000 in unpaid fees.

Don't let it happen to you. Here are a few words of advice on scareware.



How to Spot a Potential Scareware Infection

- Windows Update fails to run.
- Other legitimate security applications won't update.
- Certain website, especially Internet security sites, won't load.

How to spot a scareware scam:

- Does the pop-up use “non-clickable” icons? To build authenticity into their software, scareware will show a list of reputable icons—like those of software companies or security publications. However, the user can’t click through to the sites to see the actual reviews or recommendations.
- Is the pop-up ad hard to close? Scareware pop-ups employ aggressive techniques and will not close easily after clicking the “close” or “X” button.
- Have you heard of the software before? Cyber criminals use easy-to-remember names like Virus Shield, Antivirus, or VirusRemover.

How to protect yourself from scareware: Make sure your computer is fully protected by legitimate, up-to-date antivirus software.

If you think you’ve been victimized by scareware: Please contact the Help Desk at help@faytechcc.edu or thru the Help Desk Requester Icon on the desktop of your office computer.

Resources:

- [Chicago press release](#)