FTC Consumer Alert

Federal Trade Commission ■ Bureau of Consumer Protection ■ Division of Consumer & Business Education

"Free Security Scan" Could Cost Time and Money

Messages telling you to install and update security software for your computer seem to be everywhere. So you might be tempted by an offer of a "free security scan," especially when faced with a pop-up, an email, or an ad that claims "malicious software" has already been found on your machine. Unfortunately, it's likely that the scary message is a come-on for a rip-off.

The free scan claims to find a host of problems, and within seconds, you're getting urgent pop-ups to buy security software. After you agree to spend $40 or more on the software, the program tells you that your problems are fixed. The reality: there was nothing to fix. And what's worse, the program now installed on your computer could be harmful.

According to attorneys at the Federal Trade Commission (FTC), the nation's consumer protection agency, scammers have found ways to create realistic but phony "security alerts." Though the "alerts" look like they're being generated by your computer, they actually are created by a con artist and sent through your Internet browser.

These programs are called "scareware" because they exploit a person's fear of online viruses and security threats. The scam has many variations, but there are some telltale signs. For example:

- you may get ads that promise to "delete viruses or spyware," "protect privacy," "improve computer function," "remove harmful files," or "clean your registry;"
- you may get "alerts" about "malicious software" or "illegal pornography on your computer;"
- you may be invited to download free software for a security scan or to improve your system;
- you could get pop-ups that claim your security software is out-of-date and your computer is in immediate danger;
- you may suddenly encounter an unfamiliar website that claims to have performed a security scan and prompts you to download new software.

Scareware purveyors also go to great lengths to make their product and service look legitimate. For example, if you buy the software, you may get an email receipt with a customer service phone number. If you call, you're likely to be connected to someone, but that alone does not mean the company is legitimate. Regardless, remember that these are well-organized and profitable schemes designed to rip people off.

How Do the Scammers Do It?

Scareware schemes can be quite sophisticated. The scam artists buy ad space on trusted, popular websites. Even though the ads look legitimate and harmless to the website's operator, they actually redirect unsuspecting visitors to a fraudulent website that performs a bogus security scan. The site then causes a barrage of urgent pop-up messages that pressure users into downloading worthless software.

What to Do

If you're faced with any of the warning signs of a scareware scam or suspect a problem, shut down your browser. Don't click "No" or "Cancel," or even the "x" at the top right corner of the screen. Some scareware is designed so that any of those buttons can activate the program. If you use Windows, press Ctrl + Alt + Delete to open your Task Manager, and click "End Task." If you use a Mac, press Command + Option + Q + Esc to "Force Quit."

If you get an offer, check out the program by entering the name in a search engine. The results can help you determine if the program is on the up-and-up.

Good Security Practices

Check that your security software is active and current: at a minimum, your computer should have anti-virus and anti-spyware software, and a firewall. You can buy stand-alone programs for each element — or a security suite that includes these programs — from a variety of sources, including commercial vendors and your Internet Service Provider. The security software that was installed on your computer when you bought it generally works for just a short time — unless you pay a subscription fee to keep it in effect. Visit **http://security.getnetwise.org/tools/search** for a list of security tools from legitimate security vendors selected by GetNetWise, a project of the Internet Education Foundation.

Make it a practice not to click on any links within pop-ups.

Report possible fraud online at **ftc.gov** or by phone at 1-877-FTC-HELP. Details about the purchase — including what website you were visiting when you were redirected — are helpful to investigators.

Visit **www.OnGuardOnline.gov** to learn more about protecting your computer from bugs, viruses and scammers.

The FTC works for the consumer to prevent fraudulent, deceptive, and unfair business practices in the marketplace and to provide information to help consumers spot, stop, and avoid them. To file a complaint or to get free information on consumer issues, visit **ftc.gov** or call toll-free, 1-877-FTC-HELP (1-877-382-4357); TTY: 1-866-653-4261. The FTC enters consumer complaints into the Consumer Sentinel Network, a secure online database and investigative tool used by hundreds of civil and criminal law enforcement agencies in the U.S. and abroad.