



SANS TOUCH!

SANS Institute Security Newsletter for Computer Users

January 2010

In This Issue:

- **The Top Ten Reasons Why Computers Don't Have Security Software**
- **Patches and Updates Roundup**

[Editor's Note: (Wyman) Do you have security software installed on your computer? How effectively does it protect your computer? Is it up-to-date? Do you have just anti-virus or a full security suite? We've made a list of the top reasons that computers don't have security software and added some good reasons why you should install it on yours, as well as tips on how to shop for a good-quality, all-in-one security suite that won't bust your budget.]

The Top Ten Reasons Why Computers Don't Have Security Software

#10. "I just use my computer for email and web browsing."

You are using your computer for the same things that most people use them for most of the time. That's why scam and phishing emails, rigged websites and similar deceptions are the most rapidly growing threats. You fit the profile of computer users that the Bad Guys are targeting. A good-quality security software suite helps protect you against deception and its consequences--exploitation of personal and sensitive information that a criminal may trick you into revealing.

#9. "I've never had any virus problems."

Famous last words. Being healthy is no reason to skip vaccinations. Security software functions like your immune system. It can't prevent every infection, but without it, your computer is wide open to infection by many hundreds of types of malicious software.

#8. "It kept popping up all the time."

Don't turn off your security software or remove it from your system. Those warnings may be legitimate or could be the work of "scareware." Scareware creates misleading pop-ups and animations about bogus threats that look very convincing—all tricks to get you to click "Yes" or "No" or "Cancel." No matter which one you choose, the problem will not go away, and clicking on anything stands to make things worse. When this happens, contact your computer support provider immediately for expert assistance.

#7. "It might crash my system."

Malicious software, however, will probably do much worse. Malware can eat up your time, money, and peace of mind, and possibly steal your identity. If you don't feel confident about installing security software, let your computer support provider handle the job.

#6. "My subscription kept expiring."

Most subscriptions are good for one year. Those onscreen reminders telling you that it's time to renew are just like the "time-for-maintenance" light on the dashboard of your car. They can be annoying, and sometimes go off prematurely, but aren't you grateful they're there to remind you?

#5. “It slows down my system.”

We make trade-offs between speed and safety every day. Going without security software is always a bad choice. Not all security software is of the same quality or performs equally well. If the one you have bogs down your system too much, install one that doesn't. For shopping tips, see #1 below.

#4. “I thought it came with the computer.”

It probably did, like the seatbelts and airbags in your car. But even so, you have to activate and update pre-installed security software or it will not protect your system effectively. Most new computers come with 30- to 90-day trial versions of security software. When the trial is nearly up, you'll see onscreen warnings and instructions for how to buy a full subscription.

#3. “It's too expensive.”

One-year subscriptions to any of the leading, good-quality, all-in-one security suites, that include anti-virus, anti-spyware, anti-phishing, anti-spam, and a two-way software firewall, are available in retail stores for \$50 to \$80. Many are offered on a 30- to 90-day free trial basis and at a discount—usually \$10 off—if you buy online and download the software. Some products can be installed on two or three systems, cutting the cost of protecting each computer by 50% or more. Before you buy, check with your Internet Service Provider. You may be eligible to receive a good-quality security suite at low cost or at no cost.

#2. “Macs don't need security.”

Mac users are just as susceptible to deception as users of Windows or any other operating system. Scam phishing emails, infected email attachments, and rigged websites are the most rapidly growing threats—not malicious software or things that exploit “holes” in software. These deceptions target users, not computers, and don't need a “hole” to succeed. Good-quality security suites can detect deceptions and include tools to help you avoid revealing sensitive and personal information, such as social security, credit card and PIN numbers, as well as usernames and passwords, unwittingly or to the wrong people.

#1. “I don't know what to buy or how to install it.”



Security Software Checklist:

- ✓ Shop for a security software suite as you would when purchasing any important product.
- ✓ Gather information and recommendations from IT at the office, your Internet Service provider, or your computer support provider.
- ✓ Get some good bets by reading comparative reviews of competing products published by third-parties, such as *PCWorld*, *Consumer Reports*, and *MacWorld*.
- ✓ Hedge your bet by opting for a trial version, if available, and one that you can upgrade to a full subscription without reinstalling.
- ✓ Weigh effectiveness, performance, features, support and, lastly, price—at most a difference of \$30/year.
- ✓ Verify that the product includes anti-virus, anti-spyware, anti-phishing, anti-spam, a two-way software firewall, and automatic online updating.
- ✓ Performance and effectiveness are judged best by the results of professional testing, like those performed by AV-test.org and www.av-comparatives.org.
- ✓ If you run into difficulties, telephone support may be preferable to email or online chat.
- ✓ Familiarize yourself with the installation steps before you begin. If you get lost or stuck, call the software manufacturer's technical support line for assistance.
- ✓ If you don't feel confident about installing security software, turn the job over to your computer support provider.

Patches and Updates

Windows & PC Office: <http://update.microsoft.com> and <http://www.microsoft.com/security/updates/bulletins/200911.aspx>

OS X: <http://support.apple.com/kb/HT1338>

Mac Office: <http://www.microsoft.com/mac/help.mspx?CTT=PageView&clr=99-0-0&ep=7&target=ffe35357-8f25-4df8-a0a3-c258526c64ea1033>

iPhone/iPod: <http://support.apple.com/kb/HT1414>

iPod: <http://support.apple.com/kb/HT1483>

Windows Adobe Reader:

<http://www.adobe.com/support/downloads/product.jsp?product=10&platform=Windows>

OS X Adobe Reader:

<http://www.adobe.com/support/downloads/product.jsp?product=10&platform=Macintosh>

Flash Player: <http://get.adobe.com/flashplayer/>

Firefox: <http://www.mozilla.com/en-US/firefox/update/>

Safari: http://www.apple.com/downloads/macosx/apple/application_updates/safari.html

Opera: <http://www.opera.com/>

Chrome: <http://googlechromeupdate.com/updates.html>

Java: <http://www.java.com/en/download/manual.jsp>

iTunes: <http://www.tuaw.com/2009/09/22/itunes-9-0-1-now-in-software-update/>

Symantec:

<http://service1.symantec.com/SUPPORT/sharedtech.nsf/docid/2002021908382713>

Norton:

http://www.symantec.com/business/security_response/definitions/download/detail.jsp?gid=n95

McAfee: http://www.mcafee.com/apps/downloads/security_updates/dat.asp

Kaspersky: <http://www.kaspersky.com/avupdates>

Sophos: <https://secure.sophos.com/support/updates/>

Panda: <http://www.pandasecurity.com/homeusers/downloads/clients/>

BitDefender: <http://www.bitdefender.com/site/view/Desktop-Products-Updates.html>

Microsoft Security Essentials:

<http://www.microsoft.com/security/portal/Definitions/HowToMSE.aspx>

Copyright 2009, SANS Institute (<http://www.sans.org>)

Editorial Board: Bill Wyman, Walt Scrivens, Phil Hoffman, Alicia Beard, Alan Paller.

Email: OUCH@sans.org

Download the formatted version of the OUCH! at <https://www.sans.org/newsletters/ouch>

Permission is hereby granted for any person to redistribute this in whole or in part to any other persons as long as the distribution is not being made as part of any commercial service or as part of a promotion or marketing effort for any commercial service or product. We request that redistributions include attribution for the source of the material.