How to protect yourself from viruses without installing anti-virus software.

Thursday, October 15th, 2009

You don't really need antivirus software on your Windows computer. Over the past several years, antivirus scanning has become much more centralized. Most of what you download over email or at work has already been scanned for viruses and malware anyway—why pay Norton or McAffee to have it scanned again once it reaches your hard drive? And why have another program running on your computer, slowing it down and wasting resources?

Running antivirus software on Windows these days is almost like getting a smallpox vaccine. Your individual situation may vary (see below), but very likely you can be both free and safe without antivirus software by taking a few basic precautions and being generally security-aware. You may already be aware of these precautions, but you may not have known that following them may effectively eliminate the need for stand-alone antivirus software on your computer.

1. **Use Gmail (or your corporate account) to send and receive file attachments via email.** Many free email providers, such as Gmail, Yahoo and Hotmail, scan attachments for viruses and malware for you, so you know the file is clean when it gets to your hard drive. Many businesses, both small and large, do this as well on their own internal mail servers. (If there is a good way of testing and verifying email providers' attachment scanning claims and abilities, though, I would like to know about it.)

2. **Use the Internet from behind a router.** Don't plug directly into your Cable or DSL modem. Plug a router into that thing (a wireless router if that's how you like to roll) and then use that. Most off-the-shelf routers have built-in firewalls that prevent the most common attacks.

3. **Limit the amount of software you download.** Get the programs you like installed and then keep your computer the way you like it for a good long while. Don't be constantly looking for and downloading new utilities.

    - Especially don't download anything in response to a popup window, ever. If you ever get a popup warning you about viruses on your computer, for example, it's a lie. Just close it.

4. **Don't use LimeWire or BitTorrent** (unless you *really* know what you're doing out there). As Dylan Boom said in this comment at Lifehacker[1], *"I work at Best Buy for Geek Squad, and the computers that come in with the most viruses, etc. normally have two things on them: AVG as their virus protection software, and Limewire."* It is impossible to verify the authenticity or origin of anything that passes through a torrent service (not counting md5 signatures on Linux distributions etc). Consequently people love to insert malware on stuff and send it on to unsuspecting downloaders as the real deal.

5. **Use open-source whenever possible** and download directly from the software's main website.

6. **Stick to mainstream, trusted websites** and access them through your bookmarks or browser shortcuts whenever possible–*don't* get in the habit of visiting the same website repeatedly by typing its name into Google (or any search engine) and clicking on the top result. Stay away from porn sites and any place offering something for nothing. Don't click on ads.

7. **Keep your computer updated.** Windows has a provision for automatically downloading and installing security updates and fixes–make sure it's turned on and that it's working[2].

8. **Use a more secure web browser** such as Chrome[3] or Firefox[4]. Make sure it is fully up to date (instructions for how to do that on Chrome[5] and Fireox[6]).

    - Don't use Internet Explorer. Even the US DoHS has advised against it[7]. While that security advisory is a few years old by now, the fact remains that IE's security model is too broken to trust.

Note that if you don't follow most of these practices already, no antivirus program is going to be able to keep you safe indefinitely anyway!

The main principal here is to clean and verify all the ways that you exchange information into and out of your computer: that mainly means email, web browsing, your physical

1. http://lifehacker.com/5383383/avg-9-free-now-ready-for-download#c16073386
2. http://www.microsoft.com/windows/downloads/windowsupdate/automaticupdate.mspx
3. http://www.google.com/chrome
4. http://getfirefox.com
5. http://www.tech-recipes.com/rx/3436/google-chrome-how-to-check-for-updates/
6. http://support.mozilla.com/en-US/kb/Updating+Firefox
7. http://www.kb.cert.org/vuls/id/713878

internet connection, and being cautious about installing new software. **Note that you may still need antivirus software installed if:**

- You need to share files through shared network drives or email accounts at work that you know are not scanned by antivirus software. (this would include things like shared folders on Dropbox[8] accounts, which, as far[9] as I can tell[10] are not scanned for viruses.)
- You regularly exchange files using thumb drives or external hard drives owned by other people.

Comments and proposed changes/additions welcome!

***Update**, Nov 11 2009*—After I submitted this post a couple of times at Lifehacker, they came up with their own variant: Stop Paying for Windows Security; Microsoft's Security Tools Are Good Enough[11] [sic]. (Not suggesting there's a relationship there. Well OK maybe I am.) I still believe Microsoft's security tools are *unnecessary*, however supremely adequate they may be for the job they're supposed to do, but there are a lot of good points in the article, and I highly recommend it.

Responses

> I'll bite.
>
> For the most part I agree, with a couple of exceptions. First, this only works if you can *guarantee* than no one else will *ever* use your computer.
>
> When my son, or niece, or whoever come to visit, they use my wife's computer. Both my son and niece have managed to get the computer infected, despite the fact that they were using FireFox. I managed to recover from my niece's infection. The one my son got was so bad I had to wipe the computer and begin anew.
>
> So my second point would be to suggest Opera as an alternative browser rather than FireFox. It's more secure.

8. http://getdropbox.com
9. https://www.getdropbox.com/help/27
10. http://developer.amazonwebservices.com/connect/entry!default.jspa?categoryID=152&externalID=1697
11. http://lifehacker.com/5401453/stop-paying-for-windows-security-microsofts-security-tools-are-good-enough?skyline=true&s=x

I agree with you regarding IE, but a lot of corporate types and schools pretty much insist on it. My wife's college e-mail is broken in all browsers save IE. I tried to ban IE from my house, and she beat me down. So, again, your prescription only works if you have *100% control* over your computers at *all* times. Most of us don't.

Norton sucks. It's a pig, makes your computer run like crap, takes over the computer at inconvenient times, won't protect you much, and the Norton customer service is egregious. If you need something, I'd suggest ESET Nod32. (Larry, November 06, 2009)