

# *How do I keep my computer safe on the internet?*

*Leo A. Notenboom*  
<http://ask-leo.com>

Virii & Spyware & Worms ... oh my!

It seems like not a day goes by we don't hear about some new kind of threat aimed at wreaking havoc across machines connected to the internet. While products other than Microsoft's are certainly vulnerable, due to anti-Microsoft sentiment coupled with the massive installed base, Microsoft products seem to provide an irresistible target for hackers and "script kiddies".

Here are some things you can, and should, be doing to stay safe.

•

- **Use a Firewall** - A firewall is a piece of software or hardware that sits between you computer and the internet, and only allows certain types of things to cross the wall. For example a firewall may allow email and web browsing, but disallow things that are commonly not as useful such as RPC or "Remote Procedure Calls". It's vulnerabilities in RPC that, in fact, allowed for one of the more recent worms to propagate. (If you're using a phone to dial-in to the internet, a firewall is not as important, though it

How do I keep my computer safe on the internet?

doesn't hurt to have one. A software firewall may be your only option, though.) More: [What's a firewall, and how do I set one up?](#), [Do I need a firewall, and if so, what kind?](#), [So do I need SP2's Windows Firewall or not?](#).

- **Virus Scan** - Sometimes, typically in email, virii are able to cross the wall and end up on your computer anyway. A virus scanner will locate and remove them from your hard disk. A *real time* virus scanner will notice them as they arrive, even before they hit the disk, though at the cost of slowing down your machine a little. **Important:** because new virii are arriving every day, it's important to keep your virus definitions up-to-date. Be sure to enable the scanning software's automatic-update feature and have it do so *every day*. More: [Viruses: How do I keep myself safe from Viruses?](#), [I run Anti-Virus software, why do I still sometimes get infected?](#), [When do I actually need to run a virus scan?](#).
- **Kill Spyware** - Spyware is similar to virii, in that they arrive unexpected and unannounced and proceed to do something undesired. Normally spyware is relatively benign from a pure safety perspective, but can violate your privacy by tracking the web sites you visit, or can be annoying as "features" you didn't ask for are added to your system. The worst offenders are spyware that hijack normal functions for themselves - for example redirecting your web searches to other sites to try and sell you something. Of course there is such poorly written spyware that it might as well be a virus, given how unstable it can make your system. The good news is that, like virus scanners, there are spyware scanners that will locate and remove the offending software. More: [Spyware: How do I](#)

[How do I keep my computer safe on the internet?](#)

[remove and avoid spyware?](#), [What's the best Pop-Up Blocker?](#) [Anti-Virus Software?](#) [Anti-Spyware Software?](#), [Is Microsoft's new Anti-Spyware program any good?](#).

- **Stay Up-To-Date** - I'd wager that over 90% of virus infections *didn't have to happen*, because the vulnerability that the viruses exploit had already been patched. The user simply failed to install the latest patches and updates that would have prevented the infection in the first place. I still see this constantly, as some of the most popular articles here on Ask Leo! deal with exploits that were patched nearly 2 *years* ago. The solution is simple: enable automatic updates, and visit [Windows Update](#) periodically. More: [How do I make sure that Windows is up-to-date?](#).
- **Get Educated** - To be blunt, all the protection in the world won't save you from yourself. Don't open attachments that you aren't *positive* are ok. Don't fall for phishing scams - don't click on links in email that you aren't *positive* are safe. Don't install "free" software without checking it out first - many "free" packages are free because they come loaded with spyware, adware and worse. When visiting a web site, did you get a pop-up asking if it's ok to install some software you're *not sure* of because you've never heard of it? *Don't* say "OK". *Not sure* about some security warning you've been given? *Don't* ignore it. Choose strong passwords, and don't share them with others. More: [Phishing? What's Phishing?](#), [How do I get rid of all this SPAM?!?!.](#)
- **Secure Your Mobile Connection** - if you're traveling and using internet hot spots, free Wifi or internet cafes, you *must* take extra precautions.

How do I keep my computer safe on the internet?

Make sure that your web email access is via secure (https) connections, or that your regular mail is over a encrypted connection as well. Don't let people "shoulder surf" and steal your password my watching you type it in a public place. Make sure your home Wifi has WEP security enabled if anyone can walk within range. More: [How can I keep my email safe from sniffing?](#), [Can hackers see data going to and from my computer?](#).

- **Don't forget the physical** - an old computer adage is that "if it's not *physically* secure, it's not secure." All of the precautions I've listed above are pointless if other people can get at your computer. They may not follow the safety rules I've laid out. A thief can easily get at all the unencrypted data on your computer if they can physically get to it. The common scenario is a laptop being stolen during travel, but I've gotten reports of people who've been burned because a family member or roommate accessed their computer with out their knowledge. More: [How can I keep data on my laptop secure?](#), [What backup program should I use?](#).

It might seem overwhelming, but it's not nearly as overwhelming as a problem if and when it happens to you. And while we might want it to be otherwise, the practical reality of the internet, and computing today is that we each must take responsibility for our own security on-line.

## Related Links:

- Ask Leo! - [Can hackers see data going to and from my computer?](#)
- Ask Leo! - [Do I need a firewall, and if so, what kind?](#)
- Ask Leo! - [How can I keep data on my laptop secure?](#)
- Ask Leo! - [How can I keep my email safe from sniffing?](#)
- Ask Leo! - [How do I get rid of all this SPAM?!?!?](#)
- Ask Leo! - [How do I make sure that Windows is up-to-date?](#)
- Ask Leo! - [I run Anti-Virus software, why do I still sometimes get infected?](#)
- Ask Leo! - [Is Microsoft's new Anti-Spyware program any good?](#)
- Ask Leo! - [Phishing? What's Phishing?](#)
- Ask Leo! - [So do I need SP2's Windows Firewall or not?](#)
- Ask Leo! - [Spyware: How do I remove and avoid spyware?](#)
- Ask Leo! - [Viruses: How do I keep myself safe from Viruses?](#)
- Ask Leo! - [What backup program should I use?](#)
- Ask Leo! - [What's a firewall, and how do I set one up?](#)
- Ask Leo! - [What's the best Pop-Up Blocker? Anti-Virus Software? Anti-Spyware Software?](#)
- Ask Leo! - [When do I actually need to run a virus scan?](#)
- Microsoft - [Windows Update](#)
- Amazon.com - Best Selling books about [PC Security](#)