Internet Safety: 8 Steps to Keeping Your Computer Safe on the Internet

Ask Leo! » **Viruses and Malware**

Internet Safety is difficult. yet critical. Here are the eight key steps to internet safety - steps to keep your computer safe on the internet.

by Leo A. Notenboom, © 2013

Viruses & Spyware & Worms ... oh my!

The very concept of "Internet Safety" is almost an oxymoron these days.

It seems like not a day goes by where we don't hear about some new kind of threat aimed at wreaking havoc across machines connected to the internet.

Anti-Microsoft sentiment coupled with the massive installed base make Microsoft products, and particularly Microsoft Windows, an irresistible target for hackers and "script kiddies". In recent years, products like Adobe Reader, Java, Flash, Firefox and more have come under attack as their popularity has increased. Even the Macintosh is no longer invulnerable.

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

1. Use a Firewall

A firewall is a piece of software or hardware that sits between your computer and the network and only allows certain types of data to cross. For example, a firewall may allow checking email and browsing the web, but disallow things like Windows file sharing.

Firewall: A firewall is a barrier between something that is potentially dangerous and something that you want to keep safe. The term comes from the automotive industry where ...**continue reading**.

From the **Ask Leo! Glossary**

If you're connected to the internet through a router, then you already have a type of hardware firewall preventing random networking-based external threats from reaching your computer(s).

If you're using a dial-up internet connection, a firewall may not be as important, although it doesn't hurt to have one. A software firewall may be your only option, though.

- **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 the Windows Firewall or not?**
- **Is an outbound firewall needed?**
- **Additional Firewall articles** on Ask Leo!

2. Scan for Viruses

Sometimes, typically via email or other means, viruses are able to cross the firewall 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, but at the cost of slowing down your machine a little, and occasionally even interfering with other operations.

Virus: A virus is a computer program written by someone presumably with the intent of spreading and causing grief. Like a human virus, a virus makes the infected computer "sick": it causes poor performance, crashes, lost files, and data, or more. Also like a human virus, a computer virus ... **continue reading**.

From the **Ask Leo! Glossary**

Important: Because new viruses are arriving every day, it is *critical* 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*.

- **What Security Software do you recommend?**
- **Viruses: How do I keep myself safe from Viruses?**
- **Why wouldn't an exploit be caught by my anti-malware tools?**
- **When do I actually need to run a virus scan?**
- **How do I remove a virus if it prevents me from download or installing anything?**
- **How do I run an anti-virus scan if I can't boot?**
- **Additional virus articles** on Ask Leo!

3. Scan for Spyware

Spyware is similar to viruses in that they arrive unexpected and unannounced and proceed to do something undesired. Spyware can be relatively benign from a pure safety perspective, as it might "only" spy on you. But that's enough. It can violate your privacy by tracking the web sites that you visit, add "features" to your system that you didn't ask for, or record your keystrokes and steal your account login information for any online services that you might use.

Spyware: Spyware is a class ofmalware that, as its name implies, is typically designed to spy on you or your computer, silently collecting information that is subsequently sent on to others for typically nefarious purposes. Various forms of ... **continue reading**.

From the **Ask Leo! Glossary**

Some of the worst offenders are spyware that hijack normal functions for themselves. For example, some like to redirect your web searches to other sites to try and sell you something. Of course, some spyware is so poorly written 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.

- **What Security Software do you recommend?**
- **Spyware: How do I remove and avoid spyware?**
- **Is running two anti-spyware programs better than one?**
- **So just how sneaky can spyware be?**
- **Will using an on screen keyboard stop keyboard loggers and hackers?**
- **Additional spyware articles** on Ask Leo!

4. Stay Up-To-Date

I'd wager that over 90% of virus infections *don't have to happen*. Software vulnerabilities that malware exploits usually already have fixes available by the time the virus reaches a computer.

Vulnerability: A vulnerability is a bug or design flaw in software that allows that software to be used in some malicious and unintended way. All software has bugs, which are nothing more than ...**continue reading**.

From the **Ask Leo! Glossary**

The problem? The user simply failed to install the latest updates that would have prevented the infection in the first place.

The solution is simple: enable automatic updates in both Windows and applications, and visit **Windows Update** periodically.

- **How do I make sure that Windows is up-to-date?**
- **I got burned by Windows Update, should I just avoid it?**
- **How do I know if these update notifications are legitimate?**
- **From where should I get driver updates?**

5. Educate Yourself

To be blunt, all of the protection in the world won't save you from yourself.

Phishing: Phishing is the attempt to represent one's self - typically via email - as someone or some organization that you are not for the purposes of maliciously acquiring sensitive information. The most common examples are ... **continue reading**.

From the **Ask Leo! Glossary**

- Don't open attachments that you aren't *positive* are OK; attachments are one of the most common ways that malware sprads.
- Don't fall for phishing scams. *Be skeptical.* Phishing is a common way that online accounts are hacked into, and can lead to more serious issues like identity theft.
- 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 so 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 that you're *not sure of* because you've never heard of it? *Don't* say "OK".

Not sure about some security warning that you've been given? *Don't* ignore it, *research it* before doing anything.

And of course choose secure passwords and don't share them with *anyone*.

- **What's a good password?**
- **How long should a password be?**
- **How do I make a secure password if I can't use special characters?**
- **Is a periodic password change a good thing?**
- **Are Password Managers like Roboform and Lastpass safe?**
- **Can I check a download for viruses before I download it?**
- **Phishing? What's Phishing?**
- **I got a call from Microsoft and allowed them access to my computer. What do I do now?**

6. Secure Your Home Network and Your Mobile Connection

If you're traveling and using internet hot spots, free WiFi, hotel-provided internet, or internet cafes, you *must* take extra precautions.

Wifi - open: Open wifi is any WiFi connection that has not been configured with a password. Anyone with a WiFi-capable device can connect to an open WiFi hotspot. If a password is used on a WiFi connection, then ...**continue reading**.

From the **Ask Leo! Glossary**

Make sure that your web email access - or for that matter *any sensitive website access* is only via secure (https) connections or that your regular mail program is configured to use encrypted connections as well. Don't let people "shoulder surf" and steal your password by watching you type it in a public place.

Make sure that your home WiFi has WPA security enabled, if anyone can walk within range, and that you've changed your router's administrative password.

- **How do I use an open WiFi hotspot safely?**
- **Can hackers see data going to and from my computer?**
- **How do I secure my router?**
- **Does sharing a router make me vulnerable to those I share with?**

7. 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 that I've listed above are pointless if other people can get at your computer. A thief can easily get at all of the unencrypted data on your computer if they can physically get to it. Even login passwords can be trivially bypassed if someone has access to your computer.

Encryption: Encryption is the process of mathematically processing data using an encryption "key" - such as a password or passphrase - in such a way that ... **continue reading**.

From the **Ask Leo! Glossary**

The common scenario is a laptop being lost or stolen during travel, but I've also received many reports of people who've been burned because a family member, friend, significant-other or roommate accessed their computer without their knowledge.

- **How can I keep data on my laptop secure?**, **What backup program should I use?**
- **My computer was stolen. It's password protected, what files can the thieves see?**
- **I've lost the password to my Windows Administrator account, how do I get it back?**

8. Back Up

I know that backing up doesn't feel like a "security" measure, but ultimately it can be one of the most powerful ways to recover if you even encounter a security related issue.

Having a recent backup to restore to can quickly undo the damage done by almost any form of malware.

image backup: An image backup is a complete copy of a hard disk or other media being backed up. The copy is complete in that it can be restored to a completely empty hard drive - as in a replacement hard drive after a failure - and the result is ... **continue reading**.

From the **Ask Leo! Glossary**

Having a back copy of your data (*all* your data) can help you recover after computer is lost or stolen (not to mention when a hard disk dies).

Backing up your email and contacts can be a critical way to restore your world should your online account ever be compromised.

Backups truly are the silver bullet of the computing world: a proper and recent backup can help save you from just about any disaster, including security issues.

- **What backup program should I use?**
- **How do I backup my computer?**
- **Can't I just copy everything instead of using a backup program?**
- **How do I backup my GMail?**
- **How do I backup Windows Live Hotmail?**
- **More articles about maintenance and backup** on Ask Leo!

Overwhelming? It Might Seem So, But...

I know it all might seem overwhelming, but please believe me when I say that it's not *nearly* as overwhelming as an actual security problem if and when it happens to you.

The good news is that the majority of the things you need to do to stay safe on the internet are things that you setup once and let happen automatically thereafter, or new habits you form yourself based on the important things that you learn about keeping things secure.

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 online.

(This is an update to an article originally published June 19th, 2005 and updated periodically thereafter.)

Article **C2374** – January 25, 2013 **« »**

Leo A. Notenboom has been playing with computers since he was required to take a programming class in 1976. An 18 year career as a programmer at Microsoft soon followed. After "retiring" in 2001, Leo started **Ask Leo!** in 2003 as a place for answers to common computer and technical questions. **More about Leo.**

Want More?

Sign up for the Ask Leo! email newsletter where you'll get a regular dose of fixes to problems, tips to avoid getting into trouble, and even the occasional answer to why things are the way they are.

Visit http://newsletter.ask-leo.com and sign up today!

Leo A. Notenboom
MAINTAINING Windows 7
Backing Up
An Ask Leo! ebook
Trouble Backing Up? Let me show you how...
Maintaining Windows 7 Backing Up
Kindle and PDF for your PC, tablet or reading device
An Ask Leo! ebook

http://go.ask-leo.com/m7backstore