

Security and Privacy on Your Computer and Online

Sarah Houghton
Marin County Free Library

Introduction

Security has become an increasing concern for computer users everywhere. While you're at home or at work—downloading files, watching web videos, buying things at Amazon, or checking your e-mail—your computer is being assaulted by automated programs and live hackers looking for a way in.

Why do they do this? Money—most spyware, adware, viruses, and other nasty malware is designed to send you advertising, gather information on your surfing habits for advertising purposes, or, in the worse case scenario, use your identity to make purchases online. Some programs even use your computer to do the above things to other people. But with a little knowledge and some great free programs, you can protect yourself.

Some Signs that You're Infected with Something

- A new item mysteriously appears in your Favorites list, and no matter how many times you delete it, it keeps coming back.
- The internet connection seems to be noticeably slower than it was before.
- Your system (as a whole) runs noticeably slower than it did before.
- You get pop-up advertisements when your browser is not running, or you get pop-ups that address you by name.
- You enter a search term in IE's address bar and press Enter but instead of your usual search site, you are re-directed to an unfamiliar site.
- You run a search in a search engine (like Yahoo or Google), but are re-directed to an unfamiliar site.
- Your homepage changes itself to something different.
- Mysterious icons appear on your desktop.
- Programs appear in your Start Menu that you didn't install.
- A search toolbar appears in your browser (at the top or at the bottom) that you didn't put there, and no matter how many times you delete it, it keeps coming back.

How At Risk Are You?

Want to get some idea of how vulnerable your computer is? Go to the Audit My PC site at (<http://www.auditmypc.com>), a free site that tries to assault your computer.

- **To run the Firewall Test**
 - Click on **Start Check**, then click on **Firewall Test**. Check the **I agree** box, then click on the grey button **Firewall Test 1**. A little pop-up window will tell you the results. Go back in the browser, and do the same with Firewall Test 2.
- **To run the Spyware Remover Test**
 - Click on **Start Check**, then click on **Spyware Remover**. Scroll down and see the results in a table. It's going to show you how you "appear" to the outside world...what websites can glean from your computer when you visit their sites.
- **To run the Popup Blocking Test**
 - Click on **Start Check**, then click on **Popup Blocking**. Way down in the last paragraph, click on the link **popup blocking**. Scroll all the way to the bottom of the next page and click on **Click here to START the popup test**. It will throw popup windows at you and ask you to click on some of them as part of the test.

Secure Your Computer

#1—Turn off file sharing

File sharing opens a door wide to hackers—it's the first things a hacker looks for to access your computer. File sharing is also known as peer-to-peer networking, and is what people use to download music & movies from programs like Kazaa & LimeWire.

- How to turn off file sharing in Windows 98
(<http://site.lisco.com/support/wireless/pc/pc98fileshare.htm>)
- How to turn off file sharing in Windows XP
(<http://www.wellesley.edu/Computing/FileSharing/Windows/winxphome.html>)
- How to turn off file sharing in Mac OS X
(<http://wcts.whitman.edu/whit.bits/october2002/MacintoshFileSharing/FileSharingOSX.html>)

#2—Install a firewall

If you use an always-on broadband connection or a wireless connection, anything on your computer is accessible to hackers 24/7. Even if you use a modem, you are equally at risk—just only when you are actually logged on.

- If you don't have either a hardware firewall or the built-in Windows XP firewall on your home network, install the Zone Labs' ZoneAlarm software firewall (http://www.zonelabs.com/store/content/company/products/zna/m/compare.jsp?lid=pdb_zs2).

#3—Scan for Spyware

Spyware is software that covertly gathers user information through the user's Internet connection without his or her knowledge, usually for advertising purposes. Once installed, spyware monitors user activity and transmits that information in the background, compromising privacy & security as well as tying up system resources and bandwidth. Update often!

- **Preventative Programs**
 - **Spyware Blaster** (<http://www.javacoolsoftware.com/spywareblaster.html>) detects known spyware ActiveX controllers and prevents web pages from putting them on your system in the first place.
 - **Spyware Guard** (<http://www.javacoolsoftware.com/spywareguard.html>) detects malicious .exe programs, attempts to hijack your browser, and prevents spyware from being installed through Internet Explorer.
- **Cleaning Programs**
 - **Spybot Search & Destroy** (<http://spybot.eon.net.au/>) will search your computer for spyware that has already been installed, and then clean the files off of your system.
 - **AdAware** (<http://www.lavasoftusa.com/software/adaware/>) scans your memory, registry, and drives for known data-mining, aggressive advertising, and tracking components, and then clean the files off of your system.

#4—Have an Anti-Virus Program

There are around 70,000 known computer viruses that can be received by email or contracted just by web-surfing. Update often!

- If you can afford the \$50 pricetag, use Norton AntiVirus (<http://www.symantecstore.com/>) or PC-Cillin

(<http://www.trendmicro.com/en/products/desktop/pc-cillin/evaluate/overview.htm>).

- If you want a free anti-virus program, use AVG Anti-Virus (http://www.grisoft.com/us/us_index.php).

#5—Update your Operating System

Update your operating system as often as you can. Always run the latest patches and drivers for your system. As soon as patches are released, hackers are out there looking for people who haven't patched yet. Patches advertise existing flaws in the system.

- Windows updates (<http://v4.windowsupdate.microsoft.com/en/default.asp>)
- Mac OS X updates (<http://www.apple.com/support/>)

#6—Secure Instant Messengers

Every time you send an instant message you are sending plain text across the Internet. Like any plain text (email, Word document, etc.) it can be "sniffed" and read. Everyone wants to keep their IM conversations private.

- Try using Trillian (<http://www.trillian.cc/downloads/>), which will encrypt AOL Instant Messenger and ICQ conversations.

#7—Secure E-mail

When you send an email, it passes through several servers on the Internet. Anyone with the right software can sniff the data as it passes through the server.

- Try using Hushmail (<http://www.hushmail.com/>) is a free e-mail provider that uses 2048-bit encryption to keep your email safe and sound.

#8—Secure Your Files

Do you have sensitive files on your computer that you'd rather not have anyone find? Here are a few options for securing files.

- **Get PGP Disk** (\$59) to encrypt all your sensitive files (<http://www.pgp.com/products/desktop/personal/index.html>).
- **Store your files in the ThumbDrive Touch** (<http://www.thumbdrive.com/touch.htm>), a USB drive that uses biometrics in a built-in fingerprint reader to protect your data. \$70-\$300, depending on drive size
- **Password-protect your Microsoft Office files**
 - From within Word, Excel, or PowerPoint, click on the **Tools** menu and select **Options**.

- Click on the **Security** tab.
- Under "**File encryption options for this document**," type in a password and click **OK**.
- When you try to open the document, you will be asked to enter your password. Don't forget it, or you lose the document!

#9—Secure Passwords

Many programs, services, & utilities require a log-in and password. They need to be secure, and you need to remember them. How?

- Make sure your passwords are at least six to eight characters.
- Never use regular words. If the word is in the dictionary, don't use it. Dictionary programs are the first hackers use when trying to break a password.
- Combine symbols with numbers and upper and lowercase characters. Examples: naK@07! or 4&neBkc.
- Everyone seems to have many, many passwords right now. And the number keeps on growing. There are a number of software programs that will safely store your passwords for you so you don't have to write them down (a big no-no) or remember them. I recommend **Personal Vault** (<http://www.soft1st.com/>), which will generate, store, and encrypt all of your passwords for you.

#10—Secure Your Wireless Network (if you have one)

Don't think you need a secure wireless network? If your network is not secure, anyone nearby can tap into and use your wireless network to do just about anything—download music, spam people, anything! Wireless access points (wireless routers) are not safe "out of the box."

- Turn off beaconing. Beaconing sends a signal out with your service set identifier (SSID), and anybody can match up to it. Disable it, and the SSID in the client must match the SSID of the base station. Makes it harder for strangers to find your system and log on.
- Change the stock SSID
- Lock down your WAP using MAC addresses.
- Change your passwords on a frequent basis.
- Turn on WEP (Wired Equivalent Privacy). WEP has flaws, but it's better than nothing.

Secure Your Online Behavior

#1—Avoid Portal Sites

Many portal sites (search engine portals, shopping portals) will take over your system. They will change your homepage, add a search bar to your browser, change your default auto-search page, add bookmarks to your browser, add spyware & adware to your system, transmit viruses, install other various commercial programs on your desktop, in your system tray, or in your Program Files.

- You will often stumble upon these while searching for something through Google or another search engine—and the title for the page looks just like what you searched for (& it is, because the title of the page is written as you search to match your search criteria). You'll click on the link to the site, only to see a useless site, often with pop-ups. Examples are <http://www.trustedsearch.com>, <http://www.xupiter.com>, <http://www.coolwebsearch.com>, & <http://www.adtomi.com>.
- Avoid sites that have your search terms repeated over & over in either the title of the search result, the URL, or the text description.
- Be wary of really long, seemingly random URLs.
- Never click anywhere on a pop up window that these sites throw at you. Always click on the **X** in the corner of the window to close it. In extreme cases you will have to **Control-ALT-Delete** and shut down Internet Explorer to get out of the loop. Even clicking on a button that says "**CLOSE**" or "**NO**" won't help in most cases.

#2—Attachments

Don't ever, ever open attachments from people you don't know. Period.

#3—Downloads

Don't download random stuff! Avoid websites that install cute things like smiley faces and weather monitors (*as well as spyware*) such as

<http://www.weatherbug.com/> and <http://www.smileycentral.com/>

#4—Don't Fileshare

File sharing is the #1 way that malware gets installed on your computer. If you want to download music or movies (completely legally, of course), turn off the "upload" capability, so you are only taking files from others, not sharing yours.

#5—Ignore Spam

Don't click on links in spam e-mails, even if it's a "remove me from your list" link. You could get more than you bargained for from the site.

#6—Consider Changing your Browser

Most malware targets Microsoft Internet Explorer. Why? Because it's the most heavily-used program and it has lots of security holes just waiting to be exploited.

- Use Mozilla (<http://www.mozilla.org/>)
- Use Firefox (<http://www.mozilla.org/products/firefox/>)
- Use Opera (<http://www.opera.com/>)
- Use Safari (for Macs) (<http://www.apple.com/safari/>)

#7—Safe e-Commerce

- Shop only at reputable stores. If you've never heard of the company before, ask around before sending in your credit card. The National Fraud Information Center (<http://www.fraud.org/>) tracks disreputable Internet sites. Or, at least look on a company's website for a phone number and call it to make sure there's a person on the other end.
- Legitimate merchants will offer secure transactions. One way to check whether you are in a secure zone is to look for the "s" after the "http" in the URL. If it looks like "https" you're secure. Or you can look for the key or padlock icon in the lower left-hand corner of your browser window. If it's broken, you're not in a secure location.
- Use a credit card rather than a check or your ATM card when you shop online. By law, you are liable for no more than \$50 for unauthorized charges, in the unlikely event that someone does steal your account information. Have one credit card for online purchases only (with a low limit) so it's easier to track the activity.
- Never give your bank account number to an online merchant.
- Shred anything that contains your personal information (credit card statements, shipping invoices, etc.), so that someone going through your trash can't use your information.

This material has been adapted from material created by the author for training purposes at the Marin County Free Library.