

# Spyware, Scams, & Other Online Hazards

---

Do you know what evils are lurking on your computer? If you're online, you're at risk of a whole host of online hazards. Programs called spyware, adware, viruses, worms, and trojans (collectively called malware or spyware), may be doing bad things to your computer – and to you – without your knowledge. These problems are much more widespread than most people realize – almost every computer brought in for repairs is infected with spyware and viruses. The dangers are real, and the bad guys use very sophisticated tricks to get their malware onto computers.

## Spyware

### What is it?

Most broadly, spyware is software with malicious intent – by design, it does something bad to you or your computer. It's called spyware because it literally spies on you to gather information. Adware is a specific variety that makes ads appear on your screen (those darned pop-ups!), or redirects you to advertiser web sites. There are other names for it, but spyware is the most commonly used term.

Spyware infects millions of computers with the purpose of stealing your personal information, enabling identity theft, hijacking your computer, tracking your online activity, and selling information about you to anyone willing to pay for it.

### What are the risks? Why is it bad?

Spyware does all sorts of things, ranging from the merely annoying to the downright criminal. It may:

- use up your computer's system resources, memory, & Internet bandwidth, making your computer and/or Internet connection slow
- delete, modify, or disable files, folders, programs, and essential Windows components and services
- use worms, trojans, and "back doors" to open your computer to further invasions
- use your computer to send spam – it's estimated that 80% of the world's spam is sent by "zombie" home computers infected with "spam trojans" which were installed by spyware or worms.
- conflict with other programs, causing your computer to crash or freeze up
- hide the presence of other bad programs, and keep you from removing them
- install "keyloggers" which record *everything* you type, including passwords
- steal your passwords, credit card information, & other personal data to be used for identity theft
- monitor your web surfing habits and record the web pages you visit
- relay any of this collected data back to its makers & sell it to other companies or bad guys
- collect your e-mail address & make you the target of spam (junk e-mail)
- pester you with pop-up ads, even if you have pop-ups disabled in your web browser
- "hijack" your web browser, change your home page, and redirect you to other web sites

Spyware's ability to do all of these things is a tremendous personal and organizational security threat. It can lead to data loss, damage to legitimate software, impaired network performance, reduced productivity (for you and the Tech Support staff who have to clean it up), and, worst of all, identity theft.

### How does spyware get on computers?

- It may present a security warning saying that you're infected and/or need to install some kind of patch to protect your computer. These fake warnings can look very real.
- It may be installed by a "drive-by download": installed when you visit a web site or click a link, especially advertising links or those that say you won something. In these cases, you don't even have to do anything other than visit a web site or click a link.
- It may masquerade as something helpful, like a free virus scan or spyware removal program.
- It may hide inside of another program's installer: Many free programs install some form of spyware, especially file/music sharing programs (e.g., BitTorrent, Limewire, Kazaa, etc.), but also

screen savers, games, etc. They may or may not tell you that they're doing this; if they do, it will be in the license agreement, which they count few people actually reading.

- An e-mail or web site may make you think that you need to download something: For example, an e-mail may say that someone sent you an electronic greeting card but that you need to download a special viewer to see it, or a web site may say that you need to download a special "media player" to view their site.

## How can you avoid it?

- Don't download free programs, games, screen savers, etc., especially file/music sharing software. If you have kids, don't let them install anything on your computer without your knowledge. If you have a College-owned computer, do not install anything that is not from the SNC network without consulting with Tech Support first. If you already have peer-to-peer (P2P) file/music sharing software on your computer, uninstall it.
- Don't click on ads, offers, security warnings, or "you won!" alerts on web pages, especially those that appear in pop-up windows.
- Use spyware removal & protection programs to scan your computer for spyware and keep it from being installed (details below). Unfortunately, there are unscrupulous people who create fake anti-spyware programs that can make your problems even worse, so make sure you only use legitimate programs recommended by Tech Support. See below for details.
- Don't use Internet Explorer. Instead, use a more secure web browser like Firefox.
- Before installing software (other than big name-brands like Microsoft Office, Quicken, etc.), check online to see if it's considered spyware.

## Fake spyware removal programs

There are companies that produce *supposed* spyware removal programs that actually **are** spyware! Many of these have anti-spyware-sounding names like Spy Deleter, SpyKiller, and Spy Wiper, and come from what look like legitimate software companies, like a company called Enigma Software Group that makes a program called SpyHunter. Some of these try to confuse people by using names that are very similar to legitimate spyware removal products; for example, SpywareBlaster is a legitimate spyware removal product, while SpyBlast is fake. Don't install anything unless you're 100% sure it's legitimate.

## Removing spyware

We strongly recommend using anti-spyware programs that can scan your computer for spyware, remove it, and prevent it from being installed. There are several free programs that do basically the same thing, but we recommend using more than one, as often one finds things the other missed. For links to download these programs, see the Downloads page on <http://www.snc.edu/techsupport>.

## Scams, fraud, & other dangers

Most spam conceals a scam of some sort. The ultimate goal of most scams is identity theft or credit card fraud. Most scams are based on "social engineering" – getting people to drop their guard and do or reveal things they might otherwise refuse. Everyone thinks that they're too smart to fall for one of these scams, but the bad guys are very good at what they do, and it works because people *do* fall for it. It's so successful that organized crime has even been linked to it.

## Gone phishin'

"Phishing" is the term for scam e-mail that asks for your personal information. The objective of phishing is get enough of your personal information to access your account(s) and possibly steal your identity. The scammers send e-mail that appears to come from a recognized business (eBay, PayPal, etc.) or financial institution (American Express, Wells-Fargo Bank, etc.), or some other entity with whom you have a relationship, such as your employer or school. They ask you to reply to the e-mail or click a link and supply personal information (password, account number, date of birth, credit card information, mother's maiden name, etc.). They may even have a fake web site set up to look *exactly* like the real thing.

Don't fall for the scammers' tricks! Always be suspicious. Don't follow the instructions or links in any e-mail message, no matter how legitimate it looks. If you really think it might be legitimate, contact the business directly, preferably by phone. If you go to a company's web site, always type the address yourself, rather than clicking a link in an e-mail message.

## Web browser security

### Don't use Internet Explorer

One way to protect your computer from spyware & other security attacks is to not use Internet Explorer (IE). That's because IE – especially in its default configuration – is less secure overall than other web browsers like Firefox, Safari, and Chrome.

We recommend using Firefox as your primary web browser. We believe that this browser is the best choice, and would like the College community to use it whenever possible. Unfortunately, there are some web sites that only work in one browser, so you should always have more than one anyway.

### Browser hijacking

Browser hijacking is when a malicious spyware program or web site changes your browser settings, such as the start page or bookmarks/favorites, without your permission, and often makes it so that you can't change it back. Why would anyone want to hijack your browser? To force you to visit their web sites so that they can earn higher advertising revenues (on the web, advertisers pay based on how many people visit the site or click their ad). Browser hijacking is a symptom of a spyware infection, and means that you need to scan your computer with an anti-spyware program. Browser hijacking is less likely to happen with browsers other than IE.

### Blocking pop-ups

Pop-up windows are a common way that spyware gets installed on computers, by either getting people to click on a link in a pop-up window that installs the spyware, or by exploiting insecure programming features (mostly in IE). Fortunately, all of the newer web browsers now allow you to block pop-up windows – check your browser's settings/options.

If you still get a lot of pop-ups even after turning on pop-up blocking, the computer is probably infected with spyware, and you should scan the it with an anti-spyware program.

If you see any pop-up warning saying that the computer is infected, STOP. Do not click on anything. If you can close your web browser without clicking on anything on the screen, do so, but if not, the safest thing to do is to just turn the computer off (hold the power button until it shuts off). If you click anywhere on one of those warnings, even on what looks like a close or cancel button, you'll probably cause your computer to become infected.

## Other security measures

### Protect yourself from viruses, worms, & trojans

- Always use anti-virus software and keep it up-to-date. On campus, McAfee VirusScan updates automatically on all College-owned Windows computers on the network. For personal computers, we recommend Microsoft Security Essentials or another free product such as AVG Free or avast! Free. For links, see our downloads page: <http://www.snc.edu/techsupport/downloads.html>
- Configure your anti-virus program to automatically scan all e-mail, downloads, disks, and files. On campus, VirusScan is already configured this way on all College-owned computers on the network.
- Be suspicious of **all** e-mail attachments, no matter what type of file it is or who it's from. (Viruses & spam almost always fake the e-mail "From" line.) Even if you know and trust the person who sent the attachment, it may still contain a virus. If your anti-virus program automatically scans all e-mail & downloads, and you always have the most recent updates, you'll be mostly protected, although you could still be infected by brand new viruses. If you're suspicious of an attachment, don't open it. If it seems like fluff (jokes, etc.), just delete it. If you're not sure, you can always e-mail or call the person and ask them if they really sent it and what it is.

## Keep Windows & other software up-to-date

Microsoft frequently releases updates for the Windows operating system and Internet Explorer to patch security holes and vulnerabilities that are found. By default, Windows checks for updates automatically, although this feature may be turned off. To check or change this setting, look in the Control Panel. On College-owned computers, these options may be grayed out because our computers are kept up to date automatically.

When you run Windows Update, you'll have a choice of "Express Install" or "Custom Install." Choose "Custom Install" so that you can review and choose the updates before installing. Normally, you should install all "critical" or "high priority" updates.

Ideally, to be as secure as possible, you should also keep all of your other software – e-mail programs, web browsers, Microsoft Office, etc. – up-to-date as well, but this can be more time-consuming. Some programs have automatic update features, while for others you may need to start the process yourself from a menu option (look on the menus for the word "update"). The update settings for some common programs:

## Wireless security

If you have a wireless network set up at home, people you don't know may be accessing it and using your Internet connection! Before you say you don't care, consider this: What if that person sharing your connection commits a crime, such as hacking into a computer, spreading a virus, or putting illegal materials on the Internet? *You* could get in trouble, because the activity would be traced back to *your* Internet connection. In addition, that person and others may also be able to intercept your online transactions and access files on your computer.

Most people who set up wireless networks in their homes don't secure them properly, leaving their connections wide open and themselves vulnerable to these dangers. The solution is to secure your wireless access point. Because each wireless access point model is different, we can't give specific instructions, but the manual for your wireless access point should have instructions for enabling the following security precautions:

- Change the administrative account password
- Turn on WEP or WPA Encryption
- Change the SSID
- Disable SSID Broadcast

## Firewalls

Any time your computer is connected to the Internet, whether you're using it or not, it's at risk from hackers. To be as safe as possible and protect your computer from hackers, you should use an Internet firewall regardless of what type of Internet connection you use.

A firewall is hardware or software that helps keep out hackers, as well as some viruses and worms, that may try to reach your computer over the Internet. It essentially creates a boundary that helps keep the computer or network secure by preventing access by unauthorized users. Without a firewall, hackers may be able to access your computer and do things like steal your passwords and other personal information, install keylogging programs that record everything you type, or "hijack" your computer and use it to spread viruses, send spam, or hack into other computers.

### Hardware firewalls

The easiest firewall solution is a piece of equipment called a router, which has a built-in firewall. The main purpose of a router is to allow more than one computer to share an Internet connection, but routers protect those computers by essentially hiding them from the Internet. Most wireless routers also act as firewalls, but you have to make sure they're configured securely (see above).

### Software firewalls

A software firewall is a program you install that watches all of the Internet traffic on the computer and blocks or allows it based on your preferences. Software firewalls can be a bit annoying, especially at first, because they warn you every time there's any traffic, but once you get them "trained," they're not so bad.

**The built-in firewall in Windows:** Windows has a built-in “Internet Connection Firewall,” which is usually enabled by default. This firewall provides only basic protection, and does not include any additional security features. For more information, see Microsoft’s “PC security” page at <http://www.microsoft.com/security/pc-security/default.aspx>.

**Software you purchase/download:** There are several software firewall or security packages that you can purchase. Most of these are full security “suites” or packages that include, in addition to an Internet firewall, things like content filters/parental controls, privacy controls, pop-up ad blockers, spam filters, spyware/adware scanners, anti-virus software, etc. Some of the companies that make these products are McAfee ([mcafee.com](http://mcafee.com)), Symantec/Norton ([www.symantec.com](http://www.symantec.com)), and ZoneAlarm ([www.zonealarm.com](http://www.zonealarm.com)). ZoneAlarm also makes a free basic firewall. It’s hard to find on their site, so if you want to download it, go directly to <http://www.zonealarm.com/security/en-us/zonealarm-pc-security-free-firewall.htm>.

## **Assistance and questions**

If you have any questions or need more information, contact the Help Desk at (920) 403-HELP (4357) or [helpdesk@snc.edu](mailto:helpdesk@snc.edu). The Help Desk is for St. Norbert College students and employees only.