

Internet Safety & Computer Security for Families

by Darius Garsys and Vanessa Adams Garsys

Computer Security

Viruses & Worms: These can turn your computers into spam-sending **zombies**, log your personal information as you type it, delete your files or worse. The first line of defense against viruses and most other computer security issues, is a skeptical attitude about what you open and run. It can't be said enough: *Do NOT install or run a program from someone you do not trust!*

The next line of defense for the things you cannot see is a good antivirus program. Recommended:

- Norton Antivirus from Symantec
- AVG Antivirus from Grisoft – Free version available.
- PC-Cillin from TrendMicro

Last, if you receive an **attachment** in your e-mail that you are *NOT* expecting, from someone you do *NOT* trust, do *NOT* open it!

Spyware: This culprit is usually loaded in two ways. (1) Piggybacked into an installer for some “free” program (usually file sharing) or toolbar, or (2) by visiting the wrong webpage while using Internet Explorer. A few programs reliably help to protect you from spyware and a few help get rid of it. Recommended:

- Microsoft Anti-spyware: Free. Bought from Giant Software. Protects and removes. Still **beta**.
- Ad-Aware: Free. Removes. The paid version protects.
- Webroot Spysweeper: Free for 30 days. Protects and removes.
- Spybot Search & Destroy: Free. Good, but not kept as up to date.

The latest wrinkles by spyware makers include uninstalling protective software, and **malware** pretending to be anti-spyware scanners.

Firewalls: Use for software and hardware. Users with laptops are highly advised to get a software firewall as well. Think of it as a fence around your computer(s) with a guarded gate. This prevents worms and hackers from exploiting weaknesses in your **Operating System** and setup. The default firewall in Windows XP (Service Pack 2) is usually good enough for this purpose. Bellsouth **DSL Modems** also act as basic hardware firewalls, while most **cable modem** users should get a home router, especially if they plan on sharing computers and printers. Recommended:

- Zone Alarm: Personal (software). Free, but can be problematic for some.
- Norton Personal Firewall: Personal (software). Often packaged with Antivirus as part of “Norton Internet Security.”
- Linksys, Netgear, and D-Link Cable/DSL routers: (hardware) routers to protect one or more computers.
- Hardware routers are more secure than software routers but do not protect laptops away from home.

Browsers: Internet Explorer is inherently insecure and hijackable, almost by design. While some banks and sites (the realty MLS site, notably) do not work well with non-Microsoft browsers due to not following standards, for everything else the best browser to use is that currently provided by the people who wrote Netscape: Mozilla Firefox. For sites where you *need* Internet Explorer, go ahead and use it. Firefox is available at <http://www.mozilla.org>.

Internet Safety

Passwords: Don't use easy to guess passwords (pet or children names, etc.) Use alphanumeric passwords instead.

Spam: E-mail addresses are often farmed from web pages including **Bulletin Boards**. Most often they are sold from gathered marketing profiles or randomly guessed for common e-mail providers. Always read the privacy policy when you submit personal information. If there is an offer for advertising always check “no”. The spam you're getting can be filtered with built-in rules and blocklists. The best filters are “Bayesian” and learn from your choices. Recommended:

- Spambayes: Plug-in for Outlook (requires some technical expertise for Outlook Express). Simple, effective, free.
- Norton Antispam: Not quite as effective but easy to set up for all common e-mail programs.
- Mozilla Thunderbird: Free e-mail program similar to Outlook Express, but with good built-in spam filter.
- Mail App – on the Mac has a far better antispam filter than Microsoft Entourage. Free with Mac OS X.

Phishing, Scams and Postcards: There are many scams online. **Phishing** refers to sending an e-mail requesting you to follow a link to “validate” your banking information that has been lost due to some excuse or other. Following the link will usually lead to a very official-looking site where they harvest your personal info to steal you blind. If you ever see an

“@” symbol in a web address - *Beware!* Someone is hiding the true location. A recent twist on this and malware is to send **Postcard** notices requesting you to follow a link to see a postcard sent by a friend or family member. This will often result in software being loaded without your permission or harvesting personal information. **Scams** include the classic “Nigerian Scam” where you are e-mailed a request to deposit a large cashier’s check, *immediately* send a large chunk via personal check and you “keep the rest for your trouble.” The cashier’s check is forged. See: <http://www.snopes.com/crime/fraud/nigeria.asp>

Online Chat and games: There are First-Person-Shooter (FPS) type games, board/card games, and outright chat rooms and Instant Messaging (IM). FPS’s are much like cowboys and Indians with gorier imagery and the talk sometimes turns trashy. “Clans” with regulars who play together as teams tend to be more professional. More traditional board and card games are much more social, and give more room for conversation, but also tend to be relatively safe, usually with less profanity. Chat rooms and IM’s can range from innocent chatting with friends to online predators. While there are “logging” programs that will let you know who your children talk to, most require technical savvy to install and few of them will log your children’s activities without it being obvious they’re being monitored. The best solution, like with TV and games, is parental involvement.

Online Predators: Talk to your children about not responding to offensive or dangerous e-mail, chat, or other communications. Report any such communication to local law enforcement. Tell children not to meet in person with anyone they have first “met” online. For more online safety tips see: <http://www.netsmartz.org>. If you suspect online “stalking” or sexual exploitation of a child, report it to your local law-enforcement agency. The National Center for Missing & Exploited Children (NCMEC) has a system for identifying online predators and child pornographers and contributing to law-enforcement investigations. It’s called the [CyberTipline](http://www.cybertipline.org/)[®]. Leads forwarded to the site will be acknowledged and shared with the appropriate law-enforcement agency for investigation. See <http://www.cybertipline.org/>

Glossary

Attachment: A file (word document, picture, PDF) included with an email message.

Beta: A computer program that is still in development but far enough along to be reasonably reliable.

Bulletin Boards: Online message boards where people post messages on a topic and reply, not in real time. Along with comments, is a common “fan” element of many sites.

Cable Modem: Turns the broadband in your cable line into a network signal your computer can use.

DSL Modem: Turns the broadband in your phone line into a network signal your computer can use.

Firewall: A piece of hardware or software that allows or refuses certain types of internet messages to speak to your computer. Think of it as a guarded gate.

Malware: A type of spyware that changes how your computer works. Usually an active program constantly running in the background.

Operating System: The software that runs your computer, allows you to copy files,, run other programs, etc.

Spam: The internet term for junk e-mail. The name is taken from a Monty Python routine where everything on the menu has spam, even though the customer doesn’t want spam.

Spyware: Software that monitors what websites you go to. Also called Adware and Malware. Spyware can reset your home page and your search page, slow up your computer, pop up extra windows, and pop up ads when you are not browsing. In extreme cases it changes how you get online, and is effectively unremoveable without reinstalling Windows.

Virus: Program that reproduces itself, and causes damage to computer systems. Most commonly distributed through email. Most modern viruses randomly choose names from your address book for both “To:” and “From:” addresses, making it more difficult to trace the source when you receive one.

Worm: Generally lumped under viruses, worms actively hunt local networks for computers to load themselves into.

Zombie: Computer taken over or “owned” by a virus or worm. Most often used to send Spam.