

American Academy of Pediatrics

DEDICATED TO THE HEALTH OF ALL CHILDREN™



Be Safe, Not Sorry On Line (Part 1) (from Senior Bulletin, September 2005) Jerold M. Aronson MD FAAP

Today, many of us are purchasing computers to “surf” the World Wide Web for continuing education, on-line banking and brokerage activity, and to communicate via e-mail. In this article I will cover:

- Part 1
 - o Having the right computer hardware
 - PC
 - Modem
 - Internet Connection
 - o Having the right software
 - Web browser
 - E-mail program
 - Virus, Spyware, and Spam protection
- Part 2 (to be published December 2005)
 - o Safe “surfing” strategies
 - Using “secure” web sites, especially for financial transactions
 - Creating secure User ID and Passwords, and e-mail addresses
 - Minimizing e-mail risks
 - Netiquette

Having the right computer hardware:

Most, if not all computers (PC or Apple) are internet-ready. That is, they contain either a built-in modem (communication hardware) or network connection devices (wireless or plug-in) or both. However, all internet-ready computers need an internet connection (ISP = Internet Service Provider) to function. You have several ISP choices depending upon the connection and web-surfing speed (broadband vs. dial-up) that you wish and the price that you are willing to pay.

The most basic type of Internet connection is called a dial-up connection. This connection is made through a modem (the communication mechanism in computers) that uses a regular telephone line to connect to the Internet. The modem must dial the telephone every time it wants to connect to the Internet, hence the name dial-up connection. The fastest modem that you can use for this type of Internet connection is called a 56K modem. Since a regular telephone line is analog, and a PC is digital, the modem converts the analog signals that it receives from the telephone line into digital signals that the computer can comprehend. These conversions take time; compared to other Internet

connections and produces a relatively slow connection and ties up your telephone line. Thus, frequent users often install and pay for a second telephone line. However, dial-up is the least costly ISP and is generally sufficient for e-mail use and non-graphic intensive web surfing. A dial-up connection intermittently connects your PC to the internet.

In contrast, "always on" broadband is a high-speed Internet connection that makes surfing the web more enjoyable. It also easily accommodates the video, audio, or complex graphics that are becoming commonplace on the Internet. Broadband connections are able to transmit both voice and data over the same line at the same time and are always on (no dial-up is required). A second telephone line is not necessary.

Broadband connections are provided either by the telephone company (DSL) or by your television cable company. Your choice will be based on local availability and cost. Each service may not be available in all areas. The company you choose will either provide or rent a special modem (and/or other equipment) that connects your PC to their cable or DSL line. You do not need cable TV to purchase broadband cable. However, most cable companies give price breaks on Internet access to their cable television customers. In general, the company that provides your broadband connection will either serve as your ISP or provide you with an ISP.

Cable broadband has several drawbacks. First, it is a shared connection, meaning you share the "pipeline" with your neighbors that can decrease your connection speed. In addition, because cable modem connections are always on, they, like DSL connections, make you more vulnerable to hacking and security breaches (more on this later). And cable broadband often is more costly than DSL.

DSL is a special telephone line that also provides high speed Internet access. DSL can be as fast as cable. The closer you are to the main telephone switching station, the faster your connection speed will be. If you are accustomed to using a regular dial-up connection, you may well be amazed by the speed of a cable or DSL connection. It will make surfing the Internet a much more pleasant experience. How fast is fast? Just for a quick comparison, if a file takes one hour to download over a standard 56K modem, it will take between 2.2 and 13 minutes (cable), and between 2.2 and 26 minutes (DSL). This will be important for users that like to listen and view both audio and video on the web, or plan to use their PC to send photos/video to family, friends, and colleagues. So if you want to do some speedy surfing, think broadband. Web sites like Broadband Reports at www.broadbandreports.com can help you figure out what services are available in your area and also have message boards where people tell about their experiences. Most public libraries have high speed broadband connections. Try out broadband or dial-up at friends or neighbors to see what you prefer.

Note – when choosing a connection and/or ISP, find out what actually comes with your account. Do they provide the hardware and software you need? Will they

help you set up your computer so that you can make the Internet connection for the first time and is unlimited free technical support available? How many e - mail accounts and web storage space comes with your account? See if they provide free e-mail antivirus and anti-spam scanning by going to their web site.

Sometimes these features must be turned on. Go to your ISP website online and select member/customer services.

Having the right software:

At a minimum, your computer will need a web browser, and software protection from viruses, spam, and spyware to surf safely. Broadband connection users should have and use "firewall" protection because the PC is "always on" and potentially vulnerable to "hackers". Some of these software protections (e.g. firewall) are built into new PC operating systems e.g. Windows XP SP2, or provided as "start-up" versions (usually anti-virus/spamware that you can view and install from your PC desktop. In general, Apple computers seem less vulnerable to hacking or viruses.

Note – always install firewall, and anti-virus software before you connect to the Internet for the first time to assure that you are protected.

Remember, there is a significant amount of security built into the utilities of the software that is bundled with your computer. This includes your operating system (especially the new Windows XP SP), E-mail clients like Outlook Express or task managers/e-mail clients like Microsoft Outlook, and Microsoft Internet Explorer, the most frequently used web browser. Review the default security settings on your software and set them to either the manufacturers default recommendations or choices that you prefer. See the Microsoft site at <http://www.microsoft.com/athome/security/default.mspx> for up-to-date information on how to optimally use these products.

Internet Explorer ("IE") is automatically loaded onto all PC's as part of the Windows operating system and is bundled with Outlook Express (software to manage e-mail communication, etc.) Other web browsers, e.g. Netscape, Firefox, Opera are available (see their websites for more information). However, I suggest that novices stick with what Microsoft provides as part of its operating system. Similarly, there are alternatives to Microsoft Outlook Express to manage e-mail. Users that plan to synchronize their PDA's (address book, etc.) must use Microsoft Outlook (usually found in Microsoft Office), that has many different task management functions beyond e-mail. One benefit of using Microsoft Outlook is that you can have Windows handle operating system and Outlook updates automatically. For example, in Windows XP, right-click on "My Computer," then "Properties," "Automatic Updates" and "Keep My Computer Up To Date" to protect your computer from "hackers".

Firewall software sets up a barrier against "hacker" (outside) access to your computer and its files and is essential if you choose a broadband connection.

Windows XP has a built-in firewall. Assure that it is turned on. It works well for most users. Other firewall software (see Home Firewall Guide at <http://www.firewallguide.com/>) can be added. Their use may produce software incompatibility with other programs, however.

Anti-virus software is critical. Antivirus software programs are basically the same. For approximately \$50, no matter which application you buy, you're purchasing a scanner engine and a year's worth of signature-file updates. An antivirus product scans your computer for evidence of viruses and then removes viruses when detected. You need the updates to identify the latest viruses and worms, and most antivirus application now automatically download the updates behind the scenes, so you don't have to worry about it. The engines themselves *match patterns*, that is, they look at files on your hard drive and compare them to the signature files you just downloaded. If there's a match, the suspect file goes into *quarantine*, a protected folder on your hard drive where it can't hurt your system (again, this too has been automated so that you hardly ever notice this process). Lately, antivirus apps have added *heuristics*, the ability to sense a new virus or worm before a signature file has been downloaded based on malicious behavior. Also, most every antivirus app will check both incoming and outgoing e-mail messages for signs of infection. The differences, then, lie in the nuances of these apps. How much of your system resources do they hog? How fast or how often does the vendor release its signature-file updates? And what additional features does the software offer?

Popular anti-virus programs include, Norton Anti Virus 2005 (industry leader with starter versions usually supplied on HP and Compaq PC's), McAfee VirusScan 9.0 (starter version on Dell PC), and Trend Micro PC-cillin Internet Security 2005. Both Norton and McAfee market stand-alone anti-virus software. However, they can be purchased with integrated firewall protection at additional cost. PC-Cillin Internet Security 2005 (CNET's Editors Choice for 2005) includes an antivirus scanner, a firewall, antispam and antispyware capabilities, parental controls and more! Norton and McAfee anti-virus software slows all but the fastest computers, in contrast to PC-cillin. Calling Norton technical support is expensive after initial start-up. I suggest that you start with anti-virus programs that came with your PC before investing in a new product. And as before, during set-up, select auto-update to assure that your anti-virus software is updated regularly behind the scenes to maximize your protection. Typically, you will need to renew your "subscription" annually, to receive updates to protect against the latest viruses.

Antispam and antispyware software protect your computer from malicious mischief, performance deterioration, and identify theft. Spyware secretly gathers information about a person or a company and relays it back to advertisers or hackers. Spyware can infect a computer through a virus or through the installation of new software. Spyware aids identity theft and data corruption, and tracks users' online activities without their knowledge. Use anti-spyware programs such as Ad-Aware (www.lavasoft.com) or Spybot (<http://www.safer-networking.org/en/download/>) available either as "freeware" or purchasable.

Microsoft has a free anti-spam product for Windows XP SP2 “Microsoft Defender” and a “3 in One” product called Windows Live OneCare that contains enhanced 2-way firewall, anti-virus, and anti-spam software. See www.microsoft.com for more details.

**Be Safe, Not Sorry On Line (Part 2) (from Senior Bulletin, December 2005)
Jerold M. Aronson MD FAAP**

In Part 1 of “Be Safe, Not Sorry On Line, I covered the following:

- Having the right computer hardware
 - o PC
 - o Modem
 - o Internet Connection
- Having the right software
 - o Web browser
 - o E-mail program
 - o Virus, Spyware, and Spam protection

In Part 2, I will cover:

- Safe “surfing” strategies
 - o Using “secure” web sites, especially for financial transactions
 - o Creating secure User ID and Passwords, and e-mail addresses
 - o Minimizing e-mail risks
 - o Netiquette

Section members that would like to view Part 1 are encouraged to go to login to the AAP Senior Section webpage and safely read the article on line.

Surfing Safely

Learn to recognize a Secure Site on the web, especially for financial transactions. Look for <https://in> the Address Bar. HTTPS indicates the Web site uses Secure Sockets Layer, the most common encryption protocol. This indicates that you can safely enter personal information. When you visit a secure Web site, Internet Explorer, will indicate that the site is secure by displaying a lock icon on the status bar. Always make sure a site is secure before using it to send any confidential information such as your credit card number. Look for Information about specific site Security Certificates that confirm safety and security on the site.

Making cookies is not only for politicians! Many Web sites identify you as a unique user by storing information in a small text file on the hard disk of your computer. This file is called a cookie. Cookies enable a Web site to store information about a visitor, retrieving that data for identification in the future. Cookies record bits of information such as user name, password, and shopping purchases. This enables the Web site to recognize a returning visitor without

their having to reenter identification information.

Many Web sites use cookies to add to your Internet enjoyment. Cookies allow Web sites to be customized to your needs. For instance, a weather Web site may ask for your zip code. It will then store your zip code in a cookie so that next time you visit the site you can get your local weather without having to enter your zip code again.

Routinely delete cookies and temporary files from your PC to minimize the risk of identity theft. In Internet Explorer, go to Tools/Internet Options. Under General Tab/Temporary Internet Files click on Delete Cookies and then click on Delete Files. Although these files speed up your connection to web pages that you have visited in the past, your PC will automatically re-create these pages the next time that you go to the specific web page. Deleting files this way may eliminate cookies and other files placed onto your computer surreptitiously.

Take the following additional precautions to safely surf and prevent your PC from being invaded:

- Do not download free software without reading licenses and privacy notices association with the programs.
- Don't download programs from sites you don't trust or know. You may well be exposing your computer to spyware by downloading some of these programs.
- Do not use – or let your grandchildren use – Kazaa or any other file-sharing network. They are prime breeding grounds for spyware and other malware.
- Never agree to download an Active X program (often necessary to display graphics or to perform software diagnostics on your hard drive) from a web site unless you are 100% sure it is honest.
- If you have Windows XP or Microsoft Office 2003, upgrade to Service Pack 2. Set your operating system to automatically search for, download, and install all Microsoft security patches.
- Don't click on links within popups—pop-up windows are often spyware activators. Clicking on a pop-up link may install spyware software on your computer. Close the popup with the "X" on the title bar and not the "close" link, if any, within the window.
- Adjust your browser properties to kill popup windows. These are often generated by some kind of malicious active content. Be wary of free downloads. Many sites offering customized toolbars or other goodies are come-ons.
- Choose "no" when asked unexpected questions. Be careful of an unexpected dialog boxes asking whether you want to take a given action. Always close the dialog box by clicking the "X" icon in the title bar.
- Don't follow e-mail links offering anti-spam help. Don't trust 'em! These links may actually install the spyware they claim to be keeping off your system.

- Spam is not only our old-time favorite luncheon meat! Simply put, Spam is an unsolicited e-mail usually to many people. A message written for, and mailed to, one individual that is known to the sender is not spam, and a reply to an e-mail is not spam, unless the "reply" repeats endlessly.

E-Mail is the most popular web application. Major goals of the vendors (including Microsoft) producing web browsers, anti-virus, anti-spyware, and anti-spam software are to make browsing and e-mail more enjoyable, provide protection from potentially harmful downloads, screen unsafe e-mail attachments that could potentially spread viruses, etc. Your ISP will usually provide one or more e-mail addresses and mailboxes. These e-mail addresses are yours as long as you continue to subscribe to the ISP. If you stop subscribing to the ISP, you lose your e-mail address. However, you might choose to use one specific e-mail only for financial transactions, another for personal/family mail, and another for business. Your e-mail program can easily be set to download all mail from all e-mail addresses each time you login to your e-mail. To accomplish this, open your e-mail software, e.g. Outlook Express, click on Tools, Click on Accounts and select Mail Tab. Select Properties for the "default" e-mail address and copy the settings for each of the tabs shown onto a piece of paper. Then, while in the Mail Tab, select Add Mail. This will open a "Wizard" that will walk you through the steps of adding a new e-mail address. For all fields, except the e-mail address, use the data that you have copied to the paper. In the field for the e-mail address, use the new e-mail address, e.g. name1@att.net or name2@att.net, etc. This will assure that all e-mail addresses for the same ISP are downloaded at the time you open your email program.

In contrast, MSN Hotmail (www.hotmail.com) and Yahoo (www.yahoo.com) provide free, permanent e-mail accounts that can be accessed from any PC connected to the Internet, anywhere as well as being downloaded to your e-mail program. AAP Fellows can obtain a free, e-mail address by logging into the Members Only Channel at www.aap.org and signing up. A significant benefit of using these e-mail accounts is that these entities invest substantial resources to provide additional virus and worm protection and minimize spam to improve user satisfaction. However, these applications often limit the size and type of e-mail attachments (important with sending pictures, etc.). For more information on "How to protect yourself from spam (and viruses) using Hotmail and Outlook" see <http://security.msn.com/articles/msmailprotect.armx>

Here are some additional tips for a more enjoyable and safe e-mail and browsing experience:

- View your e-mail first via the "netmail" or "webmail" service provided by your ISP. Each ISP usually provides access to your secure e-mail at via their Home Page. Here is how to check your "netmail". Go to the webpage of your ISP (e.g. www.comcast.net or <http://webmail.att.net> or <http://netmail.verizon.net>) and click on login. Enter your ID and Password and view your e-mail. Delete any/all suspicious e-mail before downloading it to your PC. Logout and then open your e-mail program. Your e-mail will

automatically download into your mailbox. Viewing e-mail on the web first provides additional virus and worm protection since suspicious e-mail never makes it to your computer. This is fast and convenient, especially with broad band connections.

- Never open e-mail attachments from unknown senders or the message is unexpected. If it comes unexpectedly from someone you know, check with the person to verify they sent it. If it appears to come from a trusted source (a company that you do business with, for example), try to verify they sent it before you open it.
- Choose your passwords carefully--The hardest passwords to crack are at least 8 characters long and mix numbers, symbols, and letters. Don't share them. Change them monthly, especially with financial accounts.
- Never use your Social Security number for either a UserID or Password.
- Create extra e-mail IDs. Use one for registering with commercial sites or newsletters, another for your message-board and chat-room identities, and another for corresponding with friends. Use more than one e-mail address-- Use secondary addresses when registering with commercial sites, signing up for newsletters, etc. Your e-mail program will enable you to download mail from multiple e-mail addresses automatically each time that you sign on.
- Protect yourself from identity theft. Be wary of requests or "phishing"-- Scammers are great mimics. In general, most scams are distributed through unsolicited commercial e-mail or spam. Phishing is a technique used by spammers to obtain, or fish for, private consumer information like bank account numbers, social security numbers, and credit card information. Home e-mail users who do not have firewalls protecting their networks are frequent "phishing" targets. According to the Federal Trade Commission (FTC), the "phishing" e-mails pretend to be from familiar businesses - for example, like Internet Service Providers (ISP), online payment services or your bank or Credit Card Company. The e-mail might say "Your credit card is due to expire. Please enter updated information now" or "Your account has been placed on hold due to security reasons. Please verify your identity by clicking on the URL below." The E-mails instruct users to update or validate billing information to keep their accounts active. The scam directs users to click on a URL address in the body of the e-mail that directs you to a look-alike Web site of the legitimate business. Consumers think they are responding to a valid request. Unknowingly, consumers submit their financial information - not to the businesses - but the scammers, who use it to order goods, services and obtain credit. They create e-mails and Web sites asking for your credit-card numbers and passwords, and these sites can be dead-ringers for legitimate corporate sites you might be doing business with. **Whenever you get a request to give information, don't click through a message to a Web site. Instead, go to your browser and login to the web site directly by typing the address of the specific company into the Address Bar e.g. <http://www.bankofamerica.com>** . Then login to your account with your UserID and Password and check your data. Note – Bank of America recently informed me when I suspected that I was being "phished" that they do not send e-mails to customers about their account. If they have a problem, they

will call you by telephone.

- Be wary of get-rich-quick schemes or better-than-can-be-believed prices on products. Use caution when responding to requests for money to support charities. Watch out for requests to provide or confirm personal information from unknown sources. If you have any questions about what you have been asked to do, contact the corporation that you believe has sent you the e-mail or other communication.
- Avoid publishing your address on any Web page, especially in a "mailto:" link. Spammers search out these addresses and add them to their mailing lists. To see if your address appears anywhere on the Internet, go to our [Search page](#) and enter your full e-mail address. If any results are shown, contact the page owner and ask for it to be removed from the page.
- Don't place your preferred e-mail address on a Web page. Use a public e-mail address (Hotmail or Yahoo) for these listings. That enables the anti-spam software of Hotmail or Yahoo to limit your spam
- More convenience=more risk--Only save your ID and password on an authentication screen if you are the sole user of the computer you're on. If you're on a public computer, don't save your password, and be sure to fully log out and close the browser to assure that your ID and Password are deleted and cannot be viewed by the next user.
- Starve spammers – Spammers get paid by the number of click-throughs and sales. If you want to buy a product, use a Search Page (www.google.com, www.yahoo.com, etc.) to find the appropriate Web site. Don't buy anything through spam messages, and better yet, don't even open them. If you do, you only encourage the spammers!
- Use e-mail filters via your e-mail client and/or ISP. For example, at Outlook Express/Tools/Message Rules one can Block Senders or enter Subject Line or Content words that will be blocked if they appear in an e-mail. The risk is you may miss e-mail from trusted individuals whose e-mail address has changed.
- Back-up critical data (files/pictures) regularly. Backing up data means making a copy of it on another medium. For example, you might burn all of your important files onto a CD-ROM or second hard drive. This is essential in the event that your computer becomes "infected" and/or incapacitated.

Finally, use good manners called Netiquette ('Net + etiquette) while using e-mail.

- DON'T USE ALL CAPITAL LETTERS (it's hard to read and is considered shouting);
- Be brief;
- Use meaningful subject lines;
- Quote just enough from what you're answering to provide useful context;
- Don't forward to everyone you know jokes, rumors, hoaxes, chain letters, charity appeals, and such, even if the arriving note tells you to do so;
- Don't send "Me too" notes to discussion lists;
- Don't send attachments without getting the recipient's permission;

- Send plain text e-mail unless all your addressees prefer HTML format; and,
- Accept and cheerfully answer questions asked by people newly online — remember that we all started with the basics. The [Netiquette Home Page](http://www.albion.com/netiquette/) (<http://www.albion.com/netiquette/>) is an entertaining and informative reference

Remember; send your questions/concerns to jmaronson@aap.net. I'd love to hear from you. While all questions may not be able to be answered personally, your feedback will help identify topics for future articles.