Safe Internet Usage:

Please use this as a guideline for best practices for Internet usage, including web browsing, e-mail usage, and keeping your PC safe.

There are links to all the software mentioned below from www.jagcs.com, click on Links on the left hand side. Most of them are included on this CD. Remember, if you like the free software, consider donating or purchasing the full version to show these companies that you appreciate their hard work and dedication to keeping your PC running at top performance.

Windows update: Microsoft makes updates available that fix flaws and vulnerabilities in their software. By running windows update and applying patches, you can harden your system against known issues.

Antivirus Software: Make sure you have an antivirus software installed and that the antivirus software is up to date and has current definitions. If you have an expired version of software, or you can no longer update it's definitions, then you are not protected. AVG Antivirus by Grisoft (www.grisoft.com) is an excellent FREE antivirus software.

Pop-up stopper: Pop-ups can launch programs behind the scenes that try to install or place programs onto your PC without your knowledge. The best defense is a good offense. A great free Pop-up stopper can be found at www.paniware.com. Windows XP Service Pack 2 includes a Pop-up stopper.

Anti-Spyware program: If you are running Windows 2000, Windows XP, or Windows Server 2003, then you can run Microsoft's free Anti-Spyware program. If you have an older version of Windows, I suggest something from a reputable company such as WebRoot, which makes the SpySweeper software and is headquartered in Colorado (www.webroot.com). These programs can run in the background like antivirus software and will monitor your system to keep malware/spyware/adware from getting on your PC.

Spyware Remover: Adaware works very well, and is a free program. It doesn't' monitor your system, but you can run it on a regular basis to have it find and remove malware/spyware/adware from your system. Find it at www.lavasoft.de. It also has definitions that should be updated prior to running it.

Only download or install programs that come from trusted sources. If a window pops up telling you your system is infected, that you need a program to make your system run faster, or anything that wants you to install it without you having purposely started a download, close the window without clicking on yes, no, or other.

Keep your browser cache to a minimum and cleaned out. For Internet Explorer, click on the Tools menu, choose Internet Options. For Temporary Internet files, the default space is far too large, considering it's a percentage of your hard drive. For a 60 GB hard drive, 10% would be 600 Megabytes. That's a lot of temporary internet files. Click on settings and change this down to 1% of your disk space, or enter in 10 MB. What a cache does is keep 'copies' of the web sites you browse, so that if you browse away and then browse back, your computer will get the web site from your cache rather than going back to the real web site. Periodically come in here (depending on your internet browsing behavior) and click on the Delete Files button to remove the temporary files. You can also clear your browser history here.

Firewall: It's a good idea to run a firewall, you can purchase one of there are free ones available (www.free-firewall.org). Be prepared to 'train' the firewall about what is safe and what your computer can do and allow. It can be annoying at first, but it's worth it in the long run.

Spam: If you are running Outlook 2000 or Outlook 2003, you can turn on an spam filter feature (see the Microsoft KB articles on this CD for how to do this). You can also buy Spam filtering software, such as I Hate Spam (www.sunbelt-software.com) to work with your mail client. Many ISP's offer spam filtering of your e-mail before you even get it into your mailbox, so be sure to check out if that's a possibility.

Simple rules to follow: If you don't know who sent you the attachment or e-mail, delete it without opening it.

If you get an e-mail telling you about a virus, about something not to do or do, etc., it's likely a hoax. Check it out here: www.hoaxbusters.org.

Don't fall for Phishing scams. These are e-mails that look like they come from your bank, from e-bay, from Pay-Pal or other organizations. They want you to update your information, usually a very official looking website that you are directed to from a link in the e-mail. Delete them, or better yet, do what I do. Report them to the company they are pretending to be from. Most companies now want to get these e-mails so they can follow up on and close down the sites.

Shopping online: This is generally a secure way to purchase, no more risky than ordering over the phone or handing your credit card to someone at a store. Things to look for: Make sure the site is reputable. If you are uncertain, order over the phone instead of online. Look for the http:// to change to https://. This means that the information is encrypted between your browser and the site you are purchasing from, which keeps it safe from prying eyes. Don't let sites keep your credit card information on file. While it may be easy and convenient for you, most issues have been caused by person's breaking into company servers and

taking the credit card records, not by someone intercepting a card number during an order submission.

Physical access: You can do a lot to keep yourself safe, but if someone else uses your PC and you don't know their browsing habits, you could potentially make yourself vulnerable by letting someone else use your machine. If someone else uses your machine, make sure they are aware of what good computer habits are and how they can keep your machine safe.