Shanna's Basic Computer Upkeep
& Online Safety Information:

Virus Protection:

Make sure you HAVE virus protection software; I can't tell you the number of people whose computers we've had to bring back from a virus-ridden death because the owner's *thought* they had virus protection! If Norton or something similar came with your PC and you haven't paid a yearly rate to keep it running, then you do NOT have virus protection on your system! Norton & McAfee are not free virus protection programs - if you've never sent them a cent then they aren't protecting your pc, regardless of whether or not the programs are downloaded to your computer; you may have gotten a "trial run" when you first purchased your pc, but this runs out and if you don't renew/create a membership with them and send $, then you are no longer protected.

If you want a good virus protection program that is free, download AVG (http://free.grisoft.com/freeweb.php/doc/2/). It's just as good as Norton and McAfee and doesn't cost a cent. In the vast lawlessness of cyberspace and with the number of new viruses being sent out *every day* you should **never** be online without up-to-date virus protection software!

Make sure your virus definitions are up-to-date for your virus protection software.

Run periodic virus scans on your pc. I have my computer set to run a complete virus scan every Tuesday morning at 2am, the least likely time for me to be on it. You should do *at least* a weekly scan for viruses; monthly at the most.

Clean-up:

You do maintenance on your car, why not on your computer? Run Disk Cleanup, Disk Check & Defrag on your system at least once a month. This keeps the computer clean and running smoothly.

This is essential for keeping your pc running and in the best shape possible. Folders such as "Cache", "Temp" and "Temporary Internet Files" fill up quickly and eventually begin to take up valuable room in your system which can slow down performance. It is recommended that you clean these out often using Disk Cleanup.

Spy/adware:

A lot of people don't realize the amount of malicious software that is downloaded to their computer while they idly surf the web. 99% of personal computers that are brought to me to fix are running slow or not-at-all because there are literally hundreds of spywares and adwares running in the background. You can pick these up going to just about any site, even seemingly harmless ones.

These programs can and will download to your computer without your permission and will run in the background at all times - causing your computer's processes to lag and overall performance to decline. These programs are generally used to track where you surf and what you do so that they know what kind of pop-ads to send you. Some are more dangerous though and can track pertinent information that you enter into private websites (banks, online stores, etc.). It is possible that these trackers can get a hold of your credit card and bank account info this way.

If you get online (and who doesn't?), run Spybot S&D (http://www.safer-networking.org/en/index.html) *at least* once a week! If you're online and don't have Spybot S&D, you need to get it **right now**.

Some people prefer Ad-Aware (http://www.lavasoftusa.com/support/download/) and some people use both. This is up to you. I prefer Spybot because it "Immunizes" your computer so that harmful spy/adware, once recognized, can never infect your computer again, but Ad-Aware does sometimes find files that Spybot may miss.

Stay Away From:

A lot of people enjoy downloading cutesy, animated screensavers and simple, time-crunching games off of the Internet.

My best advice? Don't. I've had entire computers crash after downloading a seemingly innocent holiday screensaver. While some screensavers are from legit companies, and some games are safe (those from Yahoo!, Pogo, GameZone, etc.), the vast majority of those found from "click here" banners or other dubious means are NOT! These programs are simply full of ad/spyware that you are willfully downloading into your computer.

A lot of these programs appear innocent, and some even come up as legitimate spyware removal programs when in fact, they are anything but. Do not download *anything* from the Internet unless you are 100% certain of its validity and reputation. A good rule of thumb is to ***never*** download anything advertised on a pop-up ad.

Also be sure to stay away from gambling and pornographic websites; these sites are usually rife with spyware that will download invisibly to your computer.

I've had entire computers crash after downloading these types of things or going to questionable sites - including screensavers, rebate programs, daily horoscopes or weather bugs. That right there should tell you that this is not something you want installed on your computer; it's not worth it to get a silly screensaver or game you'll only play twice.

Email:

I cannot stress this enough - **DO NOT** open attachments in emails if you are not expecting one. Even if you know the sender, if the attachment looks in any way odd, don't open it. Shoot an email to the sender and ask if they sent you something before opening - the little bit you'll have to wait for a response is better than the hours you're going to spend fixing your now virus-ridden computer, trust me.

The new scam online is called "phishing" and scammers are using email to perpetuate it. If you get a supposed email from some large banking or credit institution or other business asking for your account information, *do not give it*.

If you have reason to believe it might be legitimate take the time to contact the institution via phone or email and verify the email. A good rule of thumb to remember is that **companies will <u>never</u> ask for your account information via email**. However, if you still believe the email is legitimate and you are worried about you account being closed or flagged, *contact the company in question before giving your information*. If you are wrong, you have just given your personal information to a scammer and your identity will be stolen.

It is also wise to be selective in the emails you choose to forward to friends/family/co-workers. A large number of forwarded emails are actually hoaxes, scams and some are even part of "email farming" schemes (getting a list of valid email addresses to send spam email to). By forwarding them on you are unwittingly contributing to the problem. Anything that asks you to "forward to x amount of people" should generally be deleted and not forwarded. If you feel you "must" forward a particular email, make

sure to "clean it up" before sending. Delete all of the previously forwarded email addresses listed and all of the superfluous ">>>>" marks. Take the original piece and cut/paste it into a fresh email from only you. This helps to eliminate the "farming" aspect of such emails.

Remember, your computer is a piece of equipment that needs care and general upkeep just like any other equipment or appliance you may own.

I like to joke that the computer is not a "self-cleaning oven". Being online is going to generate a lot of problems and malware that you do not want on your system. If you do not surf safely and responsibly, and periodically clean malicious software out of your computer it won't work well for very long.

Overall, it is imperative to:
- ❖ Always make sure you are running virus protection software and have at least one, good spyware removal tool on your system - make sure to keep these both updated.

- ❖ Do periodic system clean-ups & maintenance, and do not install questionable material from pop-up ads and gimmicky websites.

- ❖ Be selective in your surfing, downloading and installing. Think before putting something on your computer that may be harmful.

- ❖ Use caution when dealing with email. If you have doubts about anything, delete it.

- ❖ Stay abreast of the latest scams/viruses circulating on the Internet. As a member of the online community, you should always know what dangers are out there. The best protection is to be well-informed of what is going on in the World Wide Web.