Practice conservative and safe internet usage:

- Keep your antivirus and Windows Updates current. Install, use, and update spyware/ scumware utilities (check their reputation).
- Activate Windows Firewall or other firewall. Use a router if you have an always-on connection.
- Be leery of spam and all email file attachments.
- Do not install peer-to-peer file sharing and minimize use of chat programs. Close chat programs when not in use.
- Be careful not to click on internet ads and popups unless they are from companies you really want to do business with. **Never click within a popup.** Close them *only* by clicking the **x** in the upper right corner of the window. Be sure you're not clicking a fake **x** within the popup. Some business sites legitimately use popups so you'll need to know how to add friendly sites to your popup blocker.
- **Do not install** unknown programs from the internet. Anything for free that offers to add a "useful" toolbar to your browser, block ads, or speed up your browsing is suspect – including those that might come from Yahoo or Google. Some sites may require a plug-in. Often, you can reject the plug-in and continue to browse much of the site. It is reasonable to accept plug-ins from Macromedia, Microsoft or Quicktime.
  When an internet site does install a plug-in, always inspect the certificate to verify it's from the company you're expecting it to be from. *Never* check "Always trust …", even from Microsoft.
- Try to avoid utilities like Real Media that require you to register. If you must use these utilities, minimize the information you provide. Consider getting an email address just for online registrations.
- Consider using **Mozilla** instead of Internet Explorer as your default browser. Consider using **Mozilla** or **Eudora** instead of Outlook.
- Do not browse to gambling, porn or hacker sites. If you stumble onto them, *immediately turn off your computer*. If you must visit these sites, consider purchasing a computer exclusively for that purpose.