

General tips:

- **Get Antivirus Software.** <https://software.doit.wisc.edu/student/cgi-bin/home.cgi>
- **Do not open email attachments that you are not expecting. Especially to not open files that end in .exe, or .com**
- **Do not click or follow web links that come in an email message that you are not expecting or come from someone you do not know.**
- **If you are shopping or doing financial business on the internet, always look at the web page and see that the site address begins with https:// and has the padlock indicator on the bottom the page. This shows that there is at least some level of security in place at this site.**
- **If you are going to go to a website, hold your cursor over the link address and look at the bottom of your screen. See if the actual address is to the site you think you are going to.**
- **Pop-ups that advertise screen-savers, games, etc. are good places for spyware and viruses to be embedded – ready and waiting for you to download them. BEWARE!**
- **Don't ask to be removed or reply to messages asking to be removed from a mail list unless you know it is a legitimate list. Most of the time this just authenticates your email address to the sender (just what they want).**
- **Use good passwords – especially when entering a site where you are giving your personal information. Change passwords periodically.**
- **Don't use Peer-to-Peer file sharing – you use this if you are sharing files like music or movies. If you do install it – uninstall it when you are not using it.**
- **Install Anti-Spyware software. Available in Share\installable programs\AdAware, Share\installable programs\Microsoft AntiSpyware or Share\installable programs\Spybot**
- **Run a Firewall on your home computer (not on your SVM computer). Found in Windows XP from Start – Control Panel – Security or Windows Firewall. Turn it on.**
- **Back up your data!**