Safe Computing Tips

- Most viruses and worms use e-mail to propagate. In general, keep your operating system and anti-virus software applications up-to-date and apply the latest patches (a fix to a program bug). A patch is an actual piece of object code that is inserted into (patched into) an executable program) when they become available. Usually anti-virus software companies issue updates on a weekly basis or when a particular virus is discovered. Be sure to get the updates directly from the vendor.
- Configure Windows to always show file extensions. This makes it more difficult also for a harmful file (such as an EXE or VBS) to masquerade as a harmless file (such as TXT or JPG).
    - In Windows 2000 and Windows XP this is done through Explorer via the Tools menu: Tools/Folder Options/View. Uncheck "Hide file extensions for known file types".
    - In windows 9x this is done through Explorer – View/Options. Uncheck "Hide file extensions for known file types".
- Never open e-mail attachments with double file extensions such as NAME.BMP.EXE or NAME.TXT.VBS or with the file extensions VBS, SHS or PIF. These extensions are almost never used in normal attachments but viruses and worms frequently use them. Do not open the email but instead delete those emails, and upon exiting from the email software delete those emails from the deleted items folder.
- Disconnect your network or modem cable when you're not using your computer - or just power it down. If using DSL or a cable modem, desktop firewall software is highly recommended.
- Dialing up to the Internet – stay safe online. The Federal Trade Commission's mascot for staying safe online is **DEWIE** the Turtle. He is especially great for kids in grades K-12! **DEWIE** can tell you how to stay safe online at: **http://www.ftc.gov/bcp/conline/pubs/alerts/dialupalt.htm**. For other information about DEWIE, go to the FTC home page: **http://www.ftc.gov**, click on the **green** icon identified as Consumer Information Security.
- Privacy for Kidz…. **http://www.ftc.gov/bcp/conline/edcams/kidzprivacy/index.html**. The FTC seeks to identify organizations interested in

participating in the **FTC's public awareness campaign** concerning the **Children's Online Privacy Protection Act** and the FTC Rule that implements the Act.

- If you feel that an e-mail you receive from a friend is somehow strange - if it is in a foreign language or if it just says odd things, double-check with the friend before opening any attachments.
- When you receive e-mail advertisements or other unsolicited e-mail, do not open attachments in them or follow web links quoted in them.
- Do not trust the icons of attachment files. Worms often send executable files that have an icon resembling icons of picture, text or archive files - to fool the user.
- Never accept attachments from strangers in online chat systems such as IRC, ICQ or AOL Instant Messenger.
- When possible, avoid e-mail attachments both when sending and receiving e-mail. Most e-mail programs allow rules for filtering e-mail. You can usually make a rule to move all incoming e-mail with attachments to the deleted items folder or another mail folder for review and determination.
- Be careful when installing certain screen savers from the Internet. These can sometimes contain a "Trojan Horse" that may allow the filtration of a virus.
- Microsoft tips on the Internet about "Security & Privacy for Home Users". The URL for this site is:
    - **http://www.microsoft.com/security/home/**.