Security Tips for the Wild, Wild Internet

Managing your browser’s security and privacy:

- **Turn on auto-updates** for your browser, browser plug-ins, and software that runs in your browser.
- **Prompt for cookies.** Accept only those cookies that help with your needs: signing in, purchases.
- **Control pop-up windows.** Configure your browser to either prompt for or block pop-ups.

Finding websites safely:

- **Use bookmarking.** For sites that you visit often, save the web address as a favorite or bookmark.
- **Use browser security add-ons.** These applications provide safety ratings for web sites and search engine results.
- **Heed search engine warnings.** If the search engines (e.g. Google, Yahoo, Bing) show that a site might be malicious, don’t go there.
- **Avoid sensational sites.** Don’t visit sites dedicated to gossip about the latest sensational news stories or celebrities.

Protecting information:

- **Use SSL.** Always use SSL to send private information like signing into an account, important email, and purchases. Look for the "https" in the web address and the lock symbol.
- **SSL certificate warnings.** Problems with certificates can be a sign of a malicious or improperly maintained site. To be safe, don’t visit those sites.

Protecting yourself against Internet crime

- **Sign off web accounts.** As soon as you are done, end your session.
- **Don’t store passwords in your browser or websites,** as they are vulnerable to being stolen.
- **Don’t browse while signed into accounts.** Before signing into an account with private information, close all other browser windows and tabs.