UW Security Initiative

www.uwyo.edu/security

To remember:

Passwords

Passwords are the weakest link in computer security. Passwords are a common form of authentication and are often the only barrier between you and your personal information or the confidential UW related information to which you have access. By choosing good passwords and keeping them confidential, you can make it more difficult for an unauthorized person to access your information.

Password Examples

* Come up with a "**pass phrase**" – *I wish the wind would stop blowing*
* Take the first letter of each word – *iwtwwsb*
* Mix upper and lower case letters – *IwTwWsB*
* Substitute symbols for letters - *!wTwW$b*

Password Tips

Protecting Your Home Machine

1. Visit Windows Update:
Make sure that you have all the Critical Updates recommended for your operating system and IE. The first defense against infection is a properly patched OS.

2. Please use a firewall and realtime anti-virus. Keep the anti-virus software and firewall software up to date.
One option: Zone Alarm Firewall (by Checkpoint)
http://www.zonelabs.com/store/content/company/products/trial_zaFamily/trial_zaFamily.jsp?lid=home_freedownloads

3. You might consider installing Mozilla / **Firefox**. http://www.mozilla.org/

4. Do not use file sharing. Even the safest P2P file sharing programs that do not contain bundled spyware, still expose you to risks because of the very nature of the P2P file sharing process. By default, most P2P file sharing programs are configured to automatically launch at startup. They are also configured to allow other P2P users on the same network open access to a shared directory on your computer. The reason for this is simple. File sharing relies on its members giving and gaining unfettered access to computers across the P2P network. However, this practice can make you vulnerable to data and identity theft. Even if you change those risky default settings to a safer configuration, the act of downloading files from an anonymous source greatly increases your exposure to infection. That is because the files you are downloading may actually contain a disguised threat. Many very malicious worms and trojans, such as the Storm Worm, target and spread across P2P files sharing networks because of their known vulnerabilities.

5. Before using or purchasing any Spyware/Malware protection/removal program, always check the following **Rogue/Suspect Spyware Lists**.
http://www.spywarewarrior.com/rogue_anti-spyware.htm

6. If you have not already done so, you might want to install **CCleaner** and run it in each user's profile:
http://www.ccleaner.com/
** UNcheck the option to install the Yahoo toolbar that is checked by default for the Standard version, or download the toolbar-free versions (Slim or Basic) when given the option for those.

7. Practice Safe Surfing with with TrendProtect by Trendmicro.
TrendProtect is a browser plugin that assigns a safety rating to domains listed in your search engine. *TrendProtect also adds a new button to your browser's toolbar area. The icon and color of the button changes to indicate whether the page currently open is safe, unsafe, trusted, or unrated, or whether it contains unwanted content.*
The following color codes are used by TrendProtect to indicate the safety of each site.
Red for Warning
Yellow for Use Caution
Green for Safe
Grey for Unknown

8. You might consider installing SpywareBlaster: http://www.javacoolsoftware.com/spywareblaster.html
It will: Prevent the installation of ActiveX-based spyware, adware, browser hijackers, dialers, and other potentially unwanted software.
Block spyware/tracking cookies in Internet Explorer and Mozilla Firefox.
Restrict the actions of potentially unwanted sites in Internet Explorer.
Tutorial here:http://www.bleepingcomputer.com/forums/tutorial49.html
Periodically check for updates.

9. Some helpful articles:
"So how did I get infected in the first place?" by Tony Klein http://forums.spybot.info/showthread.php?t=279

Also see www.us-cert.gov/reading_room/securing_browser for tips on securing your internet browser.

Helpful Links:

For more information on many of the topics discussed in this presentation and handout, visit the following web sites:

Information Technology ASKIT
http://www.uwyo.edu/askit/default.asp
Computer Term Dictionary
http://www.webopedia.com
How to change your UW Domain password
http://www.uwyo.edu/askit/displaydoc.asp?askitdocid=43&parentid=1
Network Based anti-spyware
http://www.webroot.com/En_US/business.html
What to do if you are a victim of identity theft
http://www.ftc.gov/bcp/edu/microsites/idtheft/
DBAN – Darik's Boot & nuke (hard disk wipe)
http://dban.sourceforge.net/
Eraser – remove sensitive data from your hard drive
http://www.heidi.ie/eraser/
How to install and use Trend Micro's *Internet Security*
http://www.uwyo.edu/askit/displaydoc.asp?askitdocid=206&parentid=1
How to install and use TrueCrypt Encryption Software
http://www.truecrypt.org
Helpful tips for securing your web browser
www.us-cert.gov/reading_room/securing_browser
Strong Password Generator
http://strongpasswordgenerator.com
Free Antivirus software for your home machine (UW Employees)
www.uwyo.edu/antivirus

Don't be Puzzled by the things that can attack your computer!