DESKTOP SECURITY

A Partnership to Protect Desktop Computers
Overview

- Responsibilities
- Operating System Updates
- Password Protection
- Desktop Protection
- Anti-Virus Protection
- Surfing the Internet
- Downloading from the Internet
- Special Laptop Issues
Responsibilities

- Whose job is it?
  - To apply updates and service packs
  - To make sure anti-virus definitions are up-to-date
  - To stop unauthorized access of data
  - To travel the Internet safely

- It's a PARTNERSHIP
Operating System Updates

- Identify the Operating System your computer is running
  - Windows
    - Right click on the My Computer icon
    - Click on Properties
  - Macintosh
    - Click on the Apple icon
    - Click on About this Mac
Operating System Updates (Windows)

- At least weekly run Windows Update, by clicking on “Start” -> “Windows Update”, and apply all critical updates.
- Run Critical Updates from the system tray immediately upon notification.
- You can review Windows Update status at:
Operating System Updates (Windows)

- How do I know if my Windows operating system is current?
  - If you run “Start”-> “Windows Update”, complete the scan and no critical updates show - YOU ARE CURRENT!
  - Apply ALL critical updates that show in the bubble display on the bottom right corner
Operating System Updates (Macintosh)

- To check for updates on the Mac:
  - Click on the Apple icon in the upper left
  - Click on “Software Update…”
  - Software Update will automatically search for updates.
    - Software Update can be set to automatically check for, and download updates by checking the “Software Update” applet in System Preferences.
Password Protection

- Create a secure password
  - Don’t use simple phrases
  - Choose a password consisting of numbers and letters
  - Use a different password for different websites and logins
  - Don’t give your passwords out to others
Desktop Protection

- You are responsible for the actions taken while logged into your account
- Lock your computer when away for extended periods
- Don’t share your password
Anti-Virus Protection

- Always keep the anti-virus software updated and active.
- If downloading files from unfamiliar websites, scan the files with the anti-virus scanner before opening the file.
Surfing the Internet

- Don’t share personal information with parties you don’t know
- Use anti-spyware software, such as Spybot or Adaware
- Avoid suspicious or authorized websites
- Use common sense when online
Downloading from the Internet

- Try to only download from sites you trust
- When downloading a file you are unsure about, scan the file with the virus scanner before opening it
- Don’t open attachments from parties you don’t know
Special Laptop Issues

- Nearly all new laptops have wireless connectivity
- Wireless connections may drop or have poor signal strength - try sitting at a different location
- Make sure the wireless drivers are up-to-date and the wireless switch is on
Special Laptop Issues

- Be just as mindful when accessing the Internet or sharing information as on a desktop
- Use a strong password to prevent authorized access to the laptop
- Avoid leaving your laptop unattended
Conclusion

- Keep your computer and software up-to-date
- Use anti-virus and spyware software
- Use strong account passwords
- Be mindful when browsing the internet
- Any questions contact the UTS Helpdesk at (248)-370-4357 or email helpdesk@oakland.edu.