

### Protection for Personal Computers

- Faculty, staff and students can obtain McAfee via Zipline
  - The home-version does NOT include spyware and adware protection
  - Be sure to configure McAfee for automatic updates
- Other spyware and adware products to consider:
  - CounterSpy™ - <http://www.sunbelt-software.com/Home-Home-Office/CounterSpy/>
  - Spybot Search and Destroy - <http://www.safer-networking.org/en/download/>
  - Microsoft Windows Defender - <http://www.microsoft.com/athome/security/spyware/software/default.aspx>
  - LavaSoft Ad-Aware SE Personal - <http://www.lavasoft.com>

\*\*Good practice to run more than one anti-spyware/adware program due to the fact that software vendors cannot agree on what is spyware and what is not. Therefore, each program may identify something the others do not.

### Spyware/Adware Protection

- Keep the operating system up to date
  - All domain PCs automatically receive Windows and Office updates
  - Personal users should visit <http://update.microsoft.com>
  - UA-owned laptops receive updates via VPN – if not connected through VPN or brought to campus will need to go to Microsoft site for updates
- Do NOT use peer-to-peer networking
- Do NOT install or run any software unless you trust the source
- Perform a Google search before installing free software (software plus “adware” or “spyware”)
- Do NOT visit certain types of sites – pornography, free games, free screen savers, free smileys, free music, free online diaries
- Enable pop-up blockers in Internet Explorer

### Links

- Microsoft Security Web site: <http://www.microsoft.com/athome/security>
- Spyware Guide: <http://www.spywareguide.com>
- Anti-spyware Software review: <http://anti-spyware-review.toptenreviews.com>
- WebRoot spyware education: <http://www.webroot.com/resources/spywareinfo/infection.html>

# Spyware and Adware

## What's In Your Computer?



The University of Akron  
August 2009

<b>Definitions</b>
<p><b>Spyware</b> Any software that covertly gathers user information through the user's Internet connection without his or her knowledge usually for advertising purposes.</p> <p><b>Adware</b> Software that goes beyond the reasonable advertising that one might expect from freeware or shareware.</p>
<b>Spyware – Purpose</b>
<ul style="list-style-type: none"> <li>▪ Tracks your computer usage</li> <li>▪ Collects personal information</li> <li>▪ Reports on web sites visited</li> <li>▪ Installs components that can affect system performance or take up bandwidth</li> <li>▪ Violates your privacy</li> </ul>
<b>Spyware – Symptoms</b>
<ul style="list-style-type: none"> <li>▪ Computer crashes</li> <li>▪ Home page changes</li> <li>▪ New toolbar automatically installed</li> <li>▪ Browser settings have changed</li> <li>▪ Large number of pop-up ads</li> <li>▪ Decreased system performance</li> <li>▪ Something “new” on system</li> </ul>
<b>Adware – Purpose</b>
<ul style="list-style-type: none"> <li>▪ Advertising-supported software</li> <li>▪ Alternative to paying registration fees for software</li> <li>▪ Bombarded with advertisements</li> <li>▪ Runs in the background – acts as a mole</li> <li>▪ Information is logged and used to create a user profile</li> </ul>

<b>Adware - Symptoms</b>
<ul style="list-style-type: none"> <li>▪ Disrupts browsing with pop-ups</li> <li>▪ Decreased system performance</li> <li>▪ Pop-up advertisements multiply</li> </ul>
<b>Peer to Peer Networking</b>
<ul style="list-style-type: none"> <li>▪ File-sharing software</li> <li>▪ Allows computers to connect to one another and directly access files from one another's hard drive</li> <li>▪ Primarily used for sharing of music files</li> </ul>
<b>Peer to Peer Networking Risks</b>
<ul style="list-style-type: none"> <li>▪ Installation of malicious code             <ul style="list-style-type: none"> <li>▪ Impossible to verify the source of the files is trustworthy</li> </ul> </li> <li>▪ Exposure of sensitive/personal information</li> <li>▪ Susceptibility to attack</li> <li>▪ Denial of service</li> <li>▪ Prosecution             <ul style="list-style-type: none"> <li>▪ Shared files may include: pirated software, copyrighted software, or pornography</li> <li>▪ Even downloading these files unknowingly may result in legal action</li> </ul> </li> </ul>
<b>Pop-Ups</b>
<ul style="list-style-type: none"> <li>▪ Advertisements</li> <li>▪ Games</li> <li>▪ Clicking anywhere on pop-up can trigger installation of spyware</li> </ul>
<b>Where to Go for Assistance</b>
<ul style="list-style-type: none"> <li>▪ Support Desk – extension 6888</li> <li>▪ Campus-owned laptops: Bierce lower level and Computer Center</li> <li>▪ Personal computers: Bierce lower level and Computer Center</li> </ul>

<b>Methods Used to Install Spyware/Adware</b>
<ul style="list-style-type: none"> <li>▪ Installing free software:             <ul style="list-style-type: none"> <li>○ Toolbars</li> <li>○ Games</li> <li>○ Software</li> <li>○ Free subscriptions</li> </ul> </li> <li>▪ Swapping or sharing music files or photos</li> <li>▪ Allowing others to use your computer</li> <li>▪ Opening spam email messages</li> <li>▪ Opening attachments</li> <li>▪ Exploiting security flaws             <ul style="list-style-type: none"> <li>○ Security flaws in browsers or operating systems</li> </ul> </li> </ul>
<b>Protection for University-owned computers</b>
<b>McAfee Anti-virus</b>
<ul style="list-style-type: none"> <li>▪ Checks for viruses, spyware, and adware</li> <li>▪ Runs in the background</li> <li>▪ Checks files as they are accessed</li> <li>▪ Installed on computers on the UAnet domain</li> </ul>