

Spyware and Adware – What's in Your Computer?

Part 2

Disclaimer

- This course is designed for **Windows** operating system clients
- This course is not relevant for Mac OS clients

Objectives

- Definitions
- Purpose
- How Do You Know?
- Pop-Ups
- Peer-to-peer Network Sharing
- **Installation Methods**
- **Prevention**
- **Resources**

Spyware/Adware – Here to Stay

- Creators profit enormously:
 - Sell information on your surfing habits
 - Redirect you to sites you did not intend to visit
 - Bombard you with pop-up ads
- Almost impossible to find and stop the makers of spyware

Installation Methods

- User installs free:
 - Toolbars
 - Games
 - Software
 - Screensavers
 - Free subscriptions
- Free software is bundled with spyware and/or adware
 - "Piggyback" the spyware/adware with desirable software
- Swap or share music files or photos
- Allow others to use your computer

Installation Methods

- Open spam email messages
- Open messages or attachments
- Exploit security flaws
 - Take advantage of security flaws in popular browsers to install software

The Dilema

- No spyware standards
- Companies don't share information
- Need more than one product for protection


Protection for University-owned Computers

- University of Akron uses:
 - McAfee Anti-Virus
- McAfee Anti-Virus (anti-spyware and anti-adware)
 - Proactive tool
 - Runs in the background
 - Checks files as they are accessed for **spyware, viruses, and adware**
 - Installed as part of the imaging process (UAnet domain computers)
 - Computers on UAnet domain
 - For university-owned computers NOT on the domain
 - Contact the Support Desk at 330-972-6888 and request the software

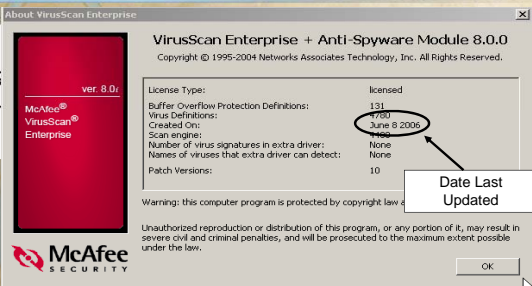
McAfee at Work

- If setup on a campus computer:
 - Controlled and updated by the server
 - The server knows if your computer is not updating correctly
 - If computer is off-campus and connected to the Internet it will go to McAfee's website for the update

McAfee At Work

- To verify your PC is getting updates:
 - Right-click McAfee shield  in lower right task tray
 - Click on the option labeled “About VirusScan Enterprise”
 - Look at the date “Created On”
 - Updates come out every weekday at 5:00 PM
 - Therefore, date should never be more than a day or two old!

Sample McAfee Screen



VirusScan Enterprise + Anti-Spyware Module 8.0.0
Copyright © 1995-2004 Networks Associates Technology, Inc. All Rights Reserved.

License Type:	licensed
Buffer Overflow Protection Definitions:	131
Virus Definitions:	3760
Created On:	June 8 2009
Scan engine:	1160
Number of virus signatures in extra driver:	None
Names of viruses that extra driver can detect:	None
Patch Versions:	10

Warning: this computer program is protected by copyright law and may be subject to patent protection. Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under the law.

OK

Protection for Personal Use Computers

- Faculty, staff and students (personal use):
 - Download via Zipline (Home Use Software Downloads link)
 - McAfee Anti-Virus
 - Home version does NOT include anti-spyware and anti-adware component
 - Configure for Auto Update:
<http://www.uakron.edu/its/learning/training/docs/McAfeeAutoUpdate.pdf>

Protection for Personal Use Computers

- CounterSpy™ (minimal charge)
 - <http://www.sunbelt-software.com/Home-Home-Office/CounterSpy/>
- Spybot Search and Destroy (free)
 - <http://www.safer-networking.org/en/download>
- Microsoft Windows Defender (free)
 - <http://www.microsoft.com/athome/security/spyware/software/default.msp>
- LavaSoft Ad-Aware SE Personal (free)
 - <http://www.lavasoft.com/>

Spyware/Adware Prevention

- Install and run spyware/adware-detection software
 - CounterSpy™
 - Microsoft Anti-Spyware
 - Ad-Aware SE Personal
 - Spybot: Search and Destroy
- Install anti-virus software

Spyware/Adware Prevention

- Keep your operating system up-to-date
 - Personal users: <http://update.microsoft.com>
 - All domain PCs automatically receive Windows and Office updates
 - Works via VPN for laptops
 - If PC is NOT brought to campus or connected through VPN – will not get automatic updates
 - Must go to Microsoft directly to get updates

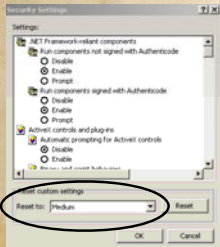
Spyware/Adware Prevention

- Do NOT use peer-to-peer networking
- Do NOT install or run any software unless you trust the source
 - Be suspicious of “free” software
 - Read the license agreement and privacy statement
- Perform a google search on software plus the word adware or spyware (BEFORE installing)
 - Results should provide a clue

Spyware/Adware Prevention

- Do NOT click anything on a pop-up except for the “X” in the upper right corner
 - Do not click on buttons – no matter what the button says!
- Maintain at least a medium security level on your browser
 - Internet Explorer: **Tools – Internet Options - Security** tab – **Custom Level** button.

Security Setting in Internet Explorer



The screenshot shows the 'Internet Options' dialog box with the 'Content Advisor' tab selected. The 'Reset to' dropdown menu is highlighted with a red circle and contains the text 'Medium'. The 'Reset' button is also visible.

Spyware/Adware Prevention

- Avoid visiting certain type of sites
 - Pornography of any kind
 - "Warez" (illegally cracked or pirated software) or unrealistically low-priced software
 - Free games, graphics, smileys, or screen savers
 - Free music, music lyrics, or sheet music
 - Free online diaries
 - Peer-to-peer file sharing programs

Spyware/Adware Prevention

- Enable Pop-Up blockers on your Browser
 - Internet Explorer 6.0 and later:
 - Tools – Pop-Up Blocker – Turn on Pop-Up Blocker
 - Allow pop-ups from a site:
 - <http://www.uakron.edu/its/learning/training/docs/DisableSitesfromPopupBlock.pdf>
 - Mozilla Firefox:
 - Tools – Options – Web Features (Turned on by default)
 - Netscape:
 - Tools – Popup Manager (Turned on by default)

Removing Spyware

- Remove the software
 - Start – Control Panel – Add or Remove Programs
 - Some components may not install completely
 - Search web for name of the software
 - +Uninstall

Removing Spyware

- Campus desktop clients
 - Support Desk 330-972-6888
- Campus-owned Laptops
 - Can bring laptop to either:
 - Bierce (lower level)
 - Computer Center
- Personal machines
 - Bierce (lower level)
 - Computer Center

Resources

- Microsoft Security Web site
 - <http://www.microsoft.com/athome/security/>
- McAfee Anti-spyware web site:
 - <http://us.mcafee.com/root/package.asp?pkgid=206>
- Spybot anti-spyware web site:
 - <http://www.safer-networking.org/en/download/>
- LavaSoft – Ad-aware Software web site:
 - <http://www.lavasoft.com/>

Resources

- WebRoot spyware Education Center
 - <http://www.webroot.com/resources/spywareinfo/infection.html>
- Anti-spyware Software Review
 - <http://anti-spyware-review.toptenreviews.com/?ttreng=1&ttrkey=anti+spyware+software>

Resources

- Spyware Watch
– <http://www.spyware.co.uk/>
- Spyware Guide
– <http://www.spywareguide.com/>
- Protecting the Web from Scumware
– <http://www.scumware.com/>
- Simply the Best – More Information
– <http://www.simplythebest.net/info/spyware.html>

Record Course Completion

- Click the following link to have this course added to your training record:

[Click Here](#)

NOTE: Failure to click the link and complete the necessary information will result in your course completion being unrecorded!

Thank You

Software Training Services/Application Support
PSTrain@uakron.edu

Questions?
