

Spyware: The Unseen Enemy

Spyware - The Unseen Enemy

One of the most prevalent risks facing computer users is spyware. Although viruses occasionally wreak more havoc, spyware has quickly become a bigger headache and can cause even greater damage.

❖ Definitions

- Spyware is software that covertly collects user information without the user's knowledge.
- Adware is software designed to customize advertising messages.
- Spyware is also a generic term used to describe all data collection software, including adware, malware, stalking horses, Trojans, key loggers, and others.

❖ Spyware Versus Viruses

- Spyware is usually installed legally.
- Spyware programs are often bundled with other applications.
- Spyware does not propagate itself, but viruses often aim to spread themselves.
- Spyware collects and shares data.
- Viruses are usually designed to inflict damage.

❖ Spyware Types

- **Adware** is designed to display advertising via pop-up windows or toolbars.
- **Stalking horses** enable adware networks to obtain information on a user.
- **Trojan horses** run surreptitiously. They often await a predetermined date or event to trigger an action. Trojans sometimes open back-door access for hackers. Trojans do not announce their installation during setup and often masquerade as useful applications.
- **Backdoor Santas** have no obvious purpose other than to collect information about surfing or shopping habits.
- **Malware** is malicious software designed to disrupt a computer, often rendering the system unusable unless the application is removed.
- **Cookies** are small files that build a user profile without notifying the user of the information being stored; cookies are potentially forwarded to an organization.

❖ Trojan and System Monitor Dangers

- Trojans and system monitors are the most dangerous types of spyware.
- These programs secretly obtain personal information, financial records, passwords, and other private data.
- These applications can collect every keystroke typed on your keyboard into a single file and send that file to a designated location or person for illicit use.
- Trojans and system monitors can lead to limitless damage.

Spyware: The Unseen Enemy

❖ **Spyware Symptoms**

- The number of advertising pop-up windows increases.
- Computer response is sluggish, even on new computers.
- New toolbars, programs, or icons suddenly appear.
- The browser home page is redirected.
- Other pages, such as search engines, are redirected.

❖ **Avoiding Spyware**

- Carefully read and react to pop-up windows. Don't click Yes just to close a window.
- Read the End User License Agreement (EULA) before installing any software; cancel installations that load other programs.
- Don't install any software unless you initiate the installation.
- Ensure that the operating system and other software applications are updated regularly.
- Use a firewall to prevent unauthorized users from accessing your computer or network.

❖ **Browser-Based Risk Mitigation**

- Leverage Internet Explorer's restricted sites to block spyware sites:
 - Click Tools from the Internet Explorer menu bar.
 - Click Internet Options.
 - Select the Security tab.
 - Click the Default Level button.
 - Move the slider to Medium or High.
 - Click OK.
 - Add spyware sites, as you encounter them, to the restricted list by highlighting the Restricted Sites icon and:
 - Clicking the Sites button.
 - Typing the address for the Web site you wish to block.
 - Clicking Add or pressing Return.
 - Clicking OK.
- Use IE privacy settings to block cookies:
 - Click Tools from the Internet Explorer menu bar.
 - Click Internet Options.
 - Select the Privacy tab.
 - Move the slider to Medium High or High (using the Block All Cookies setting will prevent any cookie from being saved).
 - Click OK.
- Tighten Internet Explorer ActiveX settings:
 - Open Control Panel.

Spyware: The Unseen Enemy

- Select the Internet Options applet.
- Click the Security tab.
- Highlight the Internet icon.
- Select Custom Level.
- Configure the following settings in the Security Settings window to create a defense against most malicious ActiveX controls:
 - Download signed ActiveX controls = Prompt
 - Download unsigned ActiveX controls = Disable
 - Initialize and script ActiveX controls not marked as safe = Disable
 - Installation of desktop items = Prompt
 - Launching programs and files in an IFRAME = Prompt
 - Click OK to save your changes.

❖ **Spyware Examples**

- Peer-to-peer file-sharing applications, including BearShare, Kazaa, and iMesh.
- Browser add-ons, including search toolbars and news tickers.
- “Helpful” utilities, such as the Gator eWallet or weather alerts.

❖ **Removing Spyware**

- Options for removing spyware include:
 - Control Panel’s Add/Remove programs applet.
 - Antispyware software.
 - Manual identification and removal (advanced users).
 - Registry edits (advanced users)

❖ **Antispyware Programs**

- Antispyware programs find and remove infestation.
- All computers that access the Internet should run antispyware software.
- Antispyware programs require updates to stay current.
- Download and install updates weekly.
- Perform full system scans weekly.
- Consider using two antispyware applications simultaneously.

❖ **Using Antispyware Programs**

- Update definition files.
- Specify the location to scan.
- Execute the scan.
- Select files to quarantine or remove.
- Execute your selection.

Spyware: The Unseen Enemy

❖ Popular Antispyware Programs

- **Ad-Aware** (free version): Lavasoft
- **Spybot S&D** (free version): Patrick Kolla's
- PestPatrol: Computer Associates
- Antispyware: Microsoft Windows
- CounterSpy: Sunbelt Software
- Spy Sweeper: Webroot Software