

Safe Computing Initiative - Spyware

Computing in a network environment presents many shared benefits and many shared dangers. In 2004 spyware infections caused more damage to school system computers than did virus infections. In order to maintain a safe and stable computing environment all computer users need to avoid activities that make the network susceptible to spyware.

DANGERS OF SPYWARE

Spyware infections result in increased occurrences of SPAM and Internet Pop-ups, increased network traffic and congestion, Virus and Trojan Horse infections. Computers infected by spyware are generally slower and often become completely disabled. Repairing these and other spyware related problems is consuming an increasing and inordinate amount of technical staff resources.

SOURCES OF SPYWARE

Most spyware infections are caused by downloading and installing "free" software, toolbars, screensavers, and programs that are offered on the Internet. These programs look appealing as they are "free" but the spyware they "co-load" is very costly to the school system. Spyware can also be installed by visiting unscrupulous web sites designed to propagate spyware. Once spyware has infected a computer, it often attempts to install other spyware programs.

REQUIRED ACTIONS

Because of the dangers presented by spyware, and its diversion of resources away from instructional issues, specific actions need to be taken that include:

1. Staff should no longer download and install programs over the Internet without first having them approved by the technical staff person assigned to the staff member's building. This would include but not be limited to:
 - a. Screen Savers and Desktop Backgrounds
 - b. Smiley Faces, Incredi-Mail
 - c. Tool Bar Helpers / Search Assistants
 - d. Games
 - e. System Utilities
 - f. WeatherBug
 - g. Instant Messengers (AIM and others)
 - h. AOL, MSN or other Internet ISP Software
2. Staff should use only those screen savers that are included with the Microsoft operating system that is on their computer. No other screen savers should be used.
3. Staff should not use AOL, AOL Instant Messenger (AIM), or other Instant Messenger programs which require a software-download to function.
4. Staff should continue to exercise due diligence when visiting web sites. Many malicious sites open Pop-Up windows which encourage you to download and install programs.
5. Staff should continue to be careful when opening mail attachments realizing that they may contain spyware or virus files.

Exceptions to the above items may be sought by contacting the technical staff person assigned to the staff member's building.

SUMMARY

In order to safeguard our network from the threats presented by spyware and virus infections Salem City School employees should discontinue downloading all software from the Internet and continue practicing safe computing habits.

Dr. Joe Coleman
Jim Rieflin