



Resources on Computer Security for Libraries

These resources were compiled by: Bill Harrison, Parsippany Public Library, bharrison@main.morris.org and Mary Martin, Morris County Library, martin@main.morris.org of the HRLC Technology Committee. Please contact them with any additions, corrections or questions.

With our recent rapid turn toward the Internet and other electronic resources, public service librarians have had to learn a lot more about computers and computer security, just to keep their PCs and their networks going.

Hackers are constantly probing our networks. Our public will try to download software onto our systems and tamper with configurations. They will go to web sites that try to install spyware, and are constantly getting viruses in their email. If our security is inadequate, these problems can bring a PC to a halt.

With few libraries having technical support staff, it has fallen to librarians who learned as they went to become the technical support staff. They are the intended audience for these tips.

In this document, you will find information on keychain drives, anti-spyware resources, and links to computer security resources on the Web.

Keychain Drives.

What are those things they're sticking into my computer? Should we allow it?

The most recent development in portable storage is known as a keychain drive, thumb drive, or jump drive, among others. It combines a small chip with a USB connector to give you 16MB to 1GB of storage that is more durable than floppies, all for \$20-100.

XP will see one as a drive when you plug it in. They each come with their own drivers for 98. On a 98 PC, you would have to disable security in order to install the drivers.

For libraries, the major security concern is that they are large enough to hold programs that you don't want to run on your system. This should not be a problem with XP. You can set your security policies to allow only authorized programs to run, to block specified programs from running, or both. Public guest accounts would not allow software installs anyway. Policies should be set to allow users to view the drive. You may also need to set your BIOS to not allow booting from a USB device. Make sure that you have a setup password to keep users out of the BIOS.

With the spread of digital photography and Acrobat, users increasingly have files too large for a floppy. A keychain drive is the easiest way to handle them. If your users are



allowed to open files on or save to a floppy or CD-RW, they should be allowed to do it on a keychain drive.

The article below recommended that you buy one for the library to show public service staff how they work and to make sure that your PCs work with them.

For more information, <http://webjunction.org/do/DisplayContent?id=7756>

Anti-Spyware Resources

Has your PC slowed down or started crashing? Do you have a lot of popups, even when you are not using the Internet? Has your home page mysteriously changed? If so, you probably have spyware.

Spyware is software that is installed on your PC, often without your knowledge, that reports your computer activities to others. Adware produces ads related to your searches, often popups. Malware is software that is intended for more malicious purposes, such as stealing passwords or credit card information, or to use your PC to relay spam or join a denial of service attack. Both types use system resources and can conflict with other programs.

AdAware and Spybot are programs that find and remove spyware. For each program, install it and then run check for updates. Click Scan or Check for Problems. Follow the prompts to remove them. You may need to run both.

Spyware Blaster is like a vaccine. It blocks most spyware from installing or running. Install the program and check for updates. Check Enable all protection. Check for updates every two weeks, as this has frequent updates.

Cool Web Search is adware that changes rapidly and is not easily removed. It is also one of the most obtrusive spyware programs. CWShredder is a program that removes it.

All of these programs are freeware and are available from <ftp://main.morris.org>. Go to /BIN/SPYWARE_CLEANING_TOOLS to download them, or visit their company websites at the addresses below.

AdAware – www.lavasoftusa.com

Spybot Search & Destroy -- www.spybot.info

SpywareBlaster -- www.javacoolsoftware.com/spywareblaster.html

CWShredder http://www.intermute.com/spysubtract/cwshredder_download.html



Other Resources on Computer Security

InfoPeople Links -- www.infopeople.org/howto/security

Links for library computer and network security. This site includes a comprehensive manual for assessing security and making a security plan.

Up Tech Creek Without A Geek -- by Andrew Mutch

www.libraryjournal.com/index.asp?layout=article&articleid=CA251684

An article with tips about how to get help when you don't have a resident "geek" at your library

Gibson Research – www.grc.com This site has three programs, DCOMbobulator, Shoot the Messenger, and UnPlugn'Pray, that turn off little used but dangerous XP services. Download and run these programs on any XP that does not have security. Run Shields Up from their site to assess the security of your PC. Click the Shields Up logo on their home page to get to these downloads.

JSI FAQ -- www.jsiinc.com/reghack.htm

This site provides a searchable archive of Windows tips and tricks, plus help on specific error messages you might encounter.

Public Access Computing -- www.pacomputing.org – Designed to support computers provided by Gates Library Foundation, but includes resources and information that can be used by anyone.

WebJunction – www.webjunction.org – “an online community where library staff meet to share ideas, solve problems, take online courses - and have fun.” The *Technology Resources* section includes information on security and other aspects of public access computing. You can sign up for the free e-newsletter, which provides resources on different topics every month.

Web4Lib - sunsite.berkeley.edu/Web4Lib

An electronic discussion group for library-based World Wide Web managers, with a searchable archive. The Reference Center is especially helpful. It has info about Web and computer-related issues within libraries -- including a section on Public Access Measures, devoted to securing public access computers.

Windows Registry Guide – www.winguides.com/registry

“Registry tweaks and fixes for Windows systems.” Information about how to lock down public access computers.