

Protecting Patron Privacy on Public PCs

Description: It's 1 a.m. Do you know where your computers have been? You may be tracking patron surfing habits on your public access PCs without even knowing it. Michael Sauers tells us how to clean out those hard drives to protect patron privacy.

Author: Michael Sauers

Publisher: WebJunction

Date Published: Sep 3, 2004

Date Posted: Sep 3, 2004

Copyright: 2004 Michael Sauers

Introduction

Over the years I've spoken with many librarians concerned with patron privacy issues when it comes to the library's public access PCs. This concern is evident in many library Internet/computer policies, in which libraries tell patrons that the privacy of their surfing should not be assumed. While no method of protecting the privacy of users on the computers is 100% assured, there are ways to minimize both the amount of information and length of time the computer will store information about your patrons.

The source of the problem is that PCs and browsers are, for the most part, designed for a one-to-one ratio between the user and the PC. Granted, Windows does allow you to create multiple logins on a computer to separate the different needs of different users, but the last thing a library wants to do is to establish individual user logins and profiles for each of its patrons. Since no one would ever think this is a feasible solution, what we end up with is a single login/profile for hundreds, if not thousands of users.

This article briefly introduces you to some of the settings and software that are available to assist you in protecting your patrons' privacy when using your public Internet terminals.

Browser Settings

When it comes to protecting patron privacy in relation to the Web browser, there are four areas that an administrator should be aware of. Here is a brief synopsis of those options and the setting changes I recommend.

1. Temporary Internet Files

This is what Internet Explorer calls the cache; a section of the hard drive that stores copies of every document and image the user has viewed. Turning off this feature will protect user privacy from those wishing to view the files in the cache (and the attached date- and time-stamps,), but it will also significantly slow down the user's surfing experience. It is generally recommended that you set the disk space allocated to the cache to a low number, somewhere around one or two megabytes, to allow it to do its job but

not to give it too much of a long-term memory. To have more control over this feature, you may want to consider also using one of the third-party solutions mentioned later in this article.

2. History

Like the cache, the history keeps a log of documents viewed by the user. Although it doesn't track the contents of those documents, it does keep track of their titles, addresses, and the date and time they were last visited. In my experience, few users are even aware of this feature of the browser, so turning it off completely by setting the days to keep in the history to zero will protect patron privacy without causing much of a fuss.

3. Cookies

Cookies are a tough one to deal with. Although many people still believe that cookies are automatically keeping track of all their credit card and social security numbers, they are not. They are tracking the computer in relation to the site currently viewed along with any advertisements that may be embedded within that site. Cookies are specifically designed with the one user / one computer design in mind. (You can read more about cookies in [The Tao of Cookies](#) right here on WebJunction.)

For example, in the one-to-one design, a cookie may keep track of the fact that a user is consistently clicking on advertisements for golfing-related products and will therefore instruct the ad server to increase the number of golfing ads that user sees. Take that concept and apply it to one of your patron computers. In the case of libraries you have probably dozens of users each day clicking on many different types of ads on the same computer. Just imagine what you're doing to those statistics!

On a more serious note, turning off cookies nowadays would cause too many hassle for both you and your patrons. Many more Web sites than you realize rely upon cookies to function properly, including those central to reference work; all those professional databases we subscribe to for example. If you turn cookies off, those sties will stop working.

Some browsers allow you to dig a little deeper into the cookie settings and turn off third-party cookies while leaving on first-party cookies. What is the difference between a third-party cookie and a first-party cookie? An example will illustrate. If you connect to Web site A and it sets a cookie, that's a first-party cookie. If an ad, embedded within site A is coming from site B, and the ad sets a cookie, that would be a third-party cookie. I'll admit, I turn off third-party cookies on my personal computers. But, that's my choice. You're welcome to try it on your public machines, but I have a warning for you: There may be some sites that no longer work properly if you turn off third-party cookies. Be prepared to assist patrons that discover them.

4. Form Memory

One other feature you'll want to disable on your public access computers is the browsers' auto-complete function. Most of today's browsers have the ability to remember what users have typed into the browser in various locations. These locations include the address bar, form fields, usernames, and passwords. In a public access environment there is absolutely no reason to keep record of any of this information, especially usernames and passwords.

These settings in Internet Explorer can be found under the Tools|Internet Options menu item. Then click on the Content tab and select the AutoComplete button. All you need to do is uncheck all of the available options. These options in Firefox can be found under the Tools|Options menu in the Privacy section. Just clear and uncheck the "Saves Form Information" and "Saved Passwords" options.

Third-Party Solutions

Once you have made decisions about how to set up your public browsers, you may quickly discover that the suggestions I've made are not perfect or foolproof. For example, even if you do set the cache to only a megabyte or two, a patron could peek at the cache to see what the previous person had been looking at. There are some additional software packages available that can assist you in overcoming these problems. Here are just a few of the programs available and a brief description of each. (For a more complete list and more significant reviews take a look at the book *The Neal-Schuman Directory of Management Software for Public Access Computers* that I wrote with Louise Alcorn.)

iClean

iClean from Alume Systems is a simple program that gives you the option of erasing data from many different areas of both the browser and Windows. Upon installation it automatically notices which version of Windows the computer is running along with which browsers are installed on the computer. (The current version will only recognize AOL, IE, Opera and Netscape however.) All you need to do is check which of the items you wish to be erased and click a "Clean" button. Additionally, iClean allows for secure erasing of information making it completely unrecoverable and the ability to have it automatically clean the selected items at boot-up. iClean currently costs \$29.99.

Internet Privacy Pro

This program is similar to iClean but has a few additional features. In addition to the ability to clean the items available in iClean, it also allows you to specify certain folders to be cleaned. For example, you could have it automatically clean out the "My Documents" folder where users may accidentally save their work. A more significant feature of Internet Privacy Pro is the ability to set it up to automatically perform its functions after a specified period of time. So, instead of needing to reboot the computer to have it cleaned, you can set this program to automatically clean every 15 or 30 minutes. The significant downside to this program is its price, which is currently \$69.95.

Window Washer

Window Washer is from Webroot Software and also offers many of the same features of the previous two programs. Like Internet Privacy Pro, it has the ability to perform a cleaning after a specified amount of time, but in order to do so you must use it in conjunction with Windows' Task Scheduler. On the plus side, this program automatically detects more than 60 programs from which it can clean information. (With the option of downloading a plug-in from the company's site that will allow it to recognize more than 150 more programs.) It also has the ability to delete certain cookies while leaving others behind. If your library is insistent on deleting cookies yet realizes that certain ones are necessary for operability, this is the program you should use. Currently this program costs \$29.95.

Deep Freeze & Drive Shield

Both Deep Freeze from Faronics and Drive Shield from Centurion Technologies offer the same sort of protection for your patrons. (They're like Word and WordPerfect. They both do the same thing but in different ways.) Ultimately, both of these packages are designed to do much, much more beyond the scope of this article, but I'll focus on their place within the privacy protection arena.

Both Deep Freeze and Drive Shield allow the user to do whatever they wish to the computer, then upon reboot, the computer will be back to the way it was before the user did whatever it was they did. When it comes to privacy, this software allows you to clear out the cache and the history. Let the user surf to their heart's content, then reboot, and all of the computer's "memory" will be reset to a blank slate.

This solution is still not without its problems. The main problem is that you don't reboot the computer after every user. Because of this, products which allow for scheduled cleaning out of the "memory" may be the better option. However, I'm sure you can see the other significant benefits to using software such as this.

As for specific differences between Deep Freeze and Drive Shield, there are a few. For example, I've found that Deep Freeze is easier to install and use and has a few additional features not found in Drive Shield. (Allowing for scheduled down time to update anti-virus software for example.) Drive Shield on the other hand does have a Macintosh version available (MacShield), and the company also makes a hardware version (Centurion Guard).

Don't forget the server logs!

The electronic records on the PC are not the only records that are being kept. Remember, every time someone requests a document via a computer on your network, a record of that request, along with the date and time of that request, is recorded somewhere in your system, the router most likely. Check to see if these records are being created and how long they're being kept. You may want to decide on a policy for disposing of those

records, or not even having them created in the first place.

A Final Note about Paper Records

Although this is not necessarily an item for a systems librarian, it does fall into the scope of this article. Most of the privacy concerns addressed in this article have to do with a record of not only where your patrons have been, but when they were there. If someone decides to look at this information, there is only so much they can glean from the fact that someone visited a certain site at a certain time on a certain computer. What makes that information more valuable is putting that together with a name. Consider your library's computer sign-in sheets. (I'm assuming that they're on paper. If your library takes computer reservations electronically, the issues still apply.)

I've met up with librarians who have told me, "Oh yeah. We keep those sign-in sheets. We've got them all in a filing cabinet in the director's office." I even had one librarian tell me that they had "the last six years' worth" in that filing cabinet. (Just think of the amount of paper!) When asked why these records are being kept the standard reply is "for the statistics."

I understand the need to keep statistics on how many people use your computers. My suggestion: Take those sign-in sheets at the end of the day, copy down the numbers, and then shred them. There is no reason for this information to be kept beyond the end of the day. Make a note that 50 people used the computers today and then get rid of their names. There are reasons we don't keep track of who checks out which book. Why should we keep track of who uses which computer?

Websites of products discussed in this article:

iClean <http://www.allume.com/win/iclean/>

Internet Privacy Pro <http://www.internetprivacypro.com/>

Windows Washer <http://www.webroot.com/wb/products/windowwasher/>

Deep Freeze <http://www.faronics.com/html/product.asp>

Drive Shield <http://www.centuriontech.com/dsms-about.htm>

Centurion Guard <http://www.centuriontech.com/centurion-about.htm>

This work is licensed under a [Creative Commons License](http://creativecommons.org/licenses/by/3.0/).

