By Phil Huang

By providing the public with online computing facilities, librarians make available a world of information resources beyond their traditional print materials. Internet-connected computers in libraries greatly enhance the opportunity for patrons to enjoy the benefits of the digital age. Unfortunately, as hackers become more sophisticated and software gets more complex, online security threats escalate as well. Keeping shared public access computers (PACs) safe has become more challenging than ever.

While there is no practical way to guarantee that a computer in a public setting can be immune to threats and while no user on such a computer can surf the Internet risk-free, we do owe it to ourselves and to our patrons to work diligently and to be vigilant over the public stations and their users' online safety. You can have 100 patrons working on 100 desktops and things may seem hunky-dory, but it only takes a single breach to rapidly compromise the other 99 computers, their users, plus a host of behind-the-scene networks and servers. The stakes are high.

On a brighter note, if you take a proactive approach to protect the health of your computing system and your users, you can mitigate the security risk before painful damage occurs. Waging the battle against hackers' threats can be difficult and expensive in terms of hardware and software costs and personnel resources. But an ounce of prevention—a few relatively simple steps carried out on a regular basis—can make a big difference.

Protecting the Digital Areas of Your Physical Space

So what can you do to protect your public computers? I've outlined some common considerations to tighten up security for a PAC. Of course, each library has its own unique situation, and procedures can vary.
PUBLIC ACCESS COMPUTERS and Their Users

Have a Good First Line of Defense

The first line of defense of a public access workstation is its operating system (OS) and the indispensable security software such as firewalls and software to fight malware, including viruses, worms, Trojan horses, spyware, etc. You must keep your OS and anti-malware up-to-date.

In 2006, Microsoft issued updates to patch 97 "critical" security holes, 14 of which were known as "zero-day" threats. This means perpetrators had been one step ahead and had already started exploiting the vulnerabilities. Microsoft's products remain the most popular targets for hacker attacks. Internet Explorer attracts about 77 percent of all browser attacks. But there is actually no safe haven here, and threats plague all platforms and major vendors' products. In March of 2007, Apple released a security update, the seventh in 3 months, for its Mac OS X to plug 45 security holes, including several zero-day vulnerabilities. Similar stories were reported about Symantec antivirus products and those of other big-name vendors.

You should always enable the auto-update of patches and anti-malware definitions. As the assaults from cybercrooks intensify, you really need to run updates and patches as frequently as possible, probably a couple of times a week.

Use Third-Party Utilities

The nature of a computer that is always exposed in a public environment requires that it can withstand things ranging from unwitting misuse to deliberate abuse or hacking. You have to look for third-party utilities that are specially designed to beef up the security of the workstation. Many libraries use restriction-based products that disable a number of functions so users can't install or run unauthorized executable files and such.

Another type of utility allows a person to work on the computer without feeling "locked down." With these sorts of tools, users can do a lot of things just as they would on a private computer, but upon logoff or reboot, everything is restored to its original state. Note that a hacker can possibly exploit this latitude to breach the network and to launch an attack on other computers. So you can't really forgo
the principle of least privilege. (That means giving each person just enough access to do his or her job, but no more.) So use restraint in conjunction with this more permissive approach.

If a Web browser is the only application you offer on a public computer, then running in kiosk mode is still a good choice due to its simplicity. (Kiosk mode, many browser functions are locked down.) Both IE and Firefox support kiosk mode. With proper configuration of the browser, and maybe the help of a third-party program, you can default the Web to full screen and disable all menus, toolbars, key commands, and the like.

**Change Defaults and Set Controls**

After installing the OS, firewall, antimalware software, and applications, it is necessary to change the out-of-the-box default settings. Default username/password (often being “user,” “password”) must be changed over. As for setting the security/privacy level of major browsers (IE, Firefox, Safari) and production software like Office, all of them allow you to tune up or down with a fair amount of control. For public computers, “high” is your best bet. Block pop-ups, which are often used by hackers to trick users into allowing malware software, and applications, it is necessary to change the out-of-the-box default settings. Default username/password (often being “user,” “password”) must be changed over. As for setting the security/privacy level of major browsers (IE, Firefox, Safari) and production software like Office, all of them allow you to tune up or down with a fair amount of control. For public computers, “high” is your best bet. Block pop-ups, which are often used by hackers to trick users into allowing malware to slip in. Be particularly wary of the use of activeX, JavaScript, and sample macro on public stations. Disable them, or, at minimum, make the application warn the user of the security implication before a Web site downloads, installs, and runs programs on the computer.

A simple and effective way to better protect user privacy is to use cleanup software, which can be set to frequently get rid of unwanted files (including those saved in the temporary folder by users), and those generated by Web browsers and other applications such as Word. Some libraries activate the cleanup at the end of each user session. That is a good practice if conditions allow.

**Perform Regular Monitoring**

Monitoring and scanning for malware on a routine basis will expose minor problems before they turn into major incidents. Check logs often; they might reveal things that are indicative of suspicious activities on computers and may hint where vulnerabilities are. With a list of potential trouble spots in hand, you can take steps to address, patch, and fix.

**Do Physical Inspections**

Librarians should physically check public computers on a periodic basis for unauthorized hardware tampering. What’s the need? A determined identity thief can use a hardware-based key logger. He or she could attach a camouflaged, compact device that looks just like an ordinary keyboard plug to the back of a workstation within seconds. Undetectable by software scanners and unnoticeable to people like you and me, it can quietly record approximately 12 months’ worth of typing, with date/time stamps. Sound outlandish? Key loggers are sold on the Internet and they can make their way to your library.

**Have a Use and Security Policy**

Last and certainly not the least important is that a library must have a computer use and security policy in place, and staffers have to make the policy abundantly clear to the patrons. The policy should include the acceptable and unacceptable uses, users’ responsibility, how the library enforces the policy, safety cautions, and a disclaimer.

**Pointers for Patrons’ Health**

User security education is vital in helping patrons stay digitally safe. No matter how tightly a workstation is configured for security, ultimately it is the user’s knowledge and actions that will steer him or her clear of the Internet pitfalls. Use signage, on-screen messages, fliers, and personal reminders to warn them about viruses, spyware, online scams, and other threats. Explain the measures they can take to avoid or mitigate risks in 15-minute walk-in workshops. These will help people maintain a keen awareness of security issues and be safer users of Internet resources. The following are a few points worth repeating to people who use your public access computers.

**Don’t Enter Sensitive Info on PACs**

There should be no e-banking, online shopping with a credit card, or stock trading. Despite the implementation of the latest crime-fighting technology, there isn’t complete protection on any PC, let alone a computer in a public setting. Determined crooks can unleash spyware on a public computer or install things like key loggers to catch each and every keystroke, including your password, name, address, Social Security number, and even credit card numbers.

**Beware of Snoopers**

Never leave a session unattended while logged in, and always be on the lookout for “over-the-shoulder surfers” in a public environment.

**Do Secure Login and Logout**

When people log in to a secure site, make sure they see the padlock, and that they later log out properly. People should not use email without a secure sign-in mechanism. If the URL area where you type in the Web address does not start with https:// (the “s” before the colon indicates it is secure), you don’t see a padlock near the URL area or the bottom area of the browser, then do not enter your password. To be extra careful, you can click the lock icon to bring up information on the security certificate, which should bear the name of the site consistent with the site name on the URL.
It's important for people to know that if they just close up a Web window without clicking the "Sign off" or "Log out" button, their sessions can still be active. So the next person to jump onto the same computer can continue from exactly where they left off, and can dig out a lot of private information.

**Do Not Open Email Attachments**

The bad guys often use attachments with email or instant messaging (IM) to spread a virus or worm. If an attachment is a simple text file with a .txt file extension, it's probably safe. Treat everything else, including picture files and music files, with caution. Watch for double extensions like "fun.txt.exe," which can slip through virus detection software. If you see those, you can almost be certain it is a virus. Tell your patrons that an innocent click can wreak havoc on them and all of the friends in their address books. Open an attachment only when you know the sender well and you are expecting such an attachment.

**Use a Temporary Password**

On a public workstation, since people have no way of knowing for sure if a key logger or other tracking software is running on the machine, their passwords are subject to theft, no matter how strong they are. If a person does want to check email, one workaround is to use a temporary password, then change it back as soon as the person gets back to his or her private computer. Better still, create a secondary email account for casual usage on a public station.

**Cover Your Tracks**

Some libraries use permissive security control software, opting for a more liberal approach to patrons’ latitude in using applications on PACs. Such configurations can leave more of the safety-related responsibility on the shoulders of the user. In such cases, the librarians should remind users to do a number of things when they're finished with the computer:

1. Uncheck the “Remember me on this computer” option when entering username and password.
2. Remove cookies and caches.
Learn More About Security

Library Computer and Network Security: Introduction
Jeff Eisenberg and Connie Lawthers, last updated March 31, 2005
www.infopeople.org/resources/security

The Ten Most Important Security Trends of the Coming Year
SANS Institute, 2006
www.sans.org/resources/10_security_trends.pdf

5 safety tips for using a public computer
Microsoft Corp., Sept. 29, 2006
www.microsoft.com/athome/security/privacy/publiccomputer.mspx

“The 10 Biggest Security Risks You Don’t Know About”
Andrew Brandt, June 22, 2006
www.pcworld.com/article/id,126083-page,1/article.html#

Watch for Phishing Scams

Phishing scams can take many forms, but they usually start with an email, instant message, or pop-up window asking you to update your personal information. They use real-looking (but phony) bank or credit card company sites to lure you into giving out your sensitive information.

Use Wi-Fi with Caution

Increasingly, libraries offer wireless connections to their authenticated users and/or to unauthenticated “guests.” However, due to high costs, many libraries are unable to provide data encryption. So data that is traveling across the airwaves, but is not traveling through otherwise-secure applications such as https and SSH, can easily be picked up by hackers outside the boundary of the library.

Also, if you want to use a public Wi-Fi network, make sure you have a firewall functioning in your laptop. Windows XP (Service Pack 2), Windows Vista, and Mac OS X run a firewall by default, but you need to verify it before going ahead. If you are in a Wi-Fi zone and you do not intend to go online, disconnect the Wi-Fi communication to minimize the possibility of hacker intrusion. The convenience of wireless comes with a higher level of risk, which requires extra precaution.

Who Will Win in the End?

Keeping our public access computers secure and providing our users with a safe Internet experience are daunting, long-term tasks. In the end, criminals will continue their attacks, and we want to fight back hard. The battle may never be won, but with maturing security technology and heightened vigilance on the part of librarians and their users, there is reason for optimism.

Phil Huang is systems coordinator for the library of California State University–Sonoma, where his work is primarily system management/administration, working with various departments in support of the library’s computing systems. Prior to that, he worked as a programmer/analyst writing and developing ILS and other information retrieval systems for several years. He holds a B.A. from Fudan University in China and an M.L.S. from SUNY–Buffalo in New York. His email address is phillhuang@sonoma.edu.