ACHIEVE NETWORK SECURITY

The transfer of sensitive information on the Web is inevitable. With hackers on the rise, no one is totally safe. How can you keep your library staff computers and public access computers safe from your patron users?

This article is sort of a Security 101 for your library. It focuses on the following three categories:

- How to intelligently choose a password.
- How to write discreet yet effective e-mail messages.
- Everything you wanted to know about cookies.

Password security
The first thing to think about when you implement a security policy is passwords. It seems so obvious, and yet it is often overlooked. If someone has your password, they have access to all the files on your workstation. Here are some common-sense guidelines for keeping your staff computers passwords secure:

Do:
- Change your password often (monthly is recommended).
- Use letter, number, and special character combinations.
- Choose a password that is easy to type.
- Choose a password that is easy to remember.
- Make your password at least six characters long.
- Choose a password that is not a word found in a dictionary - English or otherwise. Make up words either by switching syllables in real words (tefalone=telephone) or by joining words and then jumbling them.

Don't :
- Don't use your first or last name.
- Don't use the name of your pet or partner.
- Don't use any easily traceable personal information (license plate or home address).
- Don't use your login or username.
- Don't ever write your password down (on paper or e-mail).
- Don't use a password of all numbers or all letters.
- Don't ever tell anyone your password.

- Don't leave a password on someone's voice-mail.

- Don't use the same password for all of your password needs.

It might seem difficult to meet all the criteria while creating a password that is memorable. But it is possible, and a good guide is Netscape's Choosing a Good Password page. Consider following the guide's advice by using a phrase that is unique to you but easy to remember: for example, "My brother Charlie's birthday is November 29."
Be aware that passwords usually are used for staff computers and servers only. Libraries usually don't rely on passwords as the main security device on their public access computers - there would be too many people to dole passwords out to, thus rendering the password useless.

Hackers
One of the most common hacking methods is called social engineering; Hackers rely on a human to give a password. You may get a call from someone claiming to be a representative of your ISP. He may tell you that in order to determine whether there has been a security break in your account, he needs to know your password. Or you may receive a call from someone who claims that he is a library employee, and that he is about to leave on an airplane and he forgot his password. These situations are not uncommon. Get a name and a contact number for the individual and check before you give any information out.

Never give your password out over the phone. There is a useful password-related link from the people at CERN (the European Organization for Nuclear Research, the organization where the Web was conceived).

E-mail security
It is important to remember that e-mail is transferred from sender to receiver, and that this transfer is often not secure. An e-mail message is potentially viewable through every service provider through which it passes. David Raikow, Internet security specialist says, "Sending e-mail is like sending a postcard, only less secure because [the postcard] passes by fewer eyeballs. E-mail is more like note-passing in class, because it has the ability to be passed, saved, deleted, or changed without the sender or receiver ever having known of it."

Not to induce complete hysteria, but any individual with authorized access (and many without) can read your e-mail. E-mail is also easily misrouted and forwarded without your permission. And let's not forget the BCC (Blind Carbon Copy) that will allow another pair of eyes to see an e-mail message without the recipient ever knowing it.

Because e-mail and the Internet are so new, the boundaries and limits of Fourth Amendment protection have not yet evolved in the courts. But remember that employers can read any e-mail that passes through their servers. While the Fourth Amendment may apply to e-mail, it doesn't apply to mail sent through your library server. And the standard agreement that you most likely have with your ISP is that the ISP can do whatever it likes with your e-mail. So if you want to remain completely safe, do not send private or sensitive information over the Internet.

Having said that, don't believe the hype. There is a lot to be said for avoiding complete panic and steering clear of hoaxes. Salon helps soothe the excessively paranoid in this article about security.
Keep in mind that it's always good to use a common-sense standard for e-mail -- don't write something that could be libelous (or even hideously embarrassing), illegal, or indiscreet in an e-mail message. Sooner or later, someone inappropriate could see it (if for no other reason than you accidentally hit the wrong key late one afternoon and posted your highly personal message to the entire staff or listserv).

If you must send a very sensitive message, use an encryption software program like PGP (Pretty Good Privacy), discussed later in this article.

Encryption is a system that allows only those with the correct key to decode the message. It is one of the safest methods of sending information. For more information about encryption, see Net Action's Guide to Encryption parts one and two.

E-mail list security

E-mail lists are discussion bulletin boards that are visited by people with a common interest (for example, Internet security). They are referred to as listservs, conferences, majordomos, exploders, and salons. Because listservs can e-mail a number of people at once using one address (the listserv address), and the subscribers have access to the subscription list's inbox, there is plenty of room for security violations. Conversely, if you e-mail a listserv, you have no idea who may receive the information that you send. Some listservs are more secure than others, and you have no idea who may be posing as a sympathizer, but is actually an opponent. If you have any privacy questions about a listserv, contact the owner of the list.

We recommend that you follow basic e-mail security rules and refrain from mentioning sensitive or private information when posting messages to a listserv. Keep in mind that e-mails are permanently archived, and that they pass through many viewers. Use discretion when you CC (Carbon Copy) or forward a listserv to a person who does not subscribe.

Public access computers

While e-mail is an important issue for your public access computers, especially in terms of blocking viruses, the library staff's overriding concern is with patrons making changes to the computers by saving infected files to the hard drive, downloading and installing software on the hard drive, and deleting important files from the hard drive. You can solve this problem with the purchase of Centurion Guard, a physical lock on the hard drive - and through the creative use of Windows 2000's built in policy and permissions options. For non-Windows computers, software based security programs such as Deep Freeze andFortres Clean Slate are available.

Web security

The main issue in Web security is online forms. Sensitive information should not be sent to a webmaster via an online form. Any information that you submit through the Internet has an indefinite life span. Always keep in mind that the information you submit in a Web form is vulnerable to prying eyes in electronic transport. Fortunately, secure servers encrypt the information in transmission.

You can tell if you are on a secure site by looking at the URL. On a secure site, it will start with https:// and not http://. There will also be a small lock in the window of the browser, or at the bottom of the browser's frame.

Cookies can make you sick

Cookies are pieces of code that lodge on your computer and allow a Web site to trace and harvest information about your activities on that site. This means that a Web site knows when and how many times you've been there. When you log in to a site with cookies, the site saves your specific preferences (or any other information) on its server. When you go back to the site, it is able to "remember" who you are. This can be useful if the computer you're using is your home computer, or if the computer that you share does not contain any sensitive information, like your stock portfolio, that is saved to the site in the form of cookies.

The good news is cookies can be useful tools that remember your personal profile and make your surfing quicker on a site that you frequent. They also are useful for remembering your site preferences.

The bad news is that most sites use cookies for marketing information. For example, the creepy and invasive message that you receive on your computer that informs you that it's time you update your virus software is the result of a cookie. Only the Web site that sets a cookie can access it.

Different browsers have different cookie settings. With Netscape, you can have the browser allow all cookies, warn you when it comes across a cookie, or completely disable cookies. Internet Explorer has an additional feature that lets you specify different settings for different security zones. You can choose to allow Web sites to create cookies for you in your "trusted sites," warn you before you create them in your local Intranet zone, or give you an option to never allow them in a "restricted zone."

A basic precaution to follow with cookies is that if you're browsing, and you're afraid of leaving a breadcrumb trail for marketers, disable your cookies.

Be aware that you are leaving a trail everywhere you accept a cookie.

- Cookies will tell Web advertisers which ads you click on.
- The disadvantage of cookies is that your usage becomes a marketing tool.
- Cookies can be helpful to save your preferences at a site that you frequently visit.
- On a public access computer in your library, never give your sensitive information to a site with cookies or disable accepting cookies in your browser's settings.
- If you are uncertain about whether you want them, uncheck the Accept All Cookies box in your browser's Settings menu.
- If you are afraid of not having access to all sites, select "Warn Before Accepting," although the result may be annoying if an individual site has set a lot of cookies.

Source : http://www.webjunction.org/documents/webjunction/Achieve_Network_Security.html