Precautions for Using the *Internet in the Classroom*

COMPUTING

Connecting your school to the Internet opens a new world with exciting possibilities to your students and can enhance their learning experiences. They will gain access to a variety of resources otherwise unavailable to them—museums, databases of images and information, and experts who can answer questions on a variety of topics, to name just a few.

However, opening your school to the world via the Internet does pose some risks. You don't have to be a computer expert to take the basic steps to protect your students and your school's computers. Here are some things you should know about the hazards of Internet use and the precautions you can take.

Personal Security for Your Students on the Internet

Start With an AUP

It's obvious that you cannot monitor students every second they are on the Internet. You can, however, make your expectations clearly known about appropriate classroom use of the Internet. A document to help you do this is known as an Acceptable Use Policy (AUP). You should require both parents and students to sign this form. Make it clear that anyone who does not sign the form, or who violates the AUP, loses Internet privileges.

Emphasize Privacy Issues

Teaching your students to maintain their privacy while on the Internet is extremely important. The same rule applies on the Internet as in everyday life—never talk to a stranger. Tell your students not to give out personal information to anyone on the Internet. I tell my students (even at the university level) to use a pseudonym instead of their real name.

Many Web sites request a variety of information (including an E-mail address) before you can sign up for free information, prizes, or use of their services. Once again, be careful about the information that you provide. Consider creating a separate E-mail account from the one the school uses for regular personal or business E-mails. (You can get free E-mail accounts through a variety of companies like www.yahoo.com or www.hotmail.com.) Many companies will sell E-mail addresses and other personal information to marketing companies. As a result, the school's In Box will constantly be filled with junk E-mail (known as "spam") from companies trying to sell something.

Chat Rooms

Another reason to emphasize anonymity for students using the Internet is chat rooms. I tell my students never to give out personal information on the Internet. In fact, you may want to discourage or forbid students from participating in chat rooms on school computers because pedophiles and other undesirable individuals often frequent such locations. In a survey of 1,500 children ages 10 to 17, it was found that one in 33 had received an aggressive solicitation from someone on the Internet who had asked to meet them, talk on the telephone, or who sent them regular mail, money, or gifts.[1]

Web Site Cookies

Check the Privacy Policy of each Internet site you visit. Many sites gather information about you (without your awareness or consent) and your computer through the use of "cookies." How does a cookie work? When you visit a Web site for the first time, the site creates a small program that is stored on your computer. If you visit the site more than once, it looks on your computer for this cookie and uses it in a variety of ways (e.g., when you visit an online bookstore for the second time, a cookie indicates the book types you viewed or purchased on your first visit, and suggests materials you might be interested in buying, based upon your choices at that time). Sites frequently sell their visitors' E-mail addresses to other companies, which may result in your receiving a lot of unsolicited E-mails, some of which may carry computer viruses. You can block Web sites from placing cookies on your computer through your Web browser (i.e. Netscape Communicator or Microsoft Internet Explorer), but some sites will limit your access if you do so.[2]

Ensure Safe Web Surfing

Even if you require students to sign an AUP, some will still visit inappropriate Web sites. You can install a variety of software programs called "filters" that block certain types of

Precautions

Develop an AUP for your students to sign.

Install filtering software on your computer to block inappropriate Web site content.

Teach your students to not give out personal information on the Internet.

Get a free E-mail account to use for logging onto Web sites that require an E-mail address for access.

Set your Web browser to not accept cookies.

Contact your ISP to find out how to protect your computer network and your system.

Install a firewall program on school computers (especially if they are continuously hooked to the Internet).

Install virus protection software on each computer, and keep it updated by frequently visiting the software producer's Web site and downloading new versions.

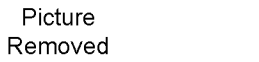
Never open an E-mail attachment from an individual you do not know.

Make frequent backups of all files on your computer in case a virus invades your system or your computers are broken into or stolen.

Shut down computers that are not in use.

content from being accessed by students.

Most filters can be set up to block specific words chosen by the user when the program is installed. Pornography sites are the most common ones blocked, but sites that promote hate groups, use vulgar language, et cetera, can also be filtered. Keep in mind that filtering software cannot block every site you do not want your students to view. Be sure to monitor what your students are doing while they are on the Internet.



Computer Network Security

A major concern about computer networks is their vulnerability to being "hacked" or broken into. Individuals with enough technical expertise can break into a computer network through the Internet and do considerable damage to both the network and the computers hooked to it (i.e., retrieve, change, or delete data; insert files and viruses; or disable the network). One reason computer networks are vulnerable to hacking is that they are generally connected to the Internet 24 hours a day, seven days a week. Computers hooked to a network are typically given a unique IP address, which identifies the computer, tells where it is located and how it is connected to the Internet. Using an IP address, a hacker can locate a particular computer and attempt to break into it (since the computers are online continuously, this can occur even when they are not in use).

Most school computer networks, however, gain access to the Internet through an Internet Service Provider (ISP) that takes great precautions to protect their network and the people to whom they provide service. Computer networks are often protected against unauthorized access through the use of "firewalls." Generally, this is sufficient to guard your school's computer network. For additional protection, however, you can load personal firewall programs onto individual computers. These programs alert the local user when the computer is being accessed illegally and maintain a record of each such incident.

What about schools with no computer network, but just a few machines connected to the Internet? If your school uses a dial-up ISP to connect to the Internet, you are reasonably safe from hacking because your computers are not continuously connected to the Internet. You can, however, load a personal firewall on each machine for added protection.

Computer Viruses

It is very important to protect your computers against viruses, computer instructions that are loaded onto your computer without your knowledge or authorization. Viruses range from the relatively harmless, such as one that flashes a message on the monitor, to the devastating, which can destroy files or lock up your hard drive. In recent years, computer viruses have appeared in E-mail attachments, word-processing documents, and other files downloaded from the Internet (such as images and executable files). When an individual opens the attachment or file, the virus runs on the computer. (Be very cautious about opening E-mail attachments, particularly ones with a name ending in .com, .bat, .exe, .dll, .pif, .hta, or .html. Never open an attachment from an individual you do not know.) A worm is a type of virus with some special characteristics. Like a typical virus, it can replicate itself and take control of one or more com-

Continued on page 46

Useful Web Resources

Many of the resources listed below are free for personal use. Most, however, do charge for commercial use. Contact each one to see if they offer free use for non-profit organizations.

Filters, Firewalls, Viruses, Internet Privacy

- "Leave Me Alone," *PC Magazine*, 20:2, January 16, 2001 (www.pcmag.com)
- Online dictionary and search engine for computer and Internet terms: http://webopedia.internet.com/
- Information about firewalls: http://webopedia.internet.com/TERM/f/firewall.html/
- Information about filters: http://www.teachersfirst.com/tutorial/filters2.shtml/
- General information about technology: www.zdnet.com/

Acceptable Use Policy

- http://netizen.uoregon.edu/templates/model_policy.html/
- http://teacher.scholastic.com/professional/teachtech/networkguide.html/

Free E-mail Accounts

- www.yahoo.com/
- www.hotmail.com/
- www.gaggle.net/ (free filtered E-mail for schools)

Personal Firewalls

- BlackICE Defender 2.5 (www.networkice.com)
- ZoneAlarm 2.6 (www.zonelabs.com)
- ESafe Desktop 3.0 (www.ealaddin.com)
- McAfee Firewall (www.mcafee-at-home.com)
- McAfee Internet Guard Dog 3.0 (www.mcafee-at-home.com)
- Norton Personal Firewall 2001 (www.symantec.com)

Virus Protection Software

- McAfee Virus Scan (www.mcafee-at-home.com)
- Norton Internet Security (www.symantec.com)

Precautions for Using the Internet in the Classroom

Continued from page 31

puters; however, a worm cannot attach itself to another program. A computer system can be infected with a worm in the same manner as with other viruses.

To protect your school computers against viruses, install virus protection software. The anti-virus software runs continuously in the background on your computer—that is, it scans each file that is loaded to detect possible viruses. If it finds a virus that it recognizes, it warns the user and most times will "clean" the infected file. New viruses are being created all the time, so be sure to update often. Most virus programs have new versions that can be downloaded for free through their Web site.

One way to keep viruses from disabling your system is to back up each computer regularly and store the data in a safe place, such as a fireproof safe or a teacher or administrator's home. This ensures that the data will continue to exist even if something happens to the school computers or the school.

Most commercial computer networks have automatic data backups. School computer networks, however, are not usually set up this way, so data backups should be made at least once a week. Back up anything that would be impossible or time consuming to replace (e.g., student demographic information, grades, financial records, personnel files, etc.). It is not usually necessary to back up software programs since they can be reinstalled from disks if damaged or lost.

Summary

You can take a variety of precautions to ensure the safety of your students and your school's computers when they are connected to the Internet. While not claiming to offer a comprehensive list of the hazards of computer use, this article did try to highlight a few of these precautions in order to heighten awareness of the dangers. It is important to be proactive and to stay informed to ensure safe and effective use of the Internet in your school classrooms and offices.

Separate Article Removed

Picture Removed

Dr. Tim Green, *guest columnist for this issue, is an Assistant Professor of Elementary Education at California State University Fullerton. Dr. Green has expertise in integrating technology into the teaching and learning process and has been helping teachers and students successfully utilize technology for a number of years. He recently served as the coordinator for the Collaboration Issue of the* JOURNAL. *Dr. Green can be reached at tgreen@fullerton.edu.*

Separate Article Removed