SECURITY ON THE INTERNET

BY TIM GREEN

Allowing students access to the Internet opens marvelous possibilities! They are no longer limited to the information and resources located at school or in the community. They can see famous paintings, listen to music, check the weather report at locations around the world, conduct scientific experiments, talk with people thousands of miles away, and access information at major libraries throughout the world.

Picture
Removed

Despite these advantages, major concerns have arisen. How do you, as a teacher, keep students from gaining access to information that might not be suitable for them? Listed below are some suggested guidelines to use when allowing students use the Internet. *These guidelines are by no means exhaustive. Rather, they are basic suggestions that you can adapt and build upon when allowing students to access the Internet.*

Guidelines

1. **Know what is out there.** Spend some time "surfing" the Internet to find out what types of information are available and how to access them. Information is available on almost any topic you can think of—and some you may *not* have thought of!

2. **Educate students and parents.** Help your students learn about what is on the Internet and how to be responsible about accessing it. Post guidelines defining what is expected of them when using the online services. This may include proper behavior on the Internet (known as "netiquette"), types of World Wide Web sites that should be avoided (i.e., pornography), and time limits on use. Students should be warned about the dangers of contact with stalkers and pedophiles on bulletin board services, the Internet, and the World Wide Web. They should never reveal the address or telephone numbers of their home or school to anyone on these services and should disconnect immediately if a person online says anything that makes them feel uncomfortable or afraid.

3. **Close supervision.** Help your students understand school-related reasons for using the Internet (i.e., assignments, e-mail, etc.), then supervise their online activity. You will thus prevent many of the problems that could arise.

4. **Structure student use of the Internet.** Students should have a definite plan or goal when using the Internet. Be sure to monitor what each student is trying to accomplish. Assigning students to submit a written request for using the Net and to summarize their results can also help you monitor their activity on the Internet.

5. **Use electronic blockers where possible.** A number of software programs allow the user to limit access to certain topics or "chat rooms" in online services and on the Internet. Access is controlled through several methods:

a. Some programs act as barriers to prevent certain persons from using the computer or to restrict access to certain areas.

A program called *Fire-Wall-1*[1] can be used with most aspects of the Internet (e-mail, World Wide Web, downloading files). *Fire-Wall-1* can prevent access to various services or Internet resources and prevents the user from bypassing the program by interrupting it in any manner. Another program, *CYBERsitter,*[2] allows secret monitoring or blocking of access to the most common picture file formats online or to full motion video files, specific files, file types, programs, directories, or even drives. Features include stealth installation, password protection, and compatibility with networks and graphics programs.

b. Built-in controls are included in the software programs of many commercial Internet providers, such as America OnLine. Such programs allow educators and parents to limit student access to certain topics or areas offered by the service. Be sure to check each program's features before buying these types of software.

Be aware, however, that such controls are not foolproof. So many new things are appearing on the Internet that it is not possible to block them all. Staying up to date about blocker programs and carefully monitoring student use of online services will help to prevent unauthorized access.

6. **Create a school-wide Acceptable Use Policy (AUP).** This is a contract signed by both students and parents. It explains what is expected of the student when using the Internet at school and the consequences if those expectations are not met. The policy also communicates to the community what the school is doing to provide a safe learning environment for students. The above guidelines and suggestions should be integrated into the policy. Information and sample AUPs may be found at the following sites:

http://riceinfo.rice.edu/armadillo/acceptable.html

http://www.erehwon.com\k12aup

http://198.51.98/policy.html

Tim Green is a Doctoral Student studying Instructional Systems Technology at Indiana University School of Education, Bloomington, Indiana. His e-mail address is tigreen@indiana.edu and his World Wide Web address is: http://copper.ucs. indiana. edu/~tigreen/first.html.

REFERENCES

1. Available from the Internet Security Company, 1 Militia Drive, Suite 3, Lexington, MA 02173. Telephone: (617) 863-6400.

2. Available from Solid Oak Software, Inc., P.O. Box 6826, Santa Barbara, CA 93160. Telephone: 805-967-9853.