Filtering Tools, Education, and the Parent: Ingredients for Surfing Safely on the Information Superhighway

Danielle M. Gallo

Senior Technical Associate, AT&T Labs-Research

FEATURE

Each day more and more people are going online to tap the Internet's rich resources. Many Internet users are children, and unfortunately, the Internet is not always a safe haven for children and teenagers.

Keeping children safe online is an arduous task that parents and educators must undertake with great intensity and enthusiasm. Lack of familiarity with the medium may serve as the largest obstacle. Many parents admit that their children know more about computers than they do. Parents' lack of knowledge may cause them to fear machines and allow the child free reign while online. In addition, parents may not be aware of the weaknesses of the filtering/blocking tools they utilize. Children, especially teenagers, may be aware of such weaknesses and find ways around them. Regardless of what filtering/blocking tool is employed, parents need to educate themselves about the Internet and sit with their children while they are online.

This is a recurring problem with filtering/blocking tools. If the child can obtain the password and maneuver his way around the system, he can easily control the content accessed.

Children's online safety is a serious business that has led to the development of a multitude of filtering/blocking tools. Currently, there are more than 40 parental empowerment tools available, including blocking/filtering tools, access control features available through the Internet Service Provider (ISP), and Web sites specifically geared toward children. Although each tool functions in a different way, the main goal is the same: to provide children with appropriate content and deter them from anything that could possibly be harmful to them. Although pornography is perceived as the greatest source of harm, there are other situations parents need to be aware of that may prove risky for their children. One example is chat rooms. Pedophiles often lurk in chat rooms, attempting to lure children into providing information that may cause a safety risk, or, more seriously, persuade the child to arrange a physical meeting. Chat rooms are covered under the scope of many blocking tools, but pedophiles may find ways that allow the child to supply information without raising a flag from the filtering device.

The most important ingredient in protecting children online is parental education and involvement. Unfortunately, there are no products that will fill all needs or be impossible to disable. Therefore, parents must educate themselves, become comfortable with the Internet and communicate with their children about these risks.

In the following paragraphs, the characteristics, both positive and negative, of four blocking tools will be discussed. This information will further clarify that a combination of technology and parental involvement is the most useful strategy in protecting children online.

Some filtering/blocking tools block content that appears on a "bad for kids list," such as sites that contain sexual content, violence, or the Federal Communication Commission's "seven dirty words." Other tools filter out all content unless it appears on a "good for kids list." Parents must first be aware that filtering/blocking tools are not a completely reliable source. Many tools utilize a keyword-blocking scheme that will block any content that contains certain words. Therefore, pages with the words "sexually linked trait" or "asexual reproduction" may be blocked. Important information about safe sex and sexually transmitted diseases will also go unseen. Unfortunately, children may miss out on educational content due to this technique.

The examples used in the following paragraphs do not encompass the entire list of available filtering/blocking tools. For the sake of brevity, a small group has been chosen to demonstrate the function of filtering/blocking tools and their characteristics.

The first example is **Access Management Engine,** or AME. AME is supplied by Bascom Global Internet Services, Inc., with a website at http://www.bascom.com. AME software allows parents and libraries to provide content that custom fits their educational needs. The "good for kids list," which contains content selected by the parent, teacher or librarian, is the only content accessible to the child. If the child requests content that does not appear on this list, a "not allowed" Web page is generated. One of the positive aspects of this tool is its scope. AME applies to Web sites, chat services, inbound and outbound e-mail, as well as newsgroups. In addition, this tool may be easier for parents and teachers because there is no software installation involved; AME products reside on the network center of the Internet Service Provider. AME allows designated users to create fully customizable "allow lists" and apply them to individual computers or groups. The weakness with this product lies in the accessibility of designated users' passwords. Each designated user requires a password; therefore, if a child were to obtain an adult's password, he could easily bypass the "allow list" and gain access to all Internet content. This is a recurring problem with filtering/blocking tools; each product described here is susceptible to this problem. If the child can obtain the password and maneuver his way around the system, he can easily control the content accessed. Other products similar to AME are Bess (http://www.n2h2.com) and I-Gear (http://www.urlabs.com).

America Online Parental Controls (http://

continued on page 24

Filtering Tools

continued from page 23

www.aol.com) is a tool that comes as a feature of the ISP service. All AOL users have access to Parental Controls, and they are easy to configure and apply to children's accounts. Parental controls are custom controls that limit children's access to the Internet and other AOL content. Controls are divided into three categories, Kids Only, Young Teen, and Mature Teen. Kids Only accounts allow limited access to Internet content while they have full access within the Kids Only portion of AOL. A positive aspect of this account is that an account designated as Kids Only will not be able to send or receive instant messages. Instant messages are private messages sent between users of the service who are logged on at the same time. Similar chat room restrictions are also applied. Young Teen accounts are limited to some AOL content and features. Young Teen accounts will not be able to send or receive email attachments unless otherwise customized. Mature Teen accounts can go anywhere on the AOL service and use all AOL features, but mature content will be blocked. These controls have a wide range of coverage, which is a positive feature parents should take advantage of. A similar product is Mayberry USA Filtered Internet Access Accounts (http://www.mayberryusa.net/).

Cyber Snoop (http://www.pearlsw.com), priced at $49.95, is an Internet monitoring and control software that produces a complete trail of all Internet activity. The password holder is able to read contents of e-mail, see Web sites visited, and read chat communication. Cyber Snoop's customizability allows the parent/educator many different options, such as controlling access to the Web while allowing unlimited access to e-mail. Keyword blocking prevents users from supplying names, addresses, etc. if they arrive at a Web site that requests such information. One of Cyber Snoop's strengths is the flexibility of configuration. The combination of options available to the administrator should easily meet any parent or librarian's needs. Cyber Snoop also has some technological features that make it difficult for even a techno-savvy child to disengage the device. The log will also be useful to administrators, as it is available for future reference and may allow guardians to set useful guidelines based on content the child has previously viewed. Other products that operate in a similar manner are The SafeSurf Rating Standard (http://www.safesurf.com) and Net Shepherd World Opinion Rating Service (http://www.netshepherd.com). Products similar to Cyber Snoop in structure and usage are Cyber Patrol (http://www.learningco.com) and GuardiaNet (http://www.guardianet.net).

The last tool is **Net Nanny** (http://www.netnanny.com). Net Nanny is priced along the same lines as Cyber Snoop, and is designed for security purposes in the home, school and business. The consumer has complete control over all content that passes through the PC. Net Nanny also has the unique feature of BioPassword technology, which is able to identify who is typing on the keyboard. The software will work with all browsers, email programs, newsgroups, ISPs and chat services. It should be noted that BioPassword is a fairly new technology. Configuration options on Net Nanny are similar to those provided by Cyber Snoop. The user can choose to establish a log that monitors all sites visited, programs used and words and phrases typed or received. Net Nanny can also be configured to block out words/phrases decided to be inappropriate, such as "where do you live?" or "what is your name?" This is probably the tool's best feature, as it may help to decrease the child's risk of finding himself in a dangerous situation while chatting. The BioPassword feature may also alleviate the risk of children overriding the password and gaining access to the configuration options. If the password is compromised, the BioPassword technology will be able to further identify the user and conclude he is not the administrator. Concerning classification content, Net Nanny's "can go" and "can't go" lists are researched and updated using information from CyberAngels Internet Safety Organization, Safeguarding Our Children, United Mothers and other organizations which seek to rate online content for the protection of children. Lastly, Net Nanny differs from other products on the market in that it allows its customer to have access to their "block lists", so parents can know specifically what materials is being screened out. Most companies that produce filtering tools keep their block lists proprietary and do not release them to the public. A similar product is CYBERsitter (http://www.cybersitter.com).

Unfortunately, parents and educators are not guaranteeing safety for their children through the tool itself.

The above filtering/blocking tools will provide the parent with a greater sense of security than if the child were allowed to freely utilize the Internet, email, and chat rooms. The most apparent weakness of each tool is the child's ability to disable the tool or find ways around its control. If technology such as BioPassword becomes very reliable, however, it will be harder for children to assume administrator status and change configuration options. Until such technology is advanced, it is important for parents to supplement a filtering/blocking tool with other resources. Unfortunately, parents and educators are not guaranteeing safety for their children through the tool itself. Children are still at risk of being abducted or harassed as a result of online communication. Simple guidelines set by the parent, however, may alleviate this problem and create a greater sense of trust between parent and child.

Larry Magid, a *Los Angeles Times* writer who has authored numerous columns on children's safety, advises "the best way to assure that your children are

continued on page 25

Filtering Tools

continued from page 24

having positive online experiences is to stay in touch with what they are doing" (Magid, 1998). This is probably the most useful approach a parent/educator can take in making their children's online experiences safer and more enjoyable. Of course, parents are not able to be at their child's side each and every time they interact online. However, procedures such as sharing an email account with your child or monitoring any files downloaded to the computer may alleviate some worry on the part of the parent.

Parents need not overreact in their guidelines; simply establish a mutual trust that will govern the child's online interactions. Essentially, the same parenting skills used in the real world can be applied to the cyber world. If adamantly told not to do something, a child may rebel and do it regardless of the warning. The same principles apply to online interaction. Therefore, parents/educators should allow the child enough freedom on the Internet but also protect safety and privacy.

There is much to be learned from children. If you are a parent who is uncomfortable around computers or are an inexperienced Internet user, ask your child to help you log on and point out certain things while surfing. You can inquire as to what content they usually access or how to better utilize your online service. When getting started online, try to visit sites centered on children, such as Bonus.com's SuperSite for Kids (http://www.bonus.com) or Disney's Blast Online (http://www.disney.com). These sites provide children with a contained environment that features a multitude of fun and educational activities. Bonus.com boasts more than 900 activities all in one place, and is a free site accessible to those who have World Wide Web access. Disney, for a small monthly fee, provides D-Mail and D-Browser, which are powerful communication tools that allow different levels of communication settings for each member of the family. As you become an experienced Internet user, you will naturally become increasingly more active in your child's online experiences. If you are having trouble getting started, try reading Donna Rice Hughes' new book, *Kids Online: Protecting Your Children in Cyberspace*. If you are familiar with the Web and looking for useful information, try Barbara Feldman's syndicated column, "Surfing the Net with Kids" at http://www.surfnetkids.com. The column reviews five Web sites each week, and the online archive is useful for accessing previous columns by subject or date. By establishing a plan of action and spending time with your children, you are accomplishing two goals: becoming more educated and establishing a mutual trust.

References

Hughes, D.R. and Campbell, P. T. (1998). *Kids Online. Protecting Your Children in Cyberspace*. Grand Rapids, MI: Fleming H. Revell Co.

Magid, L. (1998) Child Safety on the Information Highway. http://www.safekids.com/child_safety.htm. October 22, 1998.

The author is a Senior Technical Associate at AT&T Labs-Research in Florham Park, New Jersey. She co-authored the Technology Inventory: A Catalog of Tools that Support Parents' Ability to Choose Online Content Appropriate for their Children. Some of the content appearing in this article was taken from the Inventory, and further information can be found at http://www.research.att.com/projects/tech4kids/.

APSAC's Five Day Child Forensic Interview Clinic

March 7-12, 1999 (in conjunction with Huntsville Symposium on Child Sexual Abuse)
May 30 - June 5, 1999 (in conjunction with APSAC's 7th National Colloquium, San Antonio, TX)

APSAC's comprehensive interview clinic is an intensive forty-hour training experience which provides personal interaction with leading clinicians, researchers, and trainers in the field of child forensic interviewing. The interview practicum component provides participants with experience interviewing actual children in a supportive environment with constructive feedback offered to build and improve specific professional skills.

To add your name to the Forensic Clinic Mailing List, please complete and return this form by fax to 312-554-0919.

Name _____ Title _____

Agency Name _____ Address _____

City _____ State _____ Zip _____

Phone _____ Fax _____ E-mail _____