

Child Safety on the Information Highway

By Lawrence J. Magid

(c) 1998 National Center for Missing and Exploited Children

"'Cyberspace,' the 'Web,' the 'Net,' the 'Information Highway'" —

Whatever it's called, millions of people are now going online to exchange electronic mail, surf the World Wide Web, post and read messages in newsgroups (sometimes called bulletin boards), and participate in chat groups and many other online activities.

There are a number of ways to get online. In addition to major commercial online services, there are thousands of Internet Service Providers (ISPs) that provide Internet access. Telephone companies, cable TV companies, and even some local newspapers offer Internet access, usually for a monthly fee. Although most people use personal computers to get online, it's now possible to purchase a special adapter that allows you to access the Internet from a TV set.

ISPs and online services generally do everything they can to provide their subscribers with an enjoyable, safe, and rewarding online experience, but it's not possible for these companies to police everyone who uses their service anymore than a local government can control the behavior of its citizens. Besides, once you're connected to the Internet, you're able to exchange information with people who are signed on with other ISPs and online services. The Internet is a vast global network of networks that's not governed by any company or government.

Anyone in the world — companies, governments, organizations, and individuals — can publish material on the Internet. An ISP links you to these sites, but it can't control what is on them. It's up to individuals to make sure that they behave in a way that's safe and appropriate.

The Benefits of the Information Highway

The vast array of services that you currently find online is constantly growing. **Reference information** such as news, weather, sports, stock quotes, movie reviews, encyclopedias, and airline fares are readily available online. Users can conduct **transactions** such as trading stocks, making travel reservations, banking, and shopping online. You can find information about your local schools and government, read an out-of-town newspaper, or obtain vital health information. Millions of people **communicate** through electronic mail (E-mail) with family and friends around the world. Others use the public message board chat areas to make new friends who share common interests. You can even use the Internet to watch video and listen to audio programs produced by major media companies, businesses, organizations, and even individuals. As an **educational and entertainment tool** users can learn about virtually any topic, visit a museum, take a college course, or play an endless number of computer games with other users or against the computer itself.

"As an educational...tool users can learn about virtually any topic..."

Most people who go online have mainly positive experiences. But, like any endeavor — traveling, cooking, or attending school — there are some risks. The online world, like the rest of society, is made up of a wide array of people. Most are decent and respectful, but some may be

rude, obnoxious, insulting, or even mean and exploitative. Children get a lot of benefit from being online, but they can also be targets of crime and exploitation in this as in any other environment. Trusting, curious, and anxious to explore this new world and the relationships it brings, children need parental supervision and common-sense advice on how to be sure that their experiences in "cyberspace" are happy, healthy, and productive.

Putting the Issue in Perspective

Although there have been some highly publicized cases of abuse involving the Internet and online services, reported cases are relatively infrequent. Of course, like most crimes against children, many cases go unreported, especially if the child is engaged in an activity that he or she does not want to discuss with a parent.

The fact that crimes are being committed online, however, is *not* a reason to avoid using these services. To tell children to stop using these services would be like telling them to forgo attending school because students are sometimes victimized there.

A better strategy would be to instruct children about both the benefits and dangers of cyberspace and for them to learn how to be "street smart" in order to better safeguard themselves in any potentially dangerous situation.

What Are the Risks?

There are a few risks for children who use the Internet or online services. Teenagers are particularly at risk because they often use the computer unsupervised and because they are more likely than younger children to participate in online discussions regarding companionship, relationships, or sexual activity. If you have a teen in your family or you are a teenager, check out *Teen Safety on the Information Highway* at www.missingkids.com or order a free copy by calling 1-800-843-5678.

"Teenagers are particularly at risk because... they are more likely... to participate in online discussions regarding companionship..."

Some risks are

Exposure to Inappropriate Material

One risk is that a child may be exposed to inappropriate material that is sexual, hateful, or violent in nature, or encourages activities that are dangerous or illegal.

Physical Molestation

Another risk is that, while online, a child might provide information or arrange an encounter that could risk his or her safety or the safety of other family members. In a few cases, pedophiles have used E-mail, bulletin boards, and chat areas to gain a child's confidence and then arrange a face-to-face meeting.

Harassment

A third risk is that a child might encounter E-mail or chat/bulletin board messages that are harassing, demeaning, or belligerent.

Legal and Financial

There is also the risk that a child could do something that has negative legal or financial consequences such as giving out a parent's credit card number or doing something that violates another person's rights. Legal issues aside, children should be taught good "netiquette" which means to avoid being rude, mean, or inconsiderate.

How Parents Can Reduce the Risks

While children need a certain amount of privacy, they also need parental involvement and supervision in their daily lives. The same general parenting skills that apply to the "real world" also apply while online.

If you have cause for concern about your children's online activities, talk to them. Also seek out the advice and counsel of teachers, librarians, and other Internet and online service users in your area. Open communication with your children, utilization of such computer resources, and getting online yourself will help you obtain the full benefits of these systems and alert you to any potential problem that may occur with their use. If your child tells you about an upsetting person or thing encountered while online, don't blame your child but help him or her avoid problems in the future. Remember — how you respond will determine whether they confide in you the next time they encounter a problem and how they learn to deal with problems on their own.

"While children need a certain amount of privacy, they also need parental involvement."

Beyond these basics, there are some specific things that you should know about the Internet. For instance, did you know that there are web sites and newsgroups that have material that is hateful, is violent, or contains other types of material that parents might consider to be inappropriate for their children? It's possible for children to stumble across this type of material when doing a search using one of the web sites that is specifically designed to help people find information on the Internet. Most of these sites (called "search engines") do not, by default, filter out material that might be inappropriate for children, but some offer a child-safe option and some are designed specifically for use by children.

Also the Internet contains web sites, newsgroups, and other areas designed specifically for adults who wish to post, view, or read sexually explicit material including stories, pictures, and videos. Some of this material is posted on web sites where there is an attempt to verify the user's age and/or a requirement for users to enter a credit card number on the presumption that children do not have access to credit card numbers. Other areas on the Internet make no such effort to control access. Nevertheless, consider monitoring your credit card bills for such charges.

Some online services and ISPs allow parents to limit their children's access to certain services and features such as adult-oriented web sites and "chat" rooms and bulletin boards. There may be an area set aside just for kids where you don't have to worry about them stumbling onto inappropriate material or getting into an unsupervised chat.

At the very least, keep track of any files your children download to the computer, consider sharing an E-mail account with your children to oversee their mail, and consider joining your children when they are in private chat areas.

"The best way to assure that your children are having positive online experiences is to stay in touch with what they are doing."

In addition, there are filtering features built into the popular Internet browsers (the software you use to access the World Wide Web) that empower parents to limit their children's access only to those sites that have been rated appropriate for children. Other useful tools are software programs that block web sites, newsgroups, and chat areas that are known to be inappropriate for children. Most of these programs can be configured by the parent to filter out sites that contain nudity, sexual content, hateful or violent material, or that advocate the use of drugs, tobacco, or alcohol. Some can also be configured to prevent children from revealing information about themselves such as their name, address, or telephone number. You can find a directory of these filtering programs at www.safekids.com/filters.htm.

While technological child-protection tools are worth exploring, they're not a panacea. Regardless of whether you choose to use a filtering program or an Internet rating system, the best way to assure that your children are having positive online experiences is to stay in touch with what they are doing. One way to do this is to spend time with your children while they're online. Have them show you what they do, and ask them to teach you how to use the Internet or online service. You might be surprised at how much you can learn from your kids.

Guidelines for Parents

By taking responsibility for your children's online computer use, parents can greatly minimize any potential risks of being online. Make it a family rule to

- Never give out identifying information — home address, school name, or telephone number — in a public message such as chat or bulletin boards (newsgroup), and be sure you're dealing with someone that both you and your child know and trust before giving out this information via E-mail. Think carefully before revealing any personal information such as age, marital status, or financial information. Do not post photographs of your children on web sites or newsgroups that are available to the public. Consider using a pseudonym, avoid listing your child's name and E-mail address in any public directories and profiles, and find out about your ISP's privacy policies and exercise your options for how your personal information may be used.
- Get to know the Internet and any services your child uses. If you don't know how to log on, get your child to show you. Have your child show you what he or she does online, and become familiar with all the things that you can do online.
- Never allow a child to arrange a face-to-face meeting with another computer user without parental permission. If a meeting is arranged, make the first one in a public place, and be sure to accompany your child.

"If a meeting is arranged, make the first one in a public place, and be sure to accompany your child."

- Never respond to messages or bulletin board items that are suggestive, obscene, belligerent, threatening, or make you feel uncomfortable. Encourage your children to tell you if they encounter such messages. If you or your child receives a message that is harassing, of a sexual nature, or threatening, forward a copy of the message to your ISP, and ask for their assistance.

Instruct your child **not** to click on any links that are contained in E-mail from persons they don't know. Such links could lead to sexually explicit or otherwise inappropriate web sites.

- If someone sends you or your children messages or images that are obscene, lewd, filthy, or indecent with the intent to harass, abuse, annoy, or threaten, or if you become aware of the transmission, use, or viewing of child pornography while online, immediately report this to the National Center for Missing and Exploited Children's CyberTipline at 1-800-843-5678 or www.missingkids.com/cybertip.
- Remember that people online may not be who they seem. Because you can't see or even hear the person it would be easy for someone to misrepresent him- or herself. Thus, someone indicating that "she" is a "12-year-old girl" could in reality be a 40-year-old man.
- Remember that everything you read online may not be true. Any offer that's "too good to be true" probably is. Be very careful about any offers that involve you coming to a meeting, having someone visit your house, or sending money or credit card information.
- Set reasonable rules and guidelines for computer use by your children (see "My Rule for Online Safety" on the backcover). Discuss these rules and post them near the computer as a reminder. Remember to monitor your children's compliance with these rules, especially when it comes to the amount of time your children spend on the computer. A child's excessive use of online services or the Internet, especially late at night, may be a clue that there is a potential problem. Remember that personal computers and online services should not be used as electronic babysitters.
- Check out blocking, filtering, and ratings.
- Be sure to make this a family activity. Consider keeping the computer in a family room rather than the child's bedroom. Get to know their "online friends" just as you get to know all of their other friends.

My Rules for Online Safety

- I will not give out personal information such as my address, telephone number, parents' work address/telephone number, or the name and location of my school without my parents' permission.
- I will tell my parents right away if I come across any information that makes me feel uncomfortable.
- I will never agree to get together with someone I "meet" online without first checking with my parents. If my parents agree to the meeting, I will be sure that it is in a public place and bring my mother or father along.
- I will never send a person my picture or anything else without first checking with my parents.
- I will not respond to any messages that are mean or in any way make me feel uncomfortable. It is not my fault if I get a message like that. If I do I will tell my parents right away so that they can contact the online service.

- I will talk with my parents so that we can set up rules for going online. We will decide upon the time of day that I can be online, the length of time I can be online, and appropriate areas for me to visit. I will not access other areas or break these rules without their permission.

About this Document

This brochure was written by Lawrence J. Magid, a syndicated columnist for the *Los Angeles Times*, who is author of *The Little PC Book* (Peachpit Press) and host of www.safekids.com, a web site devoted to keeping kids safe in cyberspace. He is also the author of *Teen Safety on the Information Highway*, a free brochure that is also published by the National Center for Missing and Exploited Children. *Child Safety on the Information Highway* was jointly produced by the National Center for Missing and Exploited Children and Internet Alliance (formerly Interactive Services Association), PO Box 65782, Washington, DC 20035-5782, 202-955-8091, ia@internetalliance.org. The first edition of this brochure was created with the generous sponsorship of America Online®, CompuServe®, Delphi™ Internet, e•World, GENie®, Interchange™ Online Network, and Prodigy® Services.

The National Center for Missing and Exploited Children (NCMEC) is funded under Cooperative Agreement #98-MC-CX-K002 from the Office of Juvenile Justice and Delinquency Prevention, Office of Justice Programs, U.S. Department of Justice. Points of view or opinions in this brochure are those of NCMEC and do not necessarily represent the official position or policies of the U.S. Department of Justice.

Copyright © 1994 and 1998 by the National Center for Missing and Exploited Children. All rights reserved.

[National Center for Missing and Exploited Children](#)

Suite 550, 2101 Wilson Boulevard
Arlington, Virginia 22201-3077
1-800-THE-LOST (1-800-843-5678)

<http://safekids.com/>