Keeping Kids Safer on the Internet

Tips for Parents and Guardians

NATIONAL CENTER FOR MISSING & EXPLOITED CHILDREN®

OJJDP Office of Juvenile Justice and Delinquency Prevention
Office of Justice Programs ♦ U.S. Department of Justice

1 Where Do Kids Connect?

3 Browsing the Internet

4 Using E-mail

5 Social Networking

8 Posting Videos and Photos Online

9 Using Peer-to-Peer Systems

10 Other Ways to Enhance Kids' Online Safety Skills

12 Online Resources for Families

Back Cover Tips for Parents and Guardians

Keeping Kids Safer on the Internet was made possible through the joint efforts and expertise of the National Center for Missing & Exploited Children® programs noted below.

CyberTipline® is the Congressionally mandated, online-reporting tool for child sexual exploitation. For more information visit www.cybertipline.com.

The NetSmartz® Workshop is an online, educational resource to help teach kids how to be safer both on- and offline. For more information visit NetSmartz online at www.NetSmartz.org.

This project was supported by Grant No. 2005-MC-CX-K024 awarded by the Office of Juvenile Justice and Delinquency Prevention, Office of Justice Programs, U.S. Department of Justice, and Grant No. GA97-0001 awarded by the U.S. Secret Service, Department of Homeland Security. Points of view or opinions in this document are those of the author and do not necessarily represent the official position or policies of the U.S. Department of Justice or Department of Homeland Security. National Center for Missing & Exploited Children®, CyberTipline®, and NetSmartz® Workshop are registered service marks of the National Center for Missing & Exploited Children.

Copyright © 2006 National Center for Missing & Exploited Children. All rights reserved.

Keeping Kids Safer on the Internet: Tips for Parents and Guardians is the National Center for Missing & Exploited Children's newest publication addressing Internet safety. This brochure replaces four earlier NCMEC titles — *Child Safety on the Information Highway, The CyberTipline®: Your Resource for Reporting the Sexual Exploitation of Children, NetSmartz® Workshop: Keeping Kids and Teens Safer on the Internet, and Teen Safety on the Information Highway.*

Special thanks to Larry Magid, author of the original *Child/Teen Safety on the Information Highway brochures.*

provide

explore
guidance
discussion
educate
online skills
confidence
safety

Allowing kids to go online without supervision or ground rules is like allowing them to explore a major metropolitan area by themselves. The Internet, like a city, offers an enormous array of entertainment and educational resources but also presents some risks. Kids need help navigating this world.

Where Do Kids Connect?

- Kids go online almost anywhere. They surf the Internet and send messages from a home computer or one at a friend's home, library, or school.
- Kids connect at coffee shops and other "hotspots" using laptops and wireless connections.
- Internet-enabled, video-game systems allow them to compete against and chat with players around the world.
- Cell phones enable kids to surf the web and exchange messages, photos, and short videos from just about anywhere.

You can't watch your kids every minute, but you do need to use strategies to help them benefit from the Internet and avoid its risks.

By exploring the Internet with your kids, you greatly expand its capacity as an educational tool. By providing guidance and discussion along the way, you increase kids' online skills and confidence along with their ability to avoid risks. And you might be surprised by what kids teach you at the same time.

you can't take it back...

think before you type

We at the National Center for Missing & Exploited Children® (NCMEC) urge you to do one of the single most important things to promote safety — begin a dialogue with your kids about the rewards and risks of Internet use. We also encourage you to visit the NetSmartz® Workshop at www.NetSmartz.org and CyberTipline® at www.cybertipline.com to learn more about online safety.

It's up to parents and guardians to assess the risks and benefits of permitting their kids to use the wide range of Internet sites and services available. This brochure provides a list of the most popular online activities for kids along with the strategies for and benefits of reducing the risks associated with those activities.

According to the U.S. Department of Education, 23 percent of nursery school children in the United States use the Internet, 32 percent of kindergartners go online, and by high school 80 percent of children use the Internet.[1]

[1] U.S. Department of Education, "Rates of Computer and Internet Use by Children in Nursery School and Students in Kindergarten through Twelfth Grade: 2003," *in Issue Brief*, October 2005, page 1, NCES 2005111rev, accessed June 15, 2006, at http://nces.ed.gov/pubs2005//2005111rev.pdf.

Browsing the Internet

Benefits

Browsing the Internet is like having the world's largest library and entertainment system at your fingertips. Kids can read stories, tour museums, visit other countries, play games, look at photographs, shop, and do research to help with homework.

Risks

- Kids may come across sites containing adult images or demeaning, racist, sexist, violent, or false information.
- It is hard for kids to distinguish reliable sources of information from less reliable ones. Some believe because information is posted online it must be true.

Tips to Minimize Risks

- Choose search engines carefully. Some are specifically designed for kids, and others offer kid-safe options.
- Tell kids when they come across any material making them feel scared, uncomfortable, or confused to immediately tell you or another trusted adult.
- Help kids find information online. By searching the Internet together you help them find reliable sources of information and distinguish fact from fiction.

Many Internet service providers (ISPs) offer filters to prevent kids from accessing inappropriate sites. Talk to your ISP about what safe-search options they offer. Remember, as a consumer you have a right to choose an ISP with the services meeting your family's needs.

Using E-mail

Benefits

Adults and kids use E-mail to communicate rapidly and cost-effectively with people all over the world. E-mail transmits messages, documents, and photos to others in a matter of seconds or minutes.

Risks

- Kids can set up private accounts through free web-based, E-mail services without asking permission from parents or guardians.
- Anyone using E-mail is vulnerable to receiving "spam," messages from people or companies encouraging recipients to buy something, do something, or visit a particular web site. Spam may be sexually suggestive or offensive in other ways.
- Senders sometimes disguise themselves, pretending to be someone else — a friend or acquaintance, a well-known bank, a government agency — for illicit purposes. This is known as phishing.

Tips to Minimize Risks

- Talk with your kids about their E-mail accounts, and discuss the potential risks involved.
- Before you sign up with an ISP research the effectiveness of its spam filters. You may also purchase spam-filter software separately.
- Teach kids not to open spam or E-mails from people they don't know in person. Remind them not to respond to any online communication in a sexually provocative way. Ask them to show you suspicious communications.
- If your kids receive E-mail containing threats or material making them feel scared, uncomfortable, or confused, report it to your ISP. Your ISP's address is usually found on the service's homepage.

- Report E-mails with evidence of online sexual exploitation, such as child pornography, to the CyberTipline at www.cybertipline.com or 1-800-843-5678. NCMEC will refer your report to the appropriate law-enforcement agency.

Social Networking

Benefits

Social networking sites allow kids to express themselves and keep in touch with friends by exchanging messages or comments and posting personal profiles describing who they are and their interests, blogs or online diaries, photos, creative writing, artwork, videos, and music.

Instant Messaging (IM) and sharing online profiles are popular forms of social networking.

A survey of 10 to 17 year olds revealed 34% had posted their real names, telephone numbers, home addresses, or the names of their schools online where anyone could see; 45% had posted their dates of birth or ages; and 18% had posted pictures of themselves.[2]

Risks

- Some sites and services ask users to post a "profile" with their age, sex, hobbies, and interests. While these profiles help kids "connect" and share common interests, potential exploiters can and do use these profiles to search for victims.
- Kids sometimes compete to see who has the greatest number of contacts and will add new members to their lists even if they don't know them in person.

[2] Janis Wolak, Kimberly Mitchell, and David Finkelhor. *Online Victimization of Youth: Five Years Later.* Alexandria, Virginia: National Center for Missing & Exploited Children, 2006, page 50.

- Users may pose as someone else — a different person or person of a different age — without others knowing. Such users have taken advantage of this and social-networking profiles to entice or sexually exploit kids.
- Kids can't "take back" the online text and images they've entered. Once online, "chat" as well as other web postings become public information. Many web sites are "cached" by search engines, and photos and text can be retrieved long after the site has been deleted.
- Kids have been punished by their families; denied entry into schools; and even not hired because of dangerous, demeaning, or harmful information found on their personal sites or blogs.

Kids don't need to enter a chatroom to "chat" via the Internet. They also communicate with others on gaming sites; on IM sites; and via Internet Relay Chat (IRC) networks, which enable computer-to-computer access.

Tips to Minimize Risks

- Urge kids to restrict access to their profiles so only those on their contact lists are able to view them. Explain to them unrestricted posting of profiles places their personal information in a public forum and could put them at risk from those who wish to take advantage of such information.

- Encourage them to choose gender-neutral screennames or nicknames — such as their initials or a word. Make sure the name doesn't include information revealing their identity or location.
- Remind kids to use the privacy settings on social-networking sites to restrict access to their "spaces" or blogs to only people they know in person.
- Visit social networking sites with your kids, and exchange ideas about what you think is safe and unsafe.
- Ask your kids about the people they are communicating with online.
- Insist your kids never give out personal information or arrange to meet in person with someone they've met online without first checking with you.

- If your kids receive an IM from someone they don't know, tell them to block the sender. Remind kids to IM only people they know in person and who have been approved by you.
- Encourage your kids to think before typing, "Is this message hurtful or rude?" Also urge your kids not to respond to any rude or annoying messages or ones making them feel scared, uncomfortable, or confused. Have them show you such messages.

What's a P911? It's shorthand for "parent alert" — a code some kids use to let others know a parent or guardian is watching. If you have trouble translating your kids online "lingo," visit www.NetSmartz.org. There you'll find a list of popular terms and abbreviations used in IM and chatrooms.

Posting Videos and Photos Online

Benefits

Webcams, microphones, and digital cameras allow kids to post videos, photos, and audio files online and engage in video conversations. Kids often use this equipment to see each other as they IM and chat.

Webcams are often used by extended families to help kids stay in touch with distant relatives, traveling parents and guardians, and other family members and friends.

Risks

- Webcam sessions and photos can be easily captured, and users can continue to circulate those images online. In some cases people believed they were interacting with trusted friends but later found their images were distributed to others or posted on web sites.
- Kids may come across offensive or inappropriate images and videos while surfing the web.

Tips to Minimize Risks

- Kids should use webcams or post photos online only with your knowledge and supervision.
- Remind your kids to ask themselves if they would be embarrassed if their friends or family saw the pictures or video they post online. If the answer is yes, then they need to stop.
- Remind kids to be aware of what is in the camera's field of vision and remember to turn the camera off when it is not in use.
- Caution kids about posting identity-revealing or sexually provocative photos. Don't allow them to post photos of others — even their friends — without permission from their friends' parents or guardians. Remind them once such images are posted they relinquish control of them and can never get them back.

- Remind kids to immediately tell you or another trusted adult if they come across inappropriate material. If it is lewd, obscene, or contains illegal material, report it to NCMEC's CyberTipline at www.cybertipline.com or 1-800-843-5678. If not report it to your service provider and ask what they will need for review and investigative purposes.

Using Peer-to-Peer Systems

Benefits

Also known as P2P these systems make it possible for people to exchange files without having to go through a web site or other centralized system. P2P systems allow kids to exchange music, videos, movies, photographs, documents, and software.

Risks

- It is illegal to share copyrighted materials without permission. Just because something is available online doesn't mean it is legal to copy, download, or use.
- Users may not know what they have downloaded until it's on their computers. By sharing files kids could unknowingly end up downloading and distributing harmful viruses and even illegal material such as child pornography.

Tips to Minimize Risks

- Carefully check out the file-sharing services your kids want to use. Make sure the services are not offering copyrighted material without the permission of the author or artist. Also check to make sure the sites do not offer material inappropriate for your kids.

Other Ways to Enhance Kids' Online Safety Skills

Begin a Dialogue With Your Kids About Internet Use

Because we use the Internet in different ways, kids and adults can learn from each other. By talking about Internet use with your kids, you are opening the door to discussing the important issues of personal safety and helping them engage in responsible behavior. Use this brochure as a starting point, or visit www.NetSmartz.org to find safety resources for both kids and adults.

Consider Rating, Blocking, Monitoring, and Filtering Applications for Your Computer

Software and services are available to help parents and guardians set limits on kids' Internet use. Most computer operating systems have optional filters allowing parents and guardians to block sites they consider inappropriate. Some services rate web sites for content. Some programs prevent users from entering information such as names and addresses, and others keep kids away from chatrooms or restrict their ability to send or read E-mail. Monitoring programs allow you to see where your kids go online. But remember these programs and services don't develop kids' own sense of safety, and they are not substitutes for parental/guardian communication, supervision, and involvement.

Make Internet Use a Family Activity While Encouraging Critical Thinking

By setting aside time to go online with your kids you not only become more aware of what they do online, you reinforce positive Internet skills. Helping your kids with a research project is a great opportunity for them to learn about and distinguish which sites provide reliable information, are simply someone's opinion, and are to be avoided entirely. And when looking at E-mails together ask, "Are these people who they seem to be?" These are prime opportunities to help kids develop their critical-thinking skills.

Set Reasonable Rules

Work with your kids to develop reasonable rules. Consider setting rules about the time of day, length of time, people they may communicate with, and appropriate areas for them to visit while online.

Encourage Your Kids to Go to You When They Encounter Problems Online

It's important to reassure kids if they encounter problems online or view something disturbing, it's not their fault. Discussing these issues openly may reduce their fear of going to you if they encounter something online making them feel scared, uncomfortable, or confused. Be a resource. Let them know if they share the experience with you, you will try to help, not punish, them. At the same time help them understand what happened and avoid similar situations in the future.

Online Resources for Families

NetSmartz Workshop

The NetSmartz Workshop is an online educational resource to help teach kids how to be safer both on- and offline.

The NetSmartz Workshop is designed to be used at home, at school, and in the community. It provides parents, guardians, educators, community leaders, and law-enforcement officials with a wide variety of resources including activities, games, Internet safety pledges, and real-life stories. These resources help adults build kids' safety awareness, prevent their victimization, and increase their self-confidence on- and offline.

The NetSmartz Workshop was developed by the National Center for Missing & Exploited Children and Boys & Girls Clubs of America. NetSmartz content is developed in consultation with educators, administrators, and kids to help ensure its appeal to all age groups. Access the NetSmartz Workshop resources at www.NetSmartz.org.

kids
parents
teens
educators
guardians
community leaders
law-enforcement officials

CyberTipline

Visit www.cybertipline.com or call 1-800-843-5678 to report the sexual exploitation of children on- and offline. The CyberTipline accepts information about the possession, manufacture, and distribution of child pornography; online enticement of children for sexual acts; child victims of prostitution; child sex-tourism; child sexual molestation not in the family; unsolicited obscene material sent to a child; and misleading domain names. Your information will be forwarded to law enforcement for investigation and review, and, when appropriate, to Internet service provider(s).

Don't Believe the Type

Created by the Ad Council and NCMEC, "Don't Believe the Type," is part of a public-service campaign specifically designed to help teens recognize the dangers of the Internet, situations to avoid, and how to "surf safer." Visit www.cybertipline.com, and click on "Don't Believe the Type" to view the web site.

HDOP: Help Delete Online Predators

A part of NCMEC's Ad Council public-service campaign, "Help Delete Online Predators" provides information to parents and guardians about online sexual exploitation. It includes real-life stories about online exploitation, tips for talking with kids, and a list of commonly used chat abbreviations. Visit www.cybertipline.com, and then click on "HDOP" to view the web site.

Tips for Parents and Guardians

- Begin a dialogue with your kids about Internet use and supervise their online activities
- Consider rating, blocking, monitoring, and filtering applications for your computer
- Make Internet use a family activity
- Encourage your kids' critical-thinking skills
- Set reasonable rules
- Encourage your kids to go to you when they encounter problems online

Find More Help Online

Visit www.NetSmartz.org for a wealth of additional safety resources including

- Suggestions for discussing online and real-world safety with kids
- Videos about teens' real-life experiences on the Internet
- Informative statistics about kids' Internet use
- Suggestions for what to do if a kid encounters a dangerous situation online or in the real world
- A list of terms kids commonly use in IM and chatrooms
- Tips for avoiding cyberbullying
- Articles about current and developing Internet and real-world safety issues

Help Us Promote a Safer Internet

If you have information to help NCMEC in the fight against child sexual exploitation, please report it to the CyberTipline at www.cybertipline.com or 1-800-843-5678.