

Keeping Kids Safer on the Internet



Tips for Parents and Guardians

1	Where Do Kids Connect?
2	Browsing the Internet
3	Social Networking
5	Using E-Mail
6	Instant Messaging
7	Cell Phones/ Wireless Devices and Texting
8	Posting Videos and Photos Online
9	Online Gaming
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® (NCMEC) programs noted below.

CyberTipline® is the Congressionally authorized reporting mechanism for child sexual exploitation. For more information visit www.cybertipline.com or call 1-800-843-5678.

NetSmartz® Workshop is an interactive, educational safety program providing age-appropriate resources to help teach kids how to be safer online and in the real world. For more information visit www.NetSmartz.org.

This project was supported by Grant No. 2011-MC-CX-K001 awarded by the Office of Juvenile Justice and Delinquency Prevention, Office of Justice Programs, U.S. Department of Justice. This document is provided for informational purposes only and does not constitute legal advice or professional opinion on specific facts. Information provided in this document may not remain current or accurate, so recipients should use this document only as a starting point for their own independent research and analysis. If legal advice or other expert assistance is required, the services of a competent professional should be sought. 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. CyberTipline®, National Center for Missing & Exploited Children®, NetSmartz®, and NetSmartz411® are registered trademarks of the National Center for Missing & Exploited Children. NCMEC Order #168.

Copyright © 2006, 2009, and 2011 National Center for Missing & Exploited Children. All rights reserved.

Special thanks to Larry Magid, author of two earlier NCMEC brochures about this topic.

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

provide
explore
guidance
discussion
educate
online skills
confidence
safety

Where Do Kids Connect?

In general, kids

- Connect to the Internet from a computer at home, a library, school, or friend's home
- Connect from anywhere using laptops, cell phones, handheld devices, and other wireless devices
- Compete against and chat with players around the world using Internet-enabled gaming systems
- Exchange messages, photos, and videos via the Internet at any time

You cannot watch your kids every minute, but you can use strategies to help them benefit from the Internet and avoid its potential 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 their online skills and confidence along with their ability to avoid potential risks. And you might be surprised by what kids teach you at the same time.

you can't take it back...

think before you



The National Center for Missing & Exploited Children® (NCMEC) urges you to do perhaps the most important thing to promote online safety — have a conversation with your kids about the rewards and potential risks of Internet use. Visit NetSmartz® Workshop at www.NetSmartz.org and NetSmartz411® at www.NetSmartz411.org or call 1-888-NETS411 (638-7411) to learn more about online safety.

It is up to parents and guardians to assess the potential risks and benefits of permitting their kids to use the Internet and wireless devices.

According to the U.S. Department of Education, 81% of children as young as 3 years old are using the Internet. That percentage continues to increase with age with the highest percentage of usage at 88% for children age 15 to 19.¹

Browsing the Internet

Benefits

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

Potential Risks

- Kids may come across websites containing adult images or demeaning, racist, sexist, violent, or false information.
- Kids may find it difficult to determine the credibility or reliability of information found on the Internet. Some mistakenly believe because something is posted online it must be true.

¹ U.S. Department of Education, *Digest of Education Statistics 2010*, April 2011, page 36, accessed October 10, 2011, at www.nces.ed.gov/pubs2011/2011015.pdf.

Tips to Minimize Potential Risks

- Choose an Internet browser with safety options appropriate for your family. There are browsers that are specifically designed for kids, as well as browsers that offer safer and age-appropriate filtering options. Many electronic service providers (ESPs) offer free filters to help prevent kids from accessing inappropriate websites. Contact your ESP to learn what Internet-safety options are available.
- Teach your kids that if they see any material which makes them feel scared, uncomfortable, or confused to immediately tell you or another trusted adult. A trusted adult is a person you have come to rely on and with whom you and your kids feel comfortable.
- Help your kids find information online. By searching the Internet together you can help them find reliable sources of information and distinguish fact from fiction.

Social Networking

Benefits

Social-networking websites allow kids to connect with their friends and other users. Kids are able to socialize and express themselves by exchanging instant messages and e-mails, and by posting comments, articles, photos, artwork, videos, and music to their blogs and personal profiles. Some 73% of online teens use social-networking websites.²

A survey of 12 to 17 year olds revealed 38% had posted self-created content such as photos, videos, artwork, or stories.³ Another survey of 10 to 17 year olds revealed 46% admit to having given out their personal information to someone they did not know. The likelihood kids will give out personal information over the Web increases with age with 56% of 16 to 17 year olds most likely sharing personal information.⁴

² Amanda Lenhart, Kristen Purcell, Aaron Smith, and Kathryn Zickuhr. *Social Media & Mobile Internet Use Among Teens and Young Adults*. Washington, DC: Pew Internet & American Life Project, February 3, 2010, page 17, accessed October 10, 2011, at www.pewinternet.org/Reports/2010/Social-Media-and-Young-Adults.aspx.

³ *Id.*, page 23.

⁴ Andrea Pieters and Christine Krupin. *Youth Online Behavior*. Santa Clara, CA: Harris Interactive, June 1, 2010, page 11, accessed October 10, 2011, at www.safekids.com/mcafee_harris.pdf.

Potential Risks

- Social-networking websites often ask users to post a profile with their age, sex, hobbies, and interests. While these profiles help kids connect and share common interests, individuals who want to victimize kids can use those online profiles to search for potential victims.
- Kids sometimes compete to see who has the greatest number of contacts and will add new people to their lists even if they do not know them in real life.

Kids cannot “take back” the online text and images they post. Kids may display images or write information that is provocative, harmful, and/or inappropriate. Online Web postings are accessible by the public. Individuals who have access to this information can save and forward these postings to an unlimited number of users. Talk to your kids about how once images are posted online they lose control of them and can never get them back. Only allow your kids to post photos or any type of personally identifying information on websites with your knowledge and consent.



Kids may not realize the potential ramifications of their online activities. They can face consequences for posting harmful, explicit, dangerous, or demeaning information online including being humiliated in front of their families and peers, suspended from school, charged criminally, and denied employment or entry into schools.

Tips to Minimize Potential Risks

- Instruct your kids to use privacy settings to restrict access to profiles so only the individuals on their contact lists are able to view their profiles.
- Remind kids to only add people they know in real life to their contact lists.

- Encourage kids to choose appropriate screennames or nicknames. Talk to your kids about creating strong passwords, such as those that use the first letter of each word of a phrase or an easy-to-remember acronym.
- Visit social-networking websites with your kids, and exchange ideas about OK versus potentially risky websites.
- Ask your kids about the people they are communicating with online.
- Make it a rule with your kids that they can never give out personal information or meet anyone in person without your prior knowledge and consent. If you want to consider a meeting, talk to the other kid's parents/guardians. If you agree to the meeting, accompany your kids and meet with the other kid and his or her parents/guardians in a public place.
- Encourage your kids to think “Is this message harmful, dangerous, hurtful, or rude?” before posting or sending anything online. Teach your kids not to respond to any rude or harassing remarks or messages that make them feel scared, uncomfortable, or confused and to show you these messages instead.

Using E-Mail

Benefits

Adults and kids use e-mail as a way to quickly and cost-effectively communicate with people all over the world.

Potential Risks

- Kids can set up private accounts through free Web-based, e-mail services without asking permission from parents or guardians.
- People using e-mail are vulnerable to receiving “spam” messages. Individuals or companies send spam e-mails to encourage recipients to buy something, do something, or visit a particular website. Additionally, spam e-mail can include sexually suggestive or otherwise offensive material. Spam e-mails may also have attachments or links containing viruses that could be harmful if downloaded.

- Senders sometimes disguise themselves and pretend to be someone else — a friend or acquaintance, a well-known bank, a government agency — in an attempt to obtain your personal or financial information. This is known as phishing.

Tips to Minimize Potential Risks

- Talk with your kids about their e-mail accounts and the potential risks involved. Remind them to never share their passwords with anyone but you, not even their closest friends.
- Teach kids not to open spam or e-mails from people they do not know in real life and who have not been approved by you. Remind them not to respond to any online communication in a sexually provocative way. Tell them to show you any suspicious communications.
- Report to your service provider any e-mails your kids receive containing threats or material making them feel scared, uncomfortable, or confused. Your provider's address is usually found on their home page.



Instant Messaging

Benefits

Instant Messaging (IM) allows Internet users to have conversations in “real time.” IMing is particularly appealing to kids who use abbreviations to communicate with each other. Most IM services offer a feature showing a user's contacts, known as a “buddy list,” which tells the user whether a “buddy” is online and available to chat.

Potential Risks

IM is one method used to bully, harass, or intimidate others. It may also be used to engage kids in a sexually explicit conversation. IM interactions may go from an innocent conversation to a sexually explicit or otherwise inappropriate exchange without warning.

Tips to Minimize Potential Risks

- Remind kids to IM only people they know in real life and who have been approved by you.
- Use privacy settings to limit contact to only those individuals included on your kid's buddy list. Make sure other users cannot search for your kids by using their e-mail addresses and/or usernames.
- Make sure your kids and you are familiar with the blocking features available on most IM services. Tell your kids to block any sender they do not know in real life who IMs them.
- Take the time to learn the chat abbreviations used by kids so you understand what they are talking about with each other. If you have trouble translating your kids' online chat, visit www.NetSmartz411.org and search for "acronyms." There you will find a list of popular online terms and abbreviations.

Cell Phones/Wireless Devices and Texting

Benefits

Many parents and guardians look at a cell phone as a necessity for their kids. It is reassuring to know your kids may reach you or call for help in an emergency. Cell phones and wireless devices may also be used to send text messages, images, and videos.

Potential Risks

- Cell phones make it easy for kids to communicate with others without their parents' or guardians' knowledge.
- Some kids are now using cell phones and wireless devices to take sexually explicit photos of themselves or other kids and send the images to others. Once sent, there is no way to retrieve these photos or stop them from being forwarded to additional people. Images posted online can circulate forever, which damages the kid's reputation, and can even be used by offenders in an attempt to victimize other kids.
- Kids may also take embarrassing or revealing photos of others and post them online as a form of bullying.

Tips to Minimize Potential Risks

- Create rules and set limits about the appropriate use of cell phones and wireless devices including who your kids may communicate with and when they may use these devices.
- Review cell-phone records for any unknown numbers and late-night calls or text messages.
- Teach your kids to never post their cell phone number online.
- Talk to your kids about the possible implications of sending sexually explicit or provocative images of themselves or others.
- Consider removing or disabling the Internet features from your kid's cell phone and wireless device through your service provider or creating settings to control or prohibit access to the Internet, e-mail, or text messaging.

Posting Videos and Photos Online

Benefits

Webcams, cell phones, wireless devices, 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, chat, and play online games. Webcams are often used to help kids stay in touch with family members and friends including traveling parents and guardians and those living in other areas.

Potential Risks

- Capturing and saving webcam sessions and photos is easy and users may continue to circulate those images online. People may believe they are interacting with trusted friends but later find their images distributed to others or posted on websites.
- Capturing, sending, and posting sexually provocative and inappropriate images may lead to legal implications and other unexpected offline consequences.

Tips to Minimize Potential Risks

- Remind your kids to only use webcams or post photos online with your knowledge and supervision.
- Remind your kids to ask themselves if they would be embarrassed if their friends or family members saw the photos or videos 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.
- Tell your kids to never post identity-revealing or sexually provocative photos. Remind them once such images are posted they lose control of them and can never get them back.

Online Gaming

Benefits

Online gaming allows kids to engage with and challenge players from around the world over a computer network or on an Internet-enabled gaming console. Many online games have text, voice-, or video-enabled chat functions, allowing players to communicate as a group or in private. In addition online games often have associated online communities for players to share experiences and strategies. In many ways online games and gaming communities serve as a forum for social networking.

Potential Risks

- Because kids often game online with people they do not know in real life, you should speak with them about what information is appropriate to share.
- As with IM or social-networking websites, kids may be exposed to inappropriate language, harassed, threatened, or asked sexually explicit questions.

Tips to Minimize Potential Risks

- Keep the gaming console and computer in a common area of the home so you are able to monitor your kids' online communications more closely.
- Set rules, including how long your kids may play the games, with whom they are allowed to play, and what types of games are appropriate.
- Help your kids choose appropriate screennames or usernames. A screenname should never reveal any identifying information especially such things as name, age, location, year of birth, school name, and year of graduation. Talk to your kids about creating a strong password, such as one that uses the first letter of each word of a phrase or an easy-to-remember acronym.
- Review the games' rating systems to help you decide which games to allow in your home.
- Look into what types of protections or parental controls the gaming console allows and make use of them. Teach your kids to only video chat or IM with people they know in real life.

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 may 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 such as "Your Photo Fate." This powerful video is designed to help teens understand the consequences of posting and sharing inappropriate information and images. For more information visit www.NetSmartz.org/RealLifeStories and click on the link to "Your Photo Fate."

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 websites they consider inappropriate. Some services rate websites 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 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 also reinforce positive Internet skills. Helping your kids with a research project is a great opportunity for them to learn about which websites provide reliable information. 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. Posting clear, simple, easy-to-read rules is an excellent way to set boundaries for your kids' Internet use. Consider signing the rules with your kids and periodically reviewing them together. Rules should include limitations on the time of day they go online, the length of time they spend online, the people they may communicate with while online, and the appropriate areas for them to visit while online. Explain to your kids why these rules are important.

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

It is important to reassure kids if they encounter problems online or view something disturbing, it is not their fault. Discussing these issues openly may reduce their fear of going to you if they encounter something online that makes them feel scared, uncomfortable, or confused. Reassure your kids and let them know if they share the experience with you, you will try to help and will not punish them. At the same time you can help your kids

understand what happened and avoid similar situations in the future. If your kids or anyone in your home receives pornography depicting children or has been sexually solicited or received sexually explicit images from someone who knows the recipient is younger than 18, immediately report the information to local law enforcement and follow their instructions. You should keep the computer or cell-phone screen turned off in order to preserve any evidence for future law-enforcement use. Do not copy any of the images and/or text. You should also report the incident to the CyberTipline® at www.cybertipline.com or 1-800-843-5678.

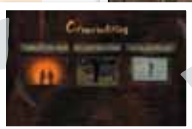
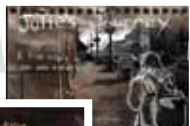
Online Resources for Families

NetSmartz® Workshop

NetSmartz Workshop is an interactive, educational safety program providing age-appropriate resources to help teach kids how to be safer online and in the real world.



NetSmartz is designed to be used in homes, schools, and communities. It provides parents, guardians, educators, community leaders, and law-enforcement officials with a wide variety of resources including activity cards, games, presentations, safety pledges, and videos.



kids
parents
teens
educators
tweens
community leaders
guardians
law-enforcement officials

These resources help trusted adults build kids' safety awareness, prevent their victimization, and increase their self-confidence online and in the real world. You may download these free resources at www.NetSmartz.org.

NetSmartz411

NetSmartz411 is the leading Internet-safety helpdesk and hotline for answers to parents' and guardians' questions about Internet safety, technology, and the Web. This free service is provided by NCMEC and sponsored by CenturyLink™. Visit NetSmartz411 for resources at www.NetSmartz411.org.

The website contains a searchable knowledgebase of frequently asked questions regarding technology and the Internet, along with the opportunity to ask questions of experts. You may get answers to your direct questions by asking online at www.NetSmartz411.org or by calling at 1-888-NETS411 (638-7411).

CyberTipline

NCMEC operates the CyberTipline®, the Congressionally authorized reporting mechanism for tips and leads relating to child sexual exploitation. Members of the public and electronic service providers can report to the CyberTipline instances of sexually based crimes committed against children including the possession, manufacture, and distribution of child pornography; online enticement of children for sexual acts; child prostitution; sex tourism involving children; extra-familial child sexual molestation; unsolicited obscene material sent to a child; and the use of misleading domain names, words, or digital images on the Internet. NCMEC processes and analyzes each CyberTipline report and makes the reports available to law enforcement for potential investigation and prosecution as appropriate. To make a report to the CyberTipline, visit www.cybertipline.com or call 1-800-843-5678.

Tips for Parents and Guardians

- Begin a dialogue with your kids about safer Internet use and supervise their online activities
- Consider rating, blocking, monitoring, and filtering applications for your home computer and kids' wireless devices
- Make Internet use a family activity
- Encourage your kids' critical-thinking skills
- Set reasonable rules for going online
- Encourage your kids to tell you or another trusted adult when they encounter problems online
- Make a report to NCMEC's CyberTipline at www.cybertipline.com or 1-800-843-5678 if your kids receive images of a sexual nature

Find More Help Online

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

- Discussion points for your family about online and real-world safety
- Informative statistics about kids' Internet use
- Safety tips for addressing risks to kids online and in the real world
- At-home activities for talking about safety during teachable moments

Visit www.NetSmartz411.org for answers to commonly asked questions about the Internet, computers, or the Web or to ask specific questions of experts

Help Us Promote a Safer Internet

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