Internet Safety

The Internet can be a wonderful resource for kids. They can use it to research school reports, communicate with teachers and other kids, and play interactive games. Kids who are old enough to punch in a few letters on the keyboard can literally access the world.

But that access can also pose hazards. For example, an 8-year-old might do an online search for "Lego." But with just one missed keystroke, the word "Legs" is entered instead, and the child may be directed to a slew of websites with a focus on legs — some of which may contain pornographic material.

That's why it's important to be aware of what your kids see and hear on the Internet, who they meet, and what they share about themselves online.

Just like any safety issue, it's wise to talk with your kids about your concerns, take advantage of resources to protect them, and keep a close eye on their activities.

Internet Safety Laws

A federal law, the Children's Online Privacy Protection Act (COPPA), was created to help protect kids online. It's designed to keep anyone from obtaining a child's personal information without a parent knowing about it and agreeing to it first.

COPPA requires websites to explain their privacy policies on the site and get parental consent before collecting or using a child's personal information, such as a name, address, phone number, or Social Security number. The law also prohibits a site from requiring a child to provide more personal information than necessary to play a game or participate in a contest.

But even with this law, your kids' best online protection is you. By talking to them about potential online dangers and monitoring their computer use, you'll help them surf the Internet safely.

Online Protection Tools

Online tools are available that will let you control your kids' access to adult material and help protect them from Internet predators. No option is going to guarantee that they'll be kept away from 100% of the risks on the Internet. So it's important to be aware of your kids' computer activities and educate them about online risks.

Many Internet service providers (ISPs) provide parent-control options to block certain material from coming into a computer. You can also get software that helps block access to certain sites based on a "bad site" list that your ISP creates. Filtering programs can block sites from coming in and restrict personal information from being sent online. Other programs can monitor and track online activity. Also, make sure your kids create a screen name to protect their real identity.

Getting Involved in Kids' Online Activities

Aside from these tools, it's wise to take an active role in protecting your kids from Internet predators and sexually explicit materials online. To do that:

- Become computer literate and learn how to block objectionable material.
- Keep the computer in a common area, not in individual bedrooms, where you can watch and monitor its use.
- Share an email account with your child so you can monitor messages.
- Bookmark kids' favorite sites for easy access.
- Spend time online together to teach your kids appropriate online behavior.
- Forbid your child from entering private chat rooms; block them with safety features provided by your Internet service provider or with special filtering software. Be aware that posting messages to chat rooms reveals a user's email address to others.
- Monitor your credit card and phone bills for unfamiliar account charges.
- Find out what, if any, online protection is offered by your child's school, after-school center, friends' homes, or anyplace where kids could use a computer without your supervision.
- Take your child seriously if he or she reports an uncomfortable online exchange.
- Forward copies of obscene or threatening messages you or your kids get to your Internet service provider.
- Call the National Center for Missing and Exploited Children at (800) 843-5678 if you're aware of the transmission, use, or viewing of child pornography online. Contact your local law enforcement agency or the FBI if your child has received child pornography via the Internet.

Many sites use "cookies," devices that track specific information about the user, such as name, email address, and shopping preferences. Cookies can be disabled. Ask your Internet service provider for more information.

Basic Rules

Set up some simple rules for your kids to follow while they're using the Internet, such as:

- Follow the rules you set, as well as those set by your Internet service provider.
- Never trade personal photographs in the mail or scanned photographs over the Internet.
- Never reveal personal information, such as address, phone number, or school name or location. Use only a screen name. Never agree to meet anyone from a chat room in person.
- Never respond to a threatening email or message.
- Always tell a parent about any communication or conversation that was scary.
- If your child has a new "friend," insist on being "introduced" online to that friend.

Chat Room Caution

Chat rooms are virtual online rooms where chat sessions take place. They're set up according to interest or subject, such as a favorite sport or TV show. Because people can communicate with each other alone or in a group, chat rooms are among the most popular destinations on the Web — especially for kids and teens.

But chat rooms can pose hazards for kids. Some kids have met "friends" in chat rooms who were

interested in exploiting them. No one knows how common chat-room predators are, but pedophiles (adults who are sexually interested in children) are known to frequent chat rooms.

These predators sometimes prod their online acquaintances to exchange personal information, such as addresses and phone numbers, thus putting the kids they are chatting with — and their families — at risk.

Pedophiles often pose as teenagers in chat rooms. Because many kids have been told by parents not to give out their home phone numbers, pedophiles may encourage kids to call them; with caller ID the offenders instantly have the kids' phone numbers.

Warning Signs

Warning signs of a child being targeted by an online predator include spending long hours online, especially at night, phone calls from people you don't know, or unsolicited gifts arriving in the mail. If your child suddenly turns off the computer when you walk into the room, ask why and monitor computer time more closely. Withdrawal from family life and reluctance to discuss online activities are other signs to watch for.

Contact your local law enforcement agency or the FBI if your child has received pornography via the Internet or has been the target of an online sex offender.

Taking an active role in your kids' Internet activities will help ensure that they benefit from the wealth of valuable information it offers without being exposed to any potential dangers.

Reviewed by: Steven Dowshen, MD
Date reviewed: June 2011