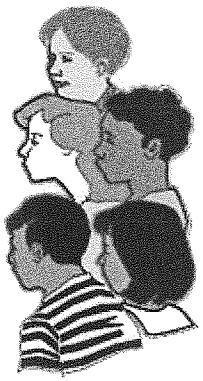
A Parent's Guide to Internet Safety

U.S. Department of Justice
Federal Bureau of Investigation - Publications

Dear Parent:



Our children are our Nation's most valuable asset. They represent the bright future of our country and hold our hopes for a better Nation. Our children are also the most vulnerable members of society. Protecting our children against the fear of crime and from becoming victims of crime must be a national priority.

Unfortunately the same advances in computer and telecommunication technology that allow our children to reach out to new sources of knowledge and cultural experiences are also leaving them vulnerable to exploitation and harm by computer-sex offenders.

I hope that this pamphlet helps you to begin to understand the complexities of on-line child exploitation. For further information, please contact your local FBI office or the National Center for Missing and Exploited Children at 1-800-843-5678.

Louis J. Freeh, Former Director
Federal Bureau of Investigation

Introduction

While on-line computer exploration opens a world of possibilities for children, expanding their horizons and exposing them to different cultures and ways of life, they can be exposed to dangers as they hit the road exploring the information highway. There are individuals who attempt to sexually exploit children through the use of on-line services and the Internet. Some of these individuals gradually seduce their targets through the use of attention, affection, kindness, and even gifts. These individuals are often willing to devote considerable amounts of time, money, and energy in this process. They listen to and empathize with the problems of children. They will be aware of the latest music, hobbies, and interests of children. These individuals attempt to gradually lower children's inhibitions by slowly introducing sexual context and content into their conversations.

There are other individuals, however, who immediately engage in sexually explicit conversation with children. Some offenders primarily collect and trade child-pornographic images, while others seek face-to-face meetings with children via on-line contacts. It is important for parents to understand that children can be indirectly victimized through conversation, i.e. "chat," as well as the transfer of sexually explicit information and material. Computer-sex offenders may also be evaluating children they come in contact with on-line for future face-to-face contact and direct victimization. Parents and children should remember that a computer-sex offender can be any age or

sex the person does not have to fit the caricature of a dirty, unkempt, older man wearing a raincoat to be someone who could harm a child.

Children, especially adolescents, are sometimes interested in and curious about sexuality and sexually explicit material. They may be moving away from the total control of parents and seeking to establish new relationships outside their family. Because they may be curious, children/adolescents sometimes use their on-line access to actively seek out such materials and individuals. Sex offenders targeting children will use and exploit these characteristics and needs. Some adolescent children may also be attracted to and lured by on-line offenders closer to their age who, although not technically child molesters, may be dangerous. Nevertheless, they have been seduced and manipulated by a clever offender and do not fully understand or recognize the potential danger of these contacts.

This guide was prepared from actual investigations involving child victims, as well as investigations where law enforcement officers posed as children. Further information on protecting your child on-line may be found in the National Center for Missing and Exploited Children's Child Safety on the Information Highway and Teen Safety on the Information Highway pamphlets.

What Are Signs That Your Child Might Be At Risk On-line?

Your child spends large amounts of time on-line, especially at night.

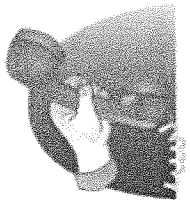
Most children that fall victim to computer-sex offenders spend large amounts of time on-line, particularly in chat rooms. They may go on-line after dinner and on the weekends. They may be latchkey kids whose parents have told them to stay at home after school. They go on-line to chat with friends, make new friends, pass time, and sometimes look for sexually explicit information. While much of the knowledge and experience gained may be valuable, parents should consider monitoring the amount of time spent on-line.

Children on-line are at the greatest risk during the evening hours. While offenders are on-line around the clock, most work during the day and spend their evenings on-line trying to locate and lure children or seeking pornography.

You find pornography on your child's computer.

Pornography is often used in the sexual victimization of children. Sex offenders often supply their potential victims with pornography as a means of opening sexual discussions and for seduction. Child pornography may be used to show the child victim that sex between children and adults is "normal." Parents should be conscious of the fact that a child may hide the pornographic files on diskettes from them. This may be especially true if the computer is used by other family members.

Your child receives phone calls from men you don't know or is making calls, sometimes long distance, to numbers you don't recognize.



While talking to a child victim on-line is a thrill for a computer-sex offender, it can be very cumbersome. Most want to talk to the children on the telephone. They often engage in "phone sex" with the children

and often seek to set up an actual meeting for real sex.

While a child may be hesitant to give out his/her home phone number, the computer-sex offenders will give out theirs. With Caller ID, they can readily find out the child's phone number. Some computer-sex offenders have even obtained toll-free 800 numbers, so that their potential victims can call them without their parents finding out. Others will tell the child to call collect. Both of these methods result in the computer-sex offender being able to find out the child's phone number.

Your child receives mail, gifts, or packages from someone you don't know.

As part of the seduction process, it is common for offenders to send letters, photographs, and all manner of gifts to their potential victims. Computer-sex offenders have even sent plane tickets in order for the child to travel across the country to meet them.

Your child turns the computer monitor off or quickly changes the screen on the monitor when you come into the room.

A child looking at pornographic images or having sexually explicit conversations does not want you to see it on the screen.

Your child becomes withdrawn from the family.

Computer-sex offenders will work very hard at driving a wedge between a child and their family or at exploiting their relationship. They will accentuate any minor problems at home that the child might have. Children may also become withdrawn after sexual victimization.

Your child is using an on-line account belonging to someone else.

Even if you don't subscribe to an on-line service or Internet service, your child may meet an offender while on-line at a friend's house or the library. Most computers come preloaded with on-line and/or Internet software. Computer-sex offenders will sometimes provide potential victims with a computer account for communications with them.

What Should You Do If You Suspect Your Child Is Communicating With A Sexual Predator On-line?

- Consider talking openly with your child about your suspicions. Tell them about the dangers of computer-sex offenders.
- Review what is on your child's computer. If you don't know how, ask a friend, coworker, relative, or other knowledgeable person. Pornography or any kind of sexual communication can be a warning sign.
- Use the Caller ID service to determine who is calling your child. Most telephone companies that offer Caller ID also offer a service that allows you to block your number from appearing on someone else's Caller ID. Telephone companies also offer an additional service feature that rejects incoming calls that you block. This rejection feature prevents computer-sex offenders or anyone else from calling your home anonymously.

- Devices can be purchased that show telephone numbers that have been dialed from your home phone. Additionally, the last number called from your home phone can be retrieved provided that the telephone is equipped with a redial feature. You will also need a telephone pager to complete this retrieval.
- This is done using a numeric-display pager and another phone that is on the same line as the first phone with the redial feature. Using the two phones and the pager, a call is placed from the second phone to the pager. When the paging terminal beeps for you to enter a telephone number, you press the redial button on the first (or suspect) phone. The last number called from that phone will then be displayed on the pager.
- Monitor your child's access to all types of live electronic communications (i.e., chat rooms, instant messages, Internet Relay Chat, etc.), and monitor your child's e-mail. Computer-sex offenders almost always meet potential victims via chat rooms. After meeting a child on-line, they will continue to communicate electronically often via e-mail.

Should any of the following situations arise in your household, via the Internet or on-line service, you should immediately contact your local or state law enforcement agency, the FBI, and the National Center for Missing and Exploited Children:

1. Your child or anyone in the household has received child pornography;
2. Your child has been sexually solicited by someone who knows that your child is under 18 years of age;
3. Your child has received sexually explicit images from someone that knows your child is under the age of 18.

If one of these scenarios occurs, keep the computer turned off in order to preserve any evidence for future law enforcement use. Unless directed to do so by the law enforcement agency, you should not attempt to copy any of the images and/or text found on the computer.

What Can You Do To Minimize The Chances Of An On-line Exploiter Victimizing Your Child?

- Communicate, and talk to your child about sexual victimization and potential on-line danger.
- Spend time with your children on-line. Have them teach you about their favorite on-line destinations.
- Keep the computer in a common room in the house, not in your child's bedroom. It is much more difficult for a computer-sex offender to communicate with a child when the computer screen is visible to a parent or another member of the household.
- Utilize parental controls provided by your service provider and/or blocking software. While electronic chat can be a great place for children to make new friends and discuss various topics of interest, it is also prowled by computer-sex offenders. Use of chat rooms, in particular, should be heavily monitored. While parents should utilize these mechanisms, they should not totally rely on them.
- Always maintain access to your child's on-line account and randomly check his/her e-mail. Be aware that your child could be contacted through the U.S. Mail. Be up front with your child about your access and reasons why.

- Teach your child the responsible use of the resources on-line. There is much more to the on-line experience than chat rooms.
- Find out what computer safeguards are utilized by your child's school, the public library, and at the homes of your child's friends. These are all places, outside your normal supervision, where your child could encounter an on-line predator.
- Understand, even if your child was a willing participant in any form of sexual exploitation, that he/she is not at fault and is the victim. The offender always bears the complete responsibility for his or her actions.
- Instruct your children:

    - to never arrange a face-to-face meeting with someone they met on- line;
    - to never upload (post) pictures of themselves onto the Internet or on-line service to people they do not personally know;
    - to never give out identifying information such as their name, home address, school name, or telephone number;
    - to never download pictures from an unknown source, as there is a good chance there could be sexually explicit images;
    - to never respond to messages or bulletin board postings that are suggestive, obscene, belligerent, or harassing;
    - that whatever they are told on-line may or may not be true.

Frequently Asked Questions:

My child has received an e-mail advertising for a pornographic website, what should I do?

Generally, advertising for an adult, pornographic website that is sent to an e-mail address does not violate federal law or the current laws of most states. In some states it may be a violation of law if the sender knows the recipient is under the age of 18. Such advertising can be reported to your service provider and, if known, the service provider of the originator. It can also be reported to your state and federal legislators, so they can be made aware of the extent of the problem.

Is any service safer than the others?

Sex offenders have contacted children via most of the major on-line services and the Internet. The most important factors in keeping your child safe on-line are the utilization of appropriate blocking software and/or parental controls, along with open, honest discussions with your child, monitoring his/her on-line activity, and following the tips in this pamphlet.

Should I just forbid my child from going on-line?

There are dangers in every part of our society. By educating your children to these dangers and taking appropriate steps to protect them, they can benefit from the wealth of information now available on-line.

Helpful Definitions:

Internet - An immense, global network that connects computers via telephone lines and/or fiber networks to storehouses of electronic information. With only a computer, a modem, a telephone line and a service provider, people from all over the world can communicate and share information with little more than a few keystrokes.

Bulletin Board Systems (BBSs) - Electronic networks of computers that are connected by a central computer setup and operated by a system administrator or operator and are distinguishable from the Internet by their "dial-up" accessibility. BBS users link their individual computers to the central BBS computer by a modem which allows them to post messages, read messages left by others, trade information, or hold direct conversations. Access to a BBS can, and often is, privileged and limited to those users who have access privileges granted by the systems operator.

Commercial On-line Service (COS) - Examples of COSs are America Online, Prodigy, CompuServe and Microsoft Network, which provide access to their service for a fee. COSs generally offer limited access to the Internet as part of their total service package.

Internet Service Provider (ISP) - Examples of ISPs are Erols, Concentric and Netcom. These services offer direct, full access to the Internet at a flat, monthly rate and often provide electronic-mail service for their customers. ISPs often provide space on their servers for their customers to maintain World Wide Web (WWW) sites. Not all ISPs are commercial enterprises. Educational, governmental and nonprofit organizations also provide Internet access to their members.

Public Chat Rooms - Created, maintained, listed and monitored by the COS and other public domain systems such as Internet Relay Chat. A number of customers can be in the public chat rooms at any given time, which are monitored for illegal activity and even appropriate language by systems operators (SYSOP). Some public chat rooms are monitored more frequently than others, depending on the COS and the type of chat room. Violators can be reported to the administrators of the system (at America On-line they are referred to as terms of service [TOS]) which can revoke user privileges. The public chat rooms usually cover a broad range of topics such as entertainment, sports, game rooms, children only, etc.

Electronic Mail (E-Mail) - A function of BBSs, COSs and ISPs which provides for the transmission of messages and files between computers over a communications network similar to mailing a letter via the postal service. E-mail is stored on a server, where it will remain until the addressee retrieves it. Anonymity can be maintained by the sender by predetermining what the receiver will see as the "from" address. Another way to conceal one's identity is to use an "anonymous remailer," which is a service that allows the user to send an e-mail message repackaged under the remailer's own header, stripping off the originator's name completely.

Chat - Real-time text conversation between users in a chat room with no expectation of privacy. All chat conversation is accessible by all individuals in the chat room while the conversation is taking place.

Instant Messages - Private, real-time text conversation between two users in a chat room.

Internet Relay Chat (IRC) - Real-time text conversation similar to public and/or private chat rooms on COS.

Usenet (Newsgroups) - Like a giant, cork bulletin board where users post messages and information. Each posting is like an open letter and is capable of having attachments, such as graphic image files (GIFs). Anyone accessing the newsgroup can read the postings, take copies of posted items, or post responses. Each newsgroup can hold thousands of postings. Currently, there are over 29,000 public newsgroups and that number is growing daily. Newsgroups are both public and/or private. There is no listing of private newsgroups. A user of private newsgroups has to be invited into the newsgroup and be provided with the newsgroup's address.

Federal Bureau of Investigation
Cyber Division, Innocent Images National Initiative
11700 Beltsville Drive
Calverton, MD 20705

Contact your local FBI office for further information.