

## **WHO ARE THE EXPERTS?**

Computer experts -- where can you find one? These days most of us do not have to look further than our own home. The true computer experts are somewhere between the third and twelfth grade, and they can be found in almost every home in America. Children are taught how to use computers as early as preschool. Unlike adults, they are not afraid of or intimidated by computers. Most children learn how to use a computer to gain access to the Internet in school. They also learn how to use search engines that allow them to locate information on any topic. This is the beginning of the problem for most families. A computer is brought into the home, usually to assist the children with their homework. The expert -- your child -- is consulted to set up the computer and online service. The child then has control of the passwords that allow access to chat rooms, newsgroups and Web sites on the Internet. However the parents' controls are not set to allow the same total access. Because the parents do not see the entire Internet they have a false sense of security about what their children are doing on the Internet. All too frequently, police officers follow up on a complaint of pornography or threats being transmitted via the Internet, only to find that the parents know almost nothing about how the computer works. When the police ask questions concerning the computer and online service, the parents summon their child to explain how the computer was set up.

After consent by the parents, the computer is searched and the offending material is located, often to the shock of the parents and embarrassment of the child. After resetting the controls and explaining the operation of the online system, the parents now have control of their own computer. When leaving the home the police officers may leave behind some kind of pamphlet, such as the one created by the National Center for Missing and Exploited Children. This pamphlet details basic online safety rules for parents and children. A complete copy of the pamphlet used by the Naperville Police Department, with permission from the NCEMC, is included in this chapter. Several of its more important safeguards are listed here:

- PUT THE COMPUTER IN A PUBLIC ROOM IN THE HOME
- NEVER GIVE OUT PERSONAL INFORMATION ONLINE
- USE SOME KIND OF PARENTAL CONTROL
- NEVER AGREE TO MEET IN PERSON SOMEONE YOU MET ONLINE WITHOUT YOUR PARENTS
- NEVER SEND ANYONE A PICTURE OF YOURSELF WITHOUT YOUR PARENTS' PERMISSION

The most important safeguard is the placement of the computer. With today's hectic lifestyles, many households have two working parents, and children often cannot be supervised all the time. By placing the computer in a public room, such as the kitchen or family room, Mom and Dad can monitor their child's online activities. Placing the computer in the child's bedroom is asking for trouble. It is comparable to placing a television set with access to all channels, including adult programming, in their child's bedroom. Why allow a computer, with access to adult sites and chat rooms, to be placed out of your sight in your child's room?

## **UNDERSTANDING THE "STRANGER DANGER" OF THE INTERNET**

Next, you want your child to understand that a stranger is a stranger. Conversing online does not change that fact. Your child knows not to speak with a stranger on the playground, so why should the rules be different for online conversations? They would not tell a stranger where they live or go to school in person, so they should behave the same way online. They should understand that strangers can find out where they live with only a little personal information.

There are online services that allow anyone to receive the name and address for any listed telephone number in the United States and Canada. After giving the address it can "link" (connect) to a program that supplies a map of the neighborhood where the residence is located. These maps can include statewide displays and then go down to the single street on which the residence is located. This could supply the pedophile with exact directions to your child.

Parental controls can greatly increase the safety of your children online. There are several good programs designed for this purpose. One program, Cyber Sentinel, incorporates several helpful features. The program is "content-driven," not "address-driven" like most parental blocking programs. Simply put, the program actually "pre-reads" the site your child is attempting to load. If the site contains content that has been prohibited by the parents, it does not allow access to the site. Instead it takes a "screen capture" (a picture) of the site and sends it to a file the parent's control. Parents can sign on to a password-protected area of the computer and obtain an audit, in pictures, of sites their child has attempted to visit. Since the program is content-driven it works for Web sites regardless of how many times the address changes. It also functions in chat rooms, instant messages/whisper boxes, E-mail and word processing.

This program allows parents to customize prohibited content by adding personal information to the prohibited list. Items such as the child's last name, address, telephone number and where they go to school are just a few examples. Pedophiles online can be very persuasive; they can gain your child's trust and trick them into giving out personal information. By prohibiting this information, it is far less likely this information can be given. When the pedophile requests personal information, the computer catches the request and does not allow the child to see it. The pedophile's request can be printed out and given to your local police department for investigation. Since the entire screen is captured, the parents are able to supply the police with information such as screen name and service provider used. That type of information will assist the police in identifying the pedophile. Credit card numbers can also be prohibited to prevent children from misusing them online.

Children need to understand that they should never meet someone in person that they met online without their parents being present. If an online relationship reaches the point where someone wants to meet you in person, your parents need to be told about the meeting. If your parents agree to a meeting it should be at a public place, arranged and attended by the parents. This way everyone can feel safe —if not, they can just walk away. If the other person is only interested in making a new friend, they won't be upset or offended if a chaperone is present.

This method also works for adults to meet people in person that they have chatted with online. Take a girlfriend, boyfriend or coworker with you if you're going to meet someone. Again, anyone who is interested in making a friend will not mind a second person being present. In fact, they may appreciate your common-sense approach. Finally, children should not send pictures of themselves to anyone online without their parents' permission. You never know what someone else will do with a picture of you. With very little knowledge and a basic graphics program, any image can be "morphed" or altered. These programs are so accurate that it is sometimes impossible to tell the image has been altered. It is not unusual for an angry ex-husband to morph the face of his wife onto a nude image of an adult film personality and then post it on the Internet or mail it to neighbors. The same thing can happen to any image your child sends out over the Internet.

### **CHAT ROOMS**

The most popular, and dangerous, areas for children on the Internet are chat rooms. Chat rooms allow users of the Internet to converse with other users in real time, no matter where in the world they are located. A local telephone call to your Internet Service Provider (ISP) allows you to converse anywhere in the world for the cost of local phone call. With the right program, users can type their messages on a keyboard; see them displayed on their monitor, then see responses from one or one hundred people throughout the world. Some users have taken to installing inexpensive video cameras on their computers, allowing them to be seen online in real time.

Some of the most frequently used chat rooms exist on IRC (Internet Relay Chat) or within online services such as America Online. These chat rooms are listed by topic. Your child selects a "screen name," a name they wanted to be known by while chatting. The child can fill out a "profile", which can contain personal information. The profile can then be accessed by anyone using that online system. No Internet Service Provider conducts a verification of the profile information. The name can be a mixture of letters and numbers. The best analogy for a screen name is a "handle" on the CB radio. After selecting a screen name, the child then selects what room they want to chat in. After selecting a room, the child's screen name appears within that room. Once the child enters a room, the pedophile can check the profile for personal information. The pedophile can learn the age, sex and geographical location of the child. The pedophile can also learn what school the child attends.

One technique used by pedophiles is to enter a room and "lurk" (observing conversations, but not participating.). This way, the pedophile can observe the behavior of the child he wants to approach. The pedophile learns the likes and dislikes of the child, or if the child recently had a fight with their parents and felt the punishment was unjust. Also, the pedophile can observe if anyone else wants to talk to the child, or if people in the room rebuked the child when he or she tried to start a conversation. Lurking is not a new behavior for pedophiles -- they've been doing it in public parks for decades.

### **THE EVOLUTION OF PEDOPHILES IN THE COMPUTER AGE**

In the past, a pedophile wanting to meet children would have to go to where they could be found, such as a playground or schoolyard. This involved certain risks, such as being spotted by teachers, school workers or parents. In the 90's, pedophiles now hang around in "virtual parks."

The pedophile can now slip past the parents and right into the child's bedroom. They don't have the same fear of being "spotted" as they would in a park or schoolyard. They can speak to children from the privacy of their own home, without the fear of parents, teachers or watchful neighbors alerting the police. If the fears being discovered while talking to a child, they just break off contact and disappear into the vast anonymity of the Internet.

After listening to the conversation (or attempts at conversation,) the pedophile will begin a conversation. Since that everyone in the chat room can see what is being said, the pedophile will start off an innocent conversation. However, after a brief period of time, a private forum will be used for the conversation. Most chat programs allow for a private method of chatting where only the two people involved in the conversation can see what is being said. At this point the pedophile will attempt to determine just how safe it is to speak with the child. Questions such as:

- ARE YOU HOME ALONE?
- WHO USES THE COMPUTER?
- WHERE IS THE COMPUTER LOCATED?

These questions will begin the "courting process." Obviously, the pedophile will terminate the conversation if these questions receive answers that say:

- THE PARENTS OR GUARDIANS ARE HOME
- THE COMPUTER IS USED BY EVERYONE IN THE HOME
- THE COMPUTER IS KEPT IN A PUBLIC AREA

The pedophile will feel "safe" and take the conversation to the next level if the answers say:

- THE CHILD IS HOME ALONE
- THE COMPUTER IS KEPT IN THE CHILD'S ROOM
- THE CHILD IS THE ONLY ONE IN THE FAMILY THAT USES THE COMPUTER

Through a series of questions the pedophile will attempt to gain the child's trust and make it seem as though they can only trust each other.

The pedophile may first send jokes that are "off-color" or suggestive to gauge the child's reaction. From this, a conversation about sexual experience will begin, with the goal of lowering the child's inhibitions. As the conversation continues, the pedophile will relate different sexual techniques or positions and may ask the child to attempt masturbation. To show the child that it is a normal practice and that "everyone does it," the pedophile may send the child graphic images showing other people involved in the activity. The photographs may be of adults, or they may be of children either at or near the age of the child the pedophile is courting. After the photographs have been sent, the pedophile may try to increase the amount of trust between the child and the pedophile by asking the child to delete the pictures. The pedophile may tell the child that the pedophile would be in a

lot of trouble if anyone else saw the pictures, and that they are trusting each other to keep the conversations private. This will be followed by a promise that the pedophile will never tell anyone about his or her conversations or friendship and he hopes your child will do the same.

As the conversations continue and the trust level elevates, the pedophile will attempt a meeting. Depending on the preference of the pedophile, he will have the child travel by supplying a bus or airplane ticket, or the pedophile will travel, sometimes even driving non-stop for days to arrive at an agreed-upon meeting location.

Understanding that parents can not always monitor their child when online parental blocking software described in this workbook is a must. It can be set to catch the normal pedophile's approach and save a record of the chat for the parents. It will also prevent an ongoing dialogue between the pedophile and your child, or inappropriate conduct between your child and other children.

Some of the more common questions we receive are:

- HOW DID MY CHILD GET THESE PICTURES?
- HOW DID THEY FIND PORNOGRAPHIC WEB SITES?
- CAN I SEARCH MY COMPUTER TO FIND WHERE MY CHILD HAS BEEN?
- IS THERE A WAY TO PREVENT MY CHILD FROM TALKING TO A PEDOPHILE ONLINE?

As discussed earlier, most children are taught how to use search engines at school. Imagine you are a twelve or thirteen year-old boy and you want to see photographs of nude girls. You do not know the address for those pictures on the Internet, but you can find them with a search engine.

Once the search engine is brought up, you type in the subject you are looking for, such as "nude girls." The search engine then searches the Internet for sites featuring nude girls. With one search engine called HOTBOT, the search found over 98,000 sites, each containing from one to one thousand pictures, available for free. All search engines will produce similar results; HOTBOT was only used as an example.

Once a site is located, your child can view any of the free photographs, which can be saved on your computer. Most graphic images are sent to the child's computer via this method, or directly via e-mail.

To check where your child has been, look for the "cache" or "history" folder in your browser. This will allow you to see images and sites your child has seen.

### **CONCLUSION**

If you allow your child onto the Internet, there is no sure-fire way to prevent them from encountering strangers. You can use software to block downloads, chat and e-mail, but none of these programs foolproof. Even online games for children have chat software running under the games so players can talk to each other. This can lead to an invitation to speak in other rooms, possibly even on the telephone or in public. The only foolproof way to eliminate the threat is to remove the modem so that your child cannot reach the

Internet. But this is drastic and unrealistic. If your child cannot reach the Internet, they cannot do the research they need for schoolwork. Because they have to be online to keep up, then parents must supervise their behavior. This can be done in person, or with software, or both. Software that works based on Web addresses is much less effective than software that works on content.

In the end this is like anything else your child is subjected to, whether it's peer pressure, drugs or alcohol. The best way to deal with this subject is to talk to your children. Tell them that you understand what can happen, and that sometimes items sent to their computer are not their fault. However, they need to understand that whenever anything improper is sent, or anyone asks them inappropriate questions, they must notify their parents or guardians as soon as possible. **THE BEST FORM OF PARENTAL CONTROL IS AN OPEN DIALOGUE BETWEEN YOU AND YOUR CHILD.**