NDOJ

INTERNET

SAFETY

what you don't know
can hurt your
child

COMPUTERS and the

INTERNET impact
how we live our lives each and every day.

What seemed impossible yesterday becomes
a necessity today.

But along with these positive changes

come new **RESPONSIBILITIES**

and potential **DANGERS**

Your front door may be locked, but if
your computer isn't used safely, it
offers an open window into your home.

Together we can help our
children learn by taking
advantage of new technology
while reducing risks
to their safety.

1 in 5 youths
between the
ages of 10 and 17
has received
unwanted sexual
solicitations
online[1]

Millions of children under the age of 18 are using the Internet every day and the number of children who are spending time online will continue to grow. This relatively new communication tool presents a variety of risks to children.

They include:

SOLICITATION BY CHILD PREDATORS

- 19% of youths who used the Internet regularly were targets of unwanted sexual solicitation in the last year[2]
- 89% of sexual solicitations were made in either chat rooms or Instant Messages[3]

UNWANTED EXPOSURE TO SEXUAL MATERIAL

- 1 in 4 youths has been exposed to sexually explicit pictures online without seeking or expecting them[1]

THREATS OR HARASSMENT ONLINE

- 1 in 17 youths has been threatened or harassed online[1]
- 1 in 33 youths has received an aggressive solicitation to meet somewhere[1]
- Only about half of the children who were threatened or harassed online reported the incident to their parents[1]

[1] David Finkelhor, Kimberly J. Mitchell and Janis Wolak. Online Victimization: A Report on the Nation's Youth. Alexandria, Virginia: National Center for Missing & Exploited Children, 2000.
[2] Kimberly J. Mitchell, David Finkelhor and Janis Wolak. Risk Factors for and Impact of Online Sexual Solicitation of Youth. Journal of the American Medical Association:June 20, 2001
[3] Pew Study reported in JAMA, 2001

HOW INTERNET PREDATORS TARGET CHILDREN

The Internet makes it easy for predators to find potential victims and communicate with them. Ultimately, they want to lure children into a face-to-face meeting or get enough information to stalk the child by searching online for clues to determine a home address. That's why it is very important for you to understand how predators target children

the Internet
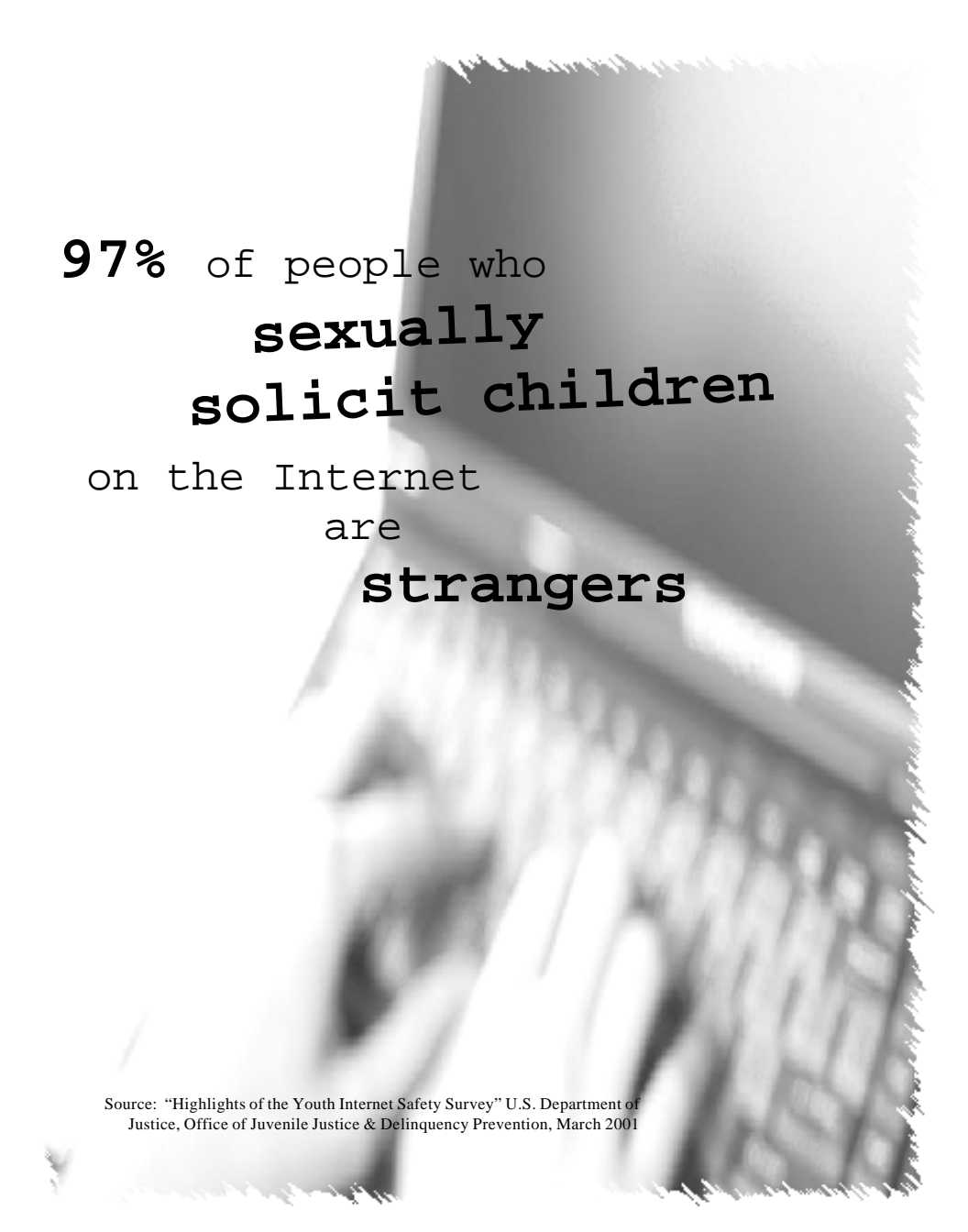makes it

EASY

for predators
to locate

POTENTIAL VICTIMS

CHILD PREDATOR CHARACTERISTICS

While most offenders are male, law enforcement experts say that a child predator can be anyone: male or female, young or old. They often hold respectable jobs and positions in their community. People who want to harm or exploit children tend to relate more easily to children than adults and they may also seek employment or volunteer at a children's organization.

CHILD VICTIM CHARACTERISTICS

Law enforcement officials also advise that ANY child can be vulnerable to a predator's enticement, including those who may be performing well at school and socializing with a "good" crowd of friends. You may believe that your child can't fall victim to a child predator. However, experts stress that such thinking can lead to a false sense of security about your child's safety.

97% of people who
sexually
solicit children
on the Internet
are
strangers

Most children who agree to meet face-to-face
with an adult do so willingly
they are not tricked or coerced

SEARCHING THE CHAT ROOMS

The Internet, with email and chat rooms, offers seemingly complete anonymity. For some teens and preteens, the apparent privacy of a chat room is comforting. They feel safe in front of a computer. But adults who are seeking children use the veil of anonymity to observe, approach and then groom their victims. That process usually ends with an attempt to lure a child to a meeting outside of the home.

PREDATORS CAN BE EXTREMELY CONVINCING

THEY ALSO RELY ON THE INEXPERIENCE OF THEIR POTENTIAL

VICTIMS AND THEY KNOW WHAT TO SAY AND DO TO GAIN

THEIR TRUST. A RECENT STUDY FOUND THAT MOST

CHILDREN WHO AGREE TO MEET FACE-TO-FACE WITH AN

ADULT DO SO WILLINGLY. THEY ARE NOT TRICKED

OR COOERCED.[4]

[4] David Finkelhor, Kimberly J. Mitchell and Janis Wolak. "Internet-Initiated Sex Crimes Against Minors: Implications for Prevention Based on Findings from a National Study" 35 Journal of Adolescent Health 11 (2004)

SEARCHES FREQUENTLY BEGINS IN A CHAT ROOM

The search for a potential victim frequently begins in a chat room.
A **CHAT ROOM** is a place online where people can go to "talk" with
each other by typing messages. These messages are usually displayed
almost instantly. Those in the chat room can view all of the conversations
taking place at once on their computer screen. Chat rooms may be di-
vided into categories. For example, an adult looking for a child victim in
Nevada may visit the **"Nevada"** chat room for teenagers.

A predator pays close attention to the conversations taking place in the
chat room and to the participants' screen names or user names.
A **SCREEN NAME** is the name a participant uses to represent himself
or herself online. A screen name of **"kaitlyn12country"** for
example, might indicate that the child is a 12-year-old female named
Kaitlyn who is interested in country music. Knowing this information, an
adult who is seeking to exploit or harm a child may then assume an iden-
tity that would be likely to attract the attention of that child. If the predator
assume the screen name **"dixiechicksrule"** for instance, the girl might
believe the person she is chatting with is a fan of the country music group
the Dixie Chicks.

Predators can use screen names to track down a child

FINDING SIMILAR INTERESTS

Even if a predator does not gather revealing or useful information from a child's screen name, he or she can still use the screen name to determine whether the child has completed an online profile. An **ONLINE PROFILE** may contain personal information such as a child's email address, interests and hobbies. Once a profile has been located, the person who has obtained it can easily send email or instant messages directly to the child.

EMAIL is a method of sending messages electronically from one computer to another. **INSTANT MESSENGING** is a service that alerts users when friends are online and allows them to communicate with each other in real time through private online chat areas. An adult who is seeking children can use the interests and hobbies located on the child's online profile to convince the child that he or she has found someone who has similar interests.

KEEPING THE RELATIONSHIP SECRET

After establishing a shared interest, a predator will work to build trust and convince the child that the predator is a better friend to the child than other friends or even family members.   The predator will also ask the child to keep the relationship secret. Later this secrecy may even be used as a weapon against the child. An adult who wants to exploit a child may threaten to expose the relationship to the child's parents or even threaten to harm the child or his or her family if the child tries to end the relationship.

SETTING UP THE MEETING OVER THE PHONE

At some point, the predator will usually engage in a phone conversation with the child victim. The ultimate goal is to arrange for a face-to-face meeting with the child.

> IM me @ LV_soccer100

With time and research

someone who is stalking

YOUR CHILD

may be able to find

his way right to

YOUR DOOR

CYBERSTALKING

GATHERING PERSONAL INFORMATION

In addition to gathering personal information about a child through an online profile, a chat room discussion or the child's screen name, a predator might also use an online discussion group. **DISCUSSION GROUPS** are like a public electronic bulletin board, where participants cam read and add (or "post") comments about a specific topic. Using an email address obtained from a child's online profile, someone who is seeking to exploit or harm a child can join a group and look for items the child has posted that contain more information. For instance, if a child has posted an item for sale, they might have provided a telephone number where buyers can call for more details. From there the predator can narrow the search.

FROM AREA CODE TO HOME ADDRESS

A predator can use the telephone area code and online resources to determine the state where the child resides. They may be able to use the telephone numbers to determine the last name of the family and even its address. With time and research, someone who is stalking your child may be able to find his way right to your front door.

The Federal Bureau of Investigation has compiled a list of warning signs that can indicate when a child might be at risk online. These warning signs can be found in the FBI's Parent's Child to Internet Safety:

TIME SPENT ONLINE

YOUR CHILD SPENDS LARGE AMOUNTS OF TIME ONLINE, ESPECIALLY AT NIGHT.
Most children who fall victim to child predators spend large amounts of time online, particularly in chat rooms. Child predators can be online at any time, but most work during the day and spend their evenings online trying to locate and lure children.

PORNOGRAPHY

YOU FIND PORNOGRAPHY ON YOUR CHILD'S COMPUTER.
Pornography is often used in the sexual victimization of children. Adults who are seeking to exploit children often supply their potential victims with pornography as a means of opening sexual discussions and for seduction. Child pornography may be used in an attempt to show the child victim that sex between children and adults is "normal." Keep in mind that a child might hide pornographic material by storing it on a disk, especially if other family members use the same computer.

Adults who are seeking
to exploit children
often supply their potential victims
with pornography
as a means of
opening sexual discussions
and for seduction

> do u wanna c what I look like?

PHONE USE

**YOUR CHILD RECEIVES PHONE CALLS FROM SOMEONE
YOU DON'T KNOW OR IS MAKING CALLS,
SOMETIMES LONG DISTANCE, TO NUMBERS
YOU DON'T RECOGNIZE.**
Predators enjoy exchanging messages with
children via computer. However, in most cases,
they also want to talk with them on the telephone
and they often engage in "phone sex" with the children. At some
point, they will usually attempt to set up a face-to-face meeting
for real sex.

Predators can also use these telephone calls to find out more
about the children they are pursuing. If a child is hesitant to
give a phone number, predators can use caller ID to determine
the phone number of a child who is calling. Some even obtain
toll-free numbers so their potential victims can call without their parents finding out.
Sometimes a child will be instructed to call collect. In each of these instances an adult
who is seeking to exploit children can get a child's phone number and such a predator
may be able to use the telephone number to determine the child's full name and home
address

UNSOLICITED MAIL AND GIFTS

YOUR CHILD RECEIVES MAIL, GIFTS OR PACKAGES FROM SOMEONE YOU DON'T KNOW.
As part of the grooming process, it is common for predators to send letters, photographs
and gifts to their potential victims. Some have even sent airline tickets so the child can
travel across the country to meet them.

When a child turns the computer monitor off or changes the screen on the monitor they are attempting to

CONCEAL SOMETHING

CONCEALING COMPUTER CONTENT

YOUR CHILD HIDES WHAT THEY ARE DOING ON THE COMPUTER.
When a child turns the computer monitor off or quickly changes the screen on the monitor, they are attempting to conceal something. A child looking at pornographic images or having sexually explicit conversations does not want you to see it on the screen.

BEHAVIOR CHANGE

YOUR CHILD BECOMES WITHDRAWN FROM THE FAMILY.
Adults who are seeking to exploit children work hard to drive a wedge between a child and his or her family. Any problem that a child has at home can be manipulated to make that child feel isolated from their loved ones. Children under the influence of a predator may pull away from their families. They may also become withdrawn after they have been victimized sexually

USING A DIFFERENT ONLINE ACCOUNT

YOUR CHILD IS USING ANOTHER EMAIL ACCOUNT.
Even if your child already has an email account, a child predator might set up another account so they can have more privacy when they communicate. Some online entities offer free email service, so email accounts can be created quickly and without cost. If your child is using an account other than the one you may have authorized, he or she may be communicating with someone who wants to keep the relationship secret. Keep in mind that your child could still meet and exchange messages with an adult while online at a friend's house, the library or at school.

CONTROL ACCESS TO CHAT ROOMS

Adults who are seeking to exploit children spend countless hours in chat rooms. Many experts believe that chat rooms are not safe for children, particularly young children. If you decide to allow your children to enter chat rooms, make sure your decision is based on their age and maturity. Children who are allowed into chat rooms need additional supervision.

CONTROL INSTANT MESSAGING

Like email and chat rooms, instant messaging (or "IMing") can be used to communicate secretly. Children often use abbreviations and code (such as "POS" which means "parent over shoulder" to change the course of the conversation when parents are watching and to keep parents from understanding online conversations.

KEEP SCREEN NAMES ANONYMOUS

Predators can use screen names to track down a child. Parents should make sure their child's screen name does not include personal information such as name, age, home address or school name.

AVOID ONLINE PROFILES

Many websites offer users the opportunity to set up an online profile where they can provide information about themselves. However, this information can be accessed and used by predators. One way to protect your child's privacy is for him or her to avoid these online profiles. Usually the online information is requested for advertising purposes and your child is not required to complete a profile in order to participate in online activities.
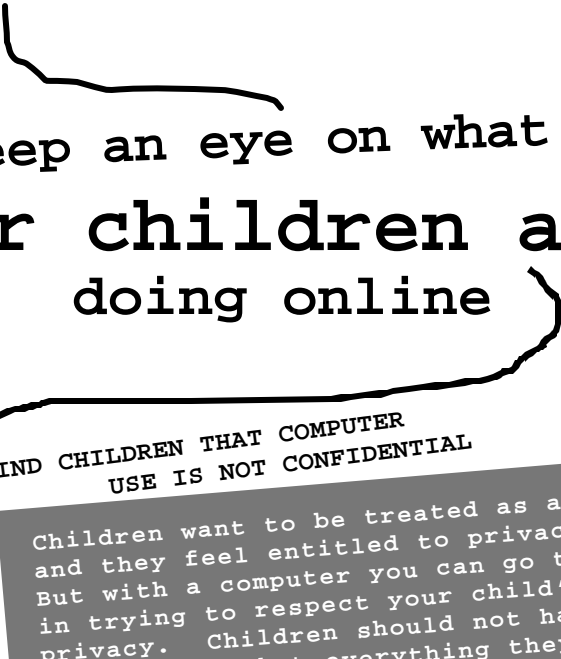
TAKE CARE WITH PHOTOGRAPHS

Computers make it easy to send and share photographs, but it should be done carefully. Children should not send photos to anyone, including other children, without parental approval. You should also avoid posting photographs of children on sites that might be accessible to predators, including so-called modeling sites.

ACCESS YOUR CHILD'S EMAIL

Experts recommend that parents share an email account with their child or maintain access to their child's email account and check it frequently. You might feel this is too intrusive, but it's not. A computer is different from a diary or a journal. A journal contains private thoughts that are not communicated to others. However, emails, chatting and instant messaging on a computer are an open window to your child's life, carrying information to and from your home.

PLACE YOUR COMPUTER IN A COMMON AREA

You should place your computer in a central room of the house, in order to monitor what your child is doing online. The computer screen should face out, into the room, so it's easy for you to see. Develop a list of family rules for using the Internet (see sample Family Rules) and post it next to the computer.

keep an eye on what your children are doing online

REMIND CHILDREN THAT COMPUTER USE IS NOT CONFIDENTIAL

Children want to be treated as adults and they feel entitled to privacy. But with a computer you can go too far in trying to respect your child's privacy. Children should not have the expectation that everything they do on a computer will be considered personal and confidential.

A STUDY BY THE NATIONAL CENTER FOR MISSING & EXPLOITED CHILDREN FOUND THAT 25 % OF YOUTH HAD EXPERIENCED UNWANTED EXPOSURE TO SEXUAL PICTURES ON THE INTERNET. IN FACT CHILDREN MIGHT ACCIDENTALLY COME ACROSS A WEBSITE THEY WEREN'T LOOKING FOR, EITHER BY MISSPELLING A WORD, TYPING IN THE WRONG DOMAIN NAME OR BY USING SEARCH TERMS. UNSOLICITED EMAIL (COMMONLY KNOWN AS "SPAM") CAN ALSO EXPOSE CHILDREN TO SEXUALLY ORIENTED MATERIAL.

To keep your child from accessing or being exposed to websites that contain inappropriate sexual material, it is important to have an understanding of how the Internet works. Let's start at the source of the Internet, the data that streams in and out of your home. Your computer connects to the online world through your Internet Service Provider (ISP).

Your ISP may be a company like America Online (AOL), Microsoft Network (MSN) or EarthLink. Many telephone companies and cable television companies are also ISPs. Regardless of which company connects your computer to the Internet, your ISP can play an important role in keeping your family safe online.

searching the words

"toy" or
        "pet"

can bring up
    sexual material

CONTACT YOUR ISP FOR HELP

The company that provides your Internet service can help you control what your child can and cannot access on the Internet. However, according to some ISPs, parents rarely take full advantage of these services. **Parents are strongly encouraged to contact their ISP to learn about the parental control features it offers.** Increasingly, ISPs are offering controls for free or at a small charge. In either case, the company has a technical support staff to help you. If you want to learn more about your company's features or how to set up the parental controls yourself, go to the company's website.

USE YOUR COMPUTER'S PARENTAL CONTROLS

In addition to the parental controls available through your ISP, you can use the computer itself to help make the Internet a safer place for your children. For instance, you can set up the computer so a child only has access to certain approved websites.

This process may seem daunting, but the computer can assist you in setting up parental controls. Most computers contain some form of a "Help" menu. You should access it and type "Parental Control." The computer will present a list of topic information based on those words. Clicking on a topic will bring more information. One of the first things your computer will do is instruct you to set up the individual logins for each family member.

> Parents can also check a record of the websites that have been visited. These are often found under "History." The websites offer clues about your child's online activities.
>
> For instance, if your child has a secret email account, the Internet History may indicated visits to the site that hosts the email account.
>
> You can set up the computer's parental controls to prevent the Internet History from being altered or deleted by your child.

ASSISTANCE IS AVAILABLE

If you aren't able to set up parental controls on your computer, here are some other options:

- **CONTACT TECHNICAL SUPPORT**

    Call the computer or software company's technical support number, or send the company an email. Software means the programs you use to access the Internet like Microsoft Internet Explorer or Netscape.

- **ARRANGE FOR A HOUSE CALL**

    Contact a local computer technical support company that makes house calls. For a fee, a technician can come directly to your home, set up the parental controls for you and show you how to use them.

- **CONTACT FAMILY AND FRIENDS**

    Many of us have a family member or a friend who is more computer-savvy than we are. If you are having difficulty setting up parental controls, ask that person to assist. They may be willing to help.
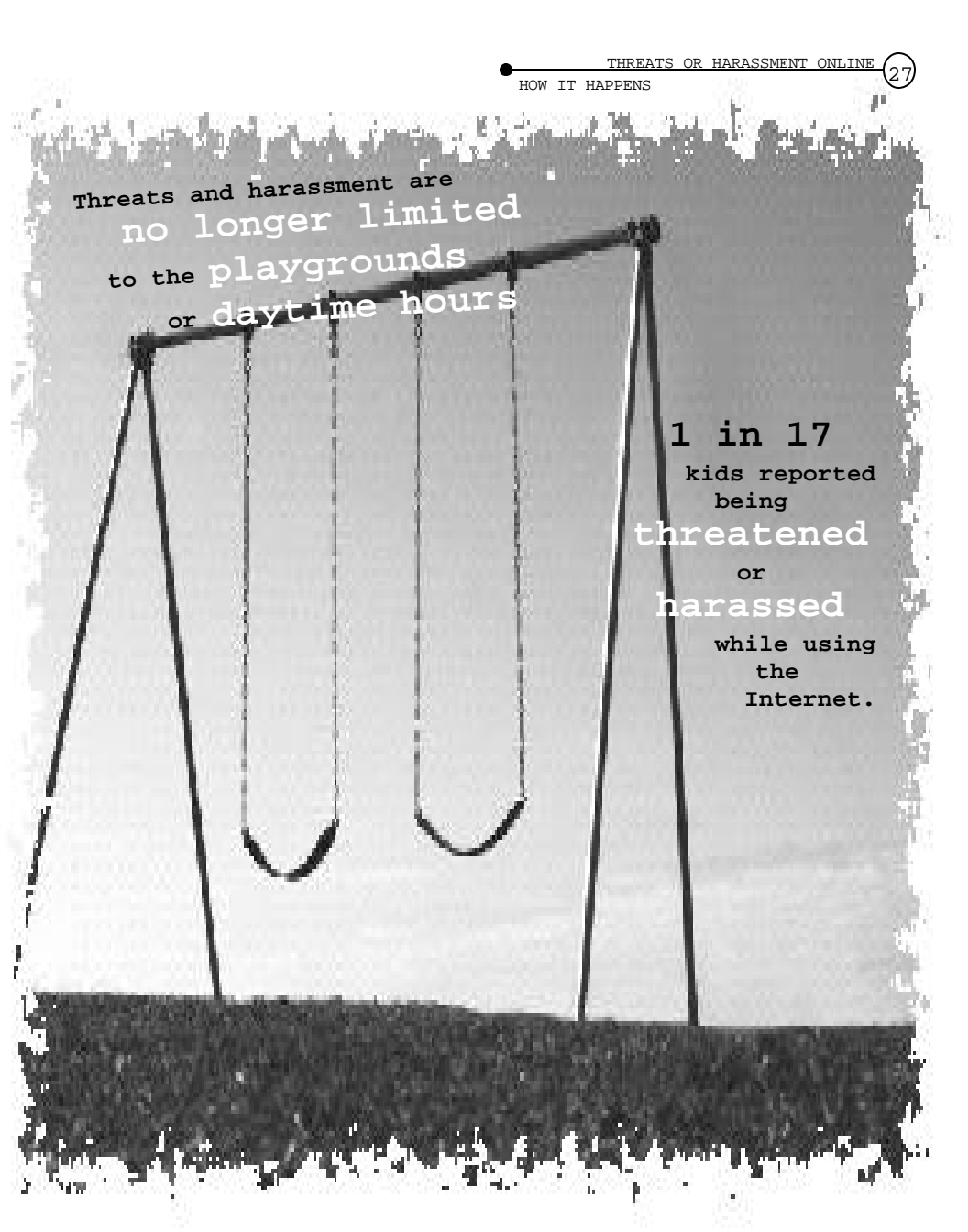
CONSIDER INSTALLING ADDITIONAL CONTROLS

You may also want to acquire additional parental control software that limits what your child can access. Filtering devices can add another level of security, although many people find that the controls available on their computer and through their ISP are sufficient.

1-800-THE-LOST

REPORT SUSPICIOUS ACTIVITY

If your child or anyone in the household has received child pornography, contact local law enforcement. You should also contact authorities if your child has received obscene material from someone who knows that your child is under the age of 16. You may also call 1-800-THE-LOST (1-800-843-5678) or visit **WWW.CYBERTIPLINE.COM**

Threats and harassment are no longer limited to the playgrounds or daytime hours

1 in 17 kids reported being threatened or harassed while using the Internet.

"CYBERBULLIES"

may use chat rooms, email, instant messaging and websites to embarrass a child.

· ·

If someone threatens your child with violence, immediately contact law enforcement officials

SAVE THE ORIGINAL MESSAGE

Don't delete or erase threatening emails or other communications from your mailbox or voicemail. If you are asked to share a threatening email message with law enforcement, forward the original message. A printed copy of the email or an excerpt from it will not be as useful to law enforcement as the original email message that you received.

If your child is being threatened or harassed online, you may want to contact one or more of the following:

SCHOOL RESOURCE OFFICER

Your child's school may have a School Resource Officer (SRO), a sworn law officer assigned to their school. If so, let the SRO know about the harassment or threats. If your school does not have an SRO, contact local law enforcement.

INTERNET SERVICE PROVIDER

Your email account settings or instant messaging software may allow you to block further messages from the sender. You can report the harassment or threats to your ISP and the harasser's ISP, if you know which ISP the harasser uses. You can ask that the harasser's account be suspended or blocked.

CYBERTIPLINE

If your child receives invitations for sexual acts or unsolicited obscene material over the Internet, you can report it by calling **1-800-THE-LOST (1-800-843-5678)** or by visiting **WWW.CYBERTIPLINE.COM**

As parents,
we can't afford
to let our

children's
knowledge

OUTSTRIP OUR OWN
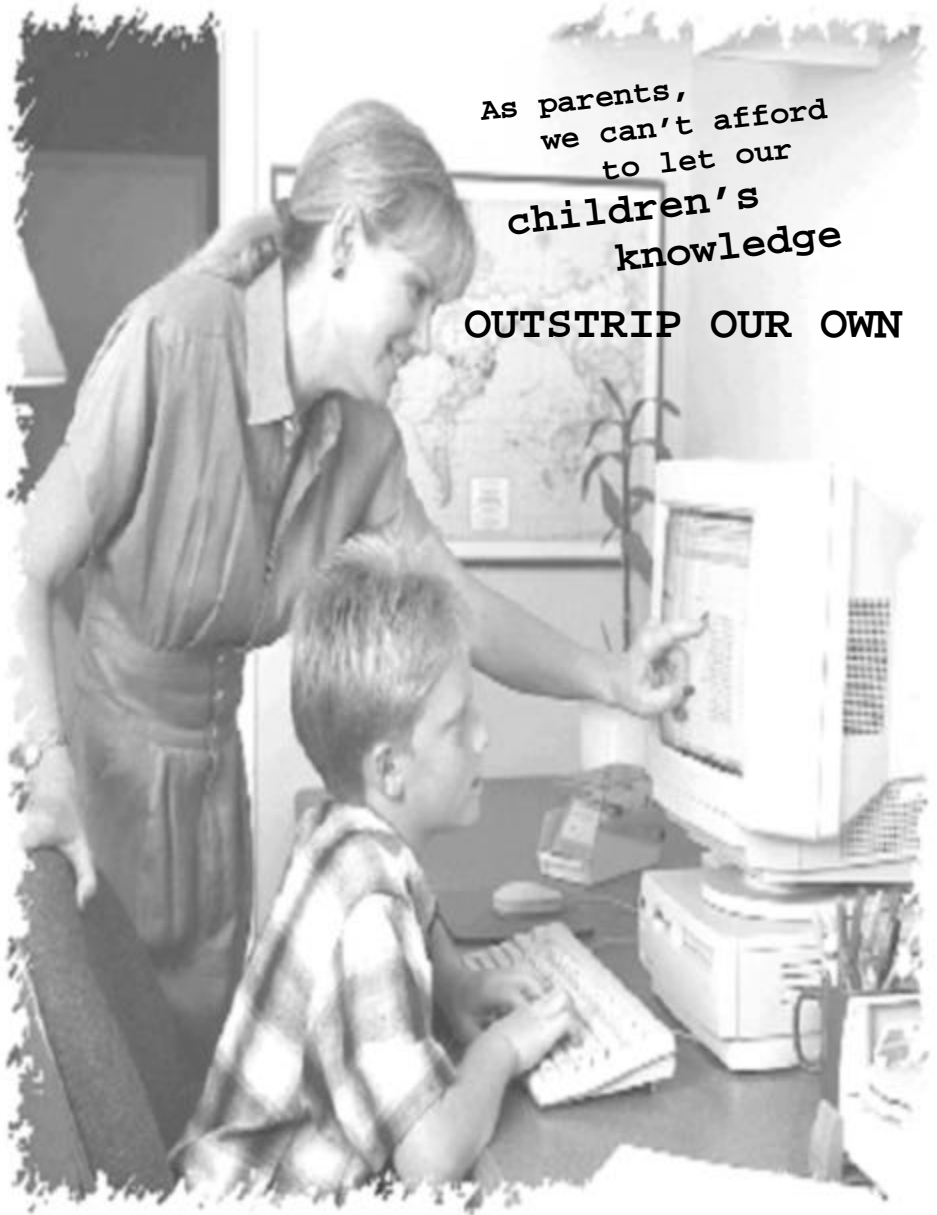
IN A CALM MANNER, TELL YOUR CHILD WHAT IS DANGEROUS ABOUT THE INTERNET

THIS CAN INCLUDE:

- Legal or financial harm to the family if you "click" without getting permission
- Exposure to harmful material (violence or sexually explicit scenes)
- People online who may start off friendly, but then change

Even the youngest child can understand the old adage "don't talk to strangers." Teach children from an early age that this includes people who try to talk to them online

TALK TO YOUR CHILDREN ABOUT POTENTIAL DANGERS

ENCOURAGE THEM TO TELL YOU WHEN:

- Someone they don't know attempts to engage them in an online chat
- An inappropriate site comes up on the screen
- Someone harasses or threatens them online

Ask your child to tell you when anything questionable happens to them online. Make it clear that they will not lose Internet privileges or be punished if they tell you

TEACH YOUR CHILDREN ABOUT THE DIFFERENCES BETWEEN "PRETEND" AND REALITY ON THE INTERNET

- Many children like to pretend to be someone else while online
- They feel they are anonymous and can take risks
- However, other people also like to pretend to be someone else while online
- But they do it for totally different reasons. Sometimes they do it to hurt people.

Children need to understand that real world rules and values apply on the Internet as they do in real life

DON'T JUST TELL YOUR CHILDREN WHAT THEY CAN'T DO

- Make a point to sit with your children and see the sites they like to visit
- Explain why you think the site is inappropriate

MAKE IT CLEAR THAT YOU'RE IN CHARGE

- Children may not realize it but they need supervision
- Remind them that you have more experience dealing with the world

Your children must understand that just as you decide which movies they are allowed to see, you will supervise their online activities.

A RECENT STUDY FOUND THAT MOST CHILDREN DID NOT INFORM THEIR PARENTS WHEN THEY FACED A DIFFICULT SITUATION ONLINE, SUCH AS BEING CONTACTED BY SOMEONE THEY DON'T KNOW.

THE MAIN REASONS FOR THEIR HESITATION WERE EMBARASSMENT AND FEAR OF LOSING ACCESS TO THE INTERNET.

Source: National Center for Missing & Exploited Children and
Internet Crimes Against Children Task Force

CREATING FAMILY RULES
FOR INTERNET USE

SOME DECISIONS TO CONSIDER IN CREATING FAMILY RULES:

- Do you want your children to ask before they access the Internet?

- Do you want to limit the time your children access the Internet?
  If so, how much time per week or day?

- Do you want to specify when your children may access the Internet?
  If so, which hours?

- Do you want to permit your children to use email?
  If so, do you want to share an email account with them or have access to their account?

- Do you want to permit your children to use instant messaging?
  If so, do you want to approve their "buddies" list and require them to provide you with an updated copy of that list?

- Do you want to permit your children to enter chat rooms?
  If so, do you want to limit them to certain chat rooms that you have approved?

When possible, have your family computer rules in place before your children begin using the computer. Children will find it easier to accept and obey rules that have already been established.

43% of children
say they
do not
have rules
about Internet use
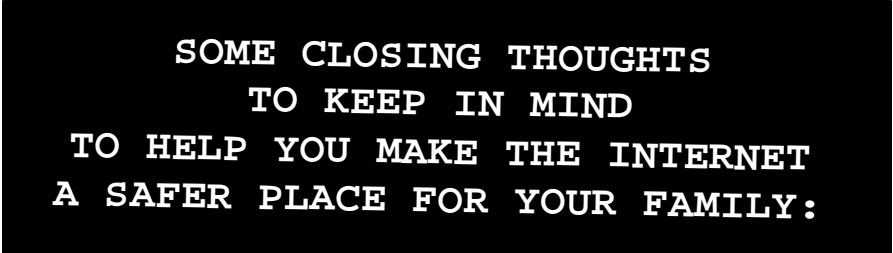in their homes

SAMPLE FAMILY RULES FOR INTERNET USE

USING THE COMPUTER IS A PRIVILEGE. IN ORDER TO ENJOY THIS PRIVILEGE AND USE THE COMPUTER, WE AGREE TO FOLLOW THESE RULES:

1) Computer use is not confidential and we do not hide hat we are doing on the computer

2) In our family, we get permission to access the Internet and we use our personal login

3) We visit websites that are appropriate for our age and we do not visit websites or access information that are "off limits" for us

4) We don't send photos or give out personal information without permission and we will tell our parents about any online messages that make us uncomfortable

5) We share an email account with our parents. We will not open or use an other email accounts

6) We do not enter chat rooms

7) We can go online between the hours of _____ and _____

8) Time on the computer is limited to: _____ hour(s) per day/week

9) Time on the Internet is limited to: _____ hour(s) per day/week

10) Instant messaging is only allowed with people that we already know. We will provide our parents with a current list of our "buddies"

11) We do not respond to messages from people we do not know

12) These rules apply to our home computer and all other computers we use

_____name _____date

YOU DON'T HAVE TO BECOME A COMPUTER EXPERT

Although young people are learning about computers at an earlier age, parents can exercise control over their children's use of computers and the Internet without having to become computer experts. As parents, we can't afford to let our own children's knowledge outstrip our own. We owe it to them to supervise and control their use of this powerful technology.

**SOME CLOSING THOUGHTS
TO KEEP IN MIND
TO HELP YOU MAKE THE INTERNET
A SAFER PLACE FOR YOUR FAMILY:**

BE ON THE LOOKOUT FOR ADVANCES IN TECHNOLOGY

For instance, your ISP may announce it has developed new parental controls tools. If so, you might have to download or activate them. These upgrades may help you better control what your child can access on the Internet. You should review your existing parental controls periodically. Make sure they are still appropriate and update them.

SPEND TIME WITH YOUR KID, OFFLINE AND ONLINE

Remember the computer is a great communication tool but you are an even better one. The best way to make sure your children aren't getting into trouble on the Internet or anywhere else in their lives is to stay engaged with them. Get them to show you what they do on the computer and the websites they visit. Ask them about anyone they've met online and familiarize yourself with those people.

IT ISN'T SNOOPING, IT'S CARING

MONITOR YOUR KIDS WHILE YOU TEACH THEM INTERNET SAFETY

Unfortunately there are real dangers lurking on the Internet. Some parents say they don't feel comfortable checking up on their child's computer activities. It is understandable that a parent would want to honor their children's privacy. However, experts say that should not come at the expense of knowing what your child is doing online. It isn't snooping it's caring.

NOTES

NOTES

**In recognition of
Cyber Security
Awareness Month
October 2005**