

**INTERNET SAFETY:
A Guide to Protecting Children in
Cyberspace**

*Information and Safety Tips
Concerning Children and
The Internet*

A Predator knows that children are not
prepared for the dangers they may face
on the Internet

In fact....

He's counting on it

WARNING



**CHILD ABUSE UNIT
LISPC
ICAC**



**CHILD ABUSE UNIT
3468 Lawson Blvd.
Oceanside, New York 11572
(516) 897-SPCC (7722)
Fax: (516) 897-4023**

With the rise in popularity of the Internet and the prominent role that it is becoming in everyday life, it has become necessary to understand that, as a fairly new medium of communication, it is largely unregulated. As a communications revolution, it's growth has exceeded our ability to police it and, while the various governments and law enforcement agencies attempt to catch up to the responsibility, it falls to the parents, schools and the vast moral majority to safeguard our children from the various elements that would use the Internet to prey on our youth. These guidelines are made merely to assist those responsible and to provide some helpful suggestions in safeguarding any child's use in the various functions such as chatting, email and browsing.



Types of Child Exploitation

- **The Possession, Manufacture and Distribution of Child Pornography**
- **The Online Enticement of Children for Sexual Acts**
- **Child Prostitution**
- **Child Sex Tourism**
- **Child Sexual Molestation (not in the family)**
- **Unsolicited Obscene Material Sent to a Child**



Risks Online

Meeting Someone Offline

Probably the most frightening result of online contact is when a child elects to meet someone in person with the knowledge of a parent or guardian.

Inappropriate Material

Pornography, anti-Semitism, gender roles, sexual deviant philosophies, How to make a bomb, etc.

Financial

Since age verification is sketchy at best, the lure of online gambling, auction houses and illegal monetary schemes is prevalent

Legal

One of the most popular aspects of the Internet in the last 3 years is the advent of "file-sharing". Copyright protected material is traded on a daily basis between computers which can lead to the liability of a financial lawsuit.

Online Fighting

Verbal disagreements during chatting sessions can sometimes lead to a continued form of harassment via chatting, emails or even hacking attempts.

Privacy

Obtaining personal information for nefarious purposes such as "identity theft" is becoming more prevalent every day.

Threats/Harassment

It is illegal to threaten or harass anyone—regardless of the medium from which it is delivered—yet, it does happen.

Misleading Information

The Internet is a vast resource of information and can, often times, be overwhelming in the amount that is found on any particular subject. Not all sources are credible and can be misleading.



Signs that your child may be at risk online

- Your child spends large amounts of time online.
- Your child changes the computer screen when you come into the room
- Your child receives phone calls from people you don't know
- Your child makes calls, sometimes long distance, to numbers you do not recognize.
- Your child receives mail from someone you don't know
- You find pornography on your child's computer.
- Your child becomes withdrawn from the family.
- Your child is using an on-line account belonging to someone else

By the end of 1998 40% of all homes in the United States had computers and 25% had Internet access. That trend is expected to continue as children and teenagers are the fastest growing users of the Internet. By 2005 an estimated 77 million children will be online.

Youth Internet Safety Survey

What you should do if you suspect that your child is communicating with a sexual predator online:



- Talk to your child. Don't approach them in an alarmed manner or one that might elicit a defensive emotional response. Instead, talk to them calmly and explain the dangers that surround online predators.
- Do not be afraid to use parental controls, Internet Filtering or Monitoring Software as an aid to help ensure child safety online. While they are not, by any means, a replacement for human involvement, they can be an invaluable aid for parents and are largely recommended and endorsed by law enforcement, teachers and administrators
- Monitor your child's use of the telephone and the calls they receive. Use the *69 feature or some form of Caller ID in an attempt to determine the source of the phone number in question. Pay attention to numbers that appear (long distance) on the phone bill and do not be afraid to question your child about them.
- Check your child's computer for any downloaded material. This may include graphics (bmp, gif, jpg) movies (mov, avi, asf, mpg, mpeg) or soundbites (wav, mp3). These files can be obtained via download from emails, various instant messaging programs (AIM, Yahoo Messenger, MSN Messenger, etc.), Content Providers (America Online, MSN), emails, or from various online sites.
- Never blame your child if he/she is a willing participant in any form of sexual exploitation. The child is not at blame or fault he/she is the victim. The offender always bears the complete responsibility for his or her actions.
- Contact the Child Abuse Unit through the "Contact" page available at childabuseunit.com

Safety Tips

- Seek out the advice and counsel of persons who are authorities on internet safety such as teachers, administrators or law enforcement (i.e. The Child Abuse Unit) so that you will gather a better understanding about issues concerning internet safety for children.
- The most important key to child safety is effective communication with your child. Remember, children who do not feel that they are listened to or who do not think that their needs are met in the home are more vulnerable to abduction or exploitation.
- Never give out identifying information
- While it may be enjoyable for a child to have a profile for content providers such as America Online or Microsoft Network (and even some Internet based services such as ICQ or Yahoo Messenger) the actual profile does provide a pedophile a tool when searching for a potential victim. With this in mind, **not** having/allowing a profile should be a consideration when creating/using an account.
- People online may not always be who they represent themselves to be. A child may be naïve enough to believe that the person they are talking to is someone of their own age but it could just as well be an adult attempting to lure them into a false sense of security
- The term stranger suggests a concept that children do not understand and is one that ignores what we do know about people who commit crimes against children. It misleads children into believing that they should only be aware of individuals who have an unusual or slovenly appearance. A clear, calm, and reassuring message about situations and actions to look out for is easier for a child to understand than a particular profile or image of a "**stranger**".
- Never allow a child to arrange a face-to-face meeting with another computer user without parental permission and observation. If a meeting is arranged, make the first one in a public spot, and be sure to accompany your child.
- Teach your child to notify you if they are contacted by an adult in instant messages, chat rooms, or e-mail
- Talk to your child about potential on-line dangers

Safety Tips (cont.)

- Teach your child the responsible use of the resources on-line. Show them the many benefits that it has to offer and how to take advantage of them for school.
- It's not at all uncommon for children to know more about the Internet and computers than their parents or teachers. As an excuse to get more involved you can ask them to teach you about the internet and the various things they have learned for it. It is a great way to learn their interests and habits online. There is absolutely no replacement for good parenting.
- Teach your children not to open e-mails, files, or Web pages that they get from people they don't really know or trust.
- For any account that gives a child access to the internet make sure that they never give out their password
- Be very leery of those who want to know too much. Teach your child to trust their instincts. If someone makes them feel uncomfortable, often enough, there is a good reason.
- Teach your kids the value of trusting their own judgment so as to strengthen them from being easily influenced into something that they feel is uncomfortable.
- Teach children to never respond to instant messages, bulletin board items, chat room queries or emails that are suggestive, obscene, belligerent or make them feel uncomfortable
- Discuss rules and guidelines for computer usage with your children. While developing some rules you give them the satisfaction of being involved in the process – even if you already had a clear objective in mind. Post these guidelines next to the computer as a reminder. Monitor your children's compliance with these rules. Excessive use of online services or the Internet, especially late at night, may be a clue that there is a potential problem.
- Parents should take an interest in the friends that a child makes online as they would those he or she makes at school.
- Review what is on your child's computer. If you don't know how or what something is then ask someone for help in finding or understanding what is found.

TERMINOLOGY

PORNOGRAPHY - A generic term that can refer to materials that are either "legal" or "illegal" to disseminate under the circumstances.

"Pornography" encompasses all sexually oriented material intended primarily to arouse the reader, viewer, or listener. Attorney General's Commission on Pornography (1986), Chapter One, "Defining our Central Terms." Serious works of art, literature, politics, or science; "mere nudity," medical works, even though they deal with sex or include sexual references or depictions, would not be considered "pornography" in the context of their legitimate uses. On the other hand, since obscenity can include both actual and simulated conduct, all "Hard-Core Pornography" that depicts penetration clearly visible ("PCV") is "implicitly" within the application of the constitutional criteria of the Supreme Court's obscenity test.

CHILD PORNOGRAPHY - Child pornography is material that visually depicts children (real children as well as computer-generated depictions of children) under the age of eighteen engaged in actual or simulated sexual activity, including lewd exhibition of the genitals. Child pornography laws were recently amended to include computerized images or altered (morphed) pictures of children, and counterfeit or synthetic images generated by computer that appear to be of real minors or that were marketed or represented to be real child pornography

Legal Definition: An unprotected visual depiction of a minor child (federal age is under eighteen) that consists of a visual depiction that "is or appears to be" of an actual minor engaging in sexually explicit conduct, including a lewd or lascivious exhibition of the genitals.

OBSCENITY - obscenity is graphic material that is obsessed with sex and/or sexual violence and is, therefore, prurient, patently offensive, and lacking in serious value. It is often referred to as hard-core pornography and includes close-ups of graphic sex acts and deviant activities, such as penetration, group sex, bestiality, torture, incest, and excretory functions.

MATERIAL HARMFUL TO MINORS - Material harmful to minors represents nudity or sex that has prurient appeal for minors, is offensive and unsuitable for minors, and lacks serious value for minors. This material is often referred to as soft-core pornography. There are "harmful to minors" laws in every state. **Note:** Indecent and harmful to minors material is legal for adults but illegal when knowingly sold or exhibited to minor children

Legal Definition: "Harmful to minors" means any written, visual, or audio matter of any kind that :

- the average person, applying contemporary community standards, would find, taken as a whole and with respect to minors, appeals to a prurient interest in nudity, sex, or excretion, and
- the average person, applying contemporary community standards, would find depicts, describes, or represents, in a patently offensive way with respect to what is suitable for minors, ultimate sexual acts, normal or perverted, actual or simulated; sadomasochistic sexual acts or abuse; or lewd exhibitions of the genitals, pubic area, buttocks, or post-pubertal female breast, and
- a reasonable person would find, taken as a whole, lacks serious literary, artistic, political, or scientific value for minors.

INDECENCY - Indecent material includes messages or pictures on telephone, radio, or broadcast TV that are patently offensive descriptions or depictions of sexual or excretory organs or activities. This is often referred to as "sexual nudity" and "dirty words"

- **broadcast indecency** - language or material that, "in context, depicts or describes in terms patently offensive as measured by contemporary community standards for the broadcast medium, sexual or excretory activities or organs.
- **computer "Internet" indecency** - "any comment, request, suggestion, proposal, image, or other communication that, in context, depicts or describes, in terms patently offensive as measured by contemporary community standards, sexual or excretory activities or organs."

SOFTWARE



Ensuring the safety of our children as they access the Internet can be a daunting task for parents and guardians. Between having to work and raise a household or being in charge of a large group of children at schools and libraries, there is only so much that any one person is capable of doing.

Available to the public are various hardware and software solutions that, while not a replacement for human involvement, can provide much needed assistance towards increasing the safety of the online environment for kids. Yet, even then attempting to gauge the reliability and effectiveness of the various products on the open market would be a monumental task in itself. There are hundreds of hardware and software "solutions" that perform distinct (and similar) functions and without a technical background their true effectiveness can not reasonably be discerned.

The Child Abuse unit has spent a considerable amount of time product testing a variety of hardware and software packages – testing their assortment of functions. We have established an opinion on a select few that we feel provide the most effective means of safeguarding the online environment which are available on the Child Abuse Unit website at childabuseunit.com.

FILTERING SOFTWARE

This is software that will block children from accessing inappropriate websites such as pornography, hate, violence, or generally any other topic a parent does not want their child to see. It is usually quite customizable (parent can add words/phrases that interest them) and also has some supplemental features: the ability to limit the amount of time kids spend online, privacy filters that can prevent a child from revealing their name, address, phone, or any other personal detail, etc.

* Using various methods, filtering software blocks content based upon parameters that are set by the guardian or parent such as whole websites or pictures. Some even block text.

* Various programs provide for a progressive monitoring of most, if not all, software programs used on any one system (not just Internet related programs)

* Most filtering software packages are highly customizable with regard to security preferences

MONITORING SOFTWARE

This is software that lets parents see everything their kids are doing online. It can be installed either totally invisible or in a mode that warns children that they are being watched. Monitoring software can record every single email, instant message, chat session, website, and even children's passwords. You get recordings of all chat conversations, instant messages, e-mails typed and read, all web sites visited, all programs/applications run, all keystrokes typed - EVERYTHING they do on the computer and on the Internet.

* Can automatically take snapshots, every hour, of the computer desktop, much like a surveillance camera. Benefits include: TRUE chat and email capture (SMTP and web-based email), TRUE chat and instant message capture and even key-logging.

* Some programs will save a file to a secret location on the computer (which only YOU can find) while others will directly email the results of any prolonged surveillance.

* Some programs can provide IMMEDIATE NOTIFICATION when someone encounters a dangerous website, chat or email.

* In some instances, email can be continually recorded and forwarded to an email address of your designation.

* The difference between various programs is a question of convenience -If you have continued access to the guarded computer or whether you travel frequently and wish to receive reports of computer activity delivered to a specific email address.

If you would like to make a donation to help the Child Abuse Unit in the fight to make the Internet safer for children please make any check payable to: **LISPC C** and mail it to:

LISPC C
3468 Lawson Blvd.
Oceanside, N.Y. 11572

Any correspondence may also be sent to the above address.

Electronic correspondence may be sent via the Child Abuse Unit website at childabuseunit.com from the **CONTACT** page or sent to: contact@childabuseunit.com

Telephone number: (516-897-SPCC (7722)
Fax number: (516) 897-4023

The Child Abuse Unit would like to acknowledge the NCMEC and Donna Rice Hughes "*Kids Online: Protecting you children in Cyberspace*" for use of material in the creation of this safety pamphlet.