



Internet Safety for Kids

A presentation for adults

The audio version of this course and accompanying PowerPoint slide deck is available online for free use at www.packet-level.com/kids. [Revision date: January 12, 2006]

Copyright (c) 2006 by Protocol Analysis Institute, LLC. This material may be distributed only subject to the terms and conditions set forth in the Open Publication License, v1.0 or later (the latest version is presently available at <http://www.opencontent.org/openpub/>).

This presentation was developed to provide awareness on Internet safety issues. The slide deck, course flyers, course description and other supplemental materials are freely available online at www.packet-level.com/kids for your use. We invite you to use the materials online to educate adults in your community on the issue of Internet predators and methods to protect our children.

This course was copyrighted with redistribution and publication rights covered by the Open Publication License defined below. Please direct questions or comments to kids@packet-level.com.

Open Publication License

v1.0, 8 June 1999

I. REQUIREMENTS ON BOTH UNMODIFIED AND MODIFIED VERSIONS

The Open Publication works may be reproduced and distributed in whole or in part, in any medium physical or electronic, provided that the terms of this license are adhered to, and that this license or an incorporation of it by reference (with any options elected by the author(s) and/or publisher) is displayed in the reproduction.

Proper form for an incorporation by reference is as follows:

Copyright (c) 2006 by Protocol Analysis Institute, LLC. This material may be distributed only subject to the terms and conditions set forth in the Open Publication License, v 1.0 or later (the latest version is presently available at <http://www.opencontent.org/openpub/>).

The reference must be immediately followed with any options elected by the author(s) and/or publisher of the document (see section VI).

Commercial redistribution of Open Publication-licensed material is permitted.

Any publication in standard (paper) book form shall require the citation of the original publisher and author. The publisher and author's names shall appear on all outer surfaces of the book. On all outer surfaces of the book the original publisher's name shall be as large as the title of the work and cited as possessive with respect to the title.

II. COPYRIGHT

The copyright to each Open Publication is owned by its author(s) or designee.

III. SCOPE OF LICENSE

The following license terms apply to all Open Publication works, unless otherwise explicitly stated in the document.

Mere aggregation of Open Publication works or a portion of an Open Publication work with other works or programs on the same media shall not cause this license to apply to those other works. The aggregate work shall contain a notice specifying the inclusion of the Open Publication material and appropriate copyright notice.

SEVERABILITY. If any part of this license is found to be unenforceable in any jurisdiction, the remaining portions of the license remain in force.

NO WARRANTY. Open Publication works are licensed and provided "as is" without warranty of any kind, express or implied, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose or a warranty of non-infringement.

IV. REQUIREMENTS ON MODIFIED WORKS

All modified versions of documents covered by this license, including translations, anthologies, compilations and partial documents, must meet the following requirements:

1. The modified version must be labeled as such.
2. The person making the modifications must be identified and the modifications dated.
3. Acknowledgement of the original author and publisher if applicable must be retained according to normal academic citation practices.
4. The location of the original unmodified document must be identified.
5. The original author's (or authors') name(s) may not be used to assert or imply endorsement of the resulting document without the original author's (or authors') permission.

V. GOOD-PRACTICE RECOMMENDATIONS

In addition to the requirements of this license, it is requested from and strongly recommended of redistributors that:

1. If you are distributing Open Publication works on hardcopy or CD-ROM, you provide email notification to the authors of your intent to redistribute at least thirty days before your manuscript or media freeze, to give the authors time to provide updated documents. This notification should describe modifications, if any, made to the document.
2. All substantive modifications (including deletions) be either clearly marked up in the document or else described in an attachment to the document.
3. Finally, while it is not mandatory under this license, it is considered good form to offer a free copy of any hardcopy and CD-ROM expression of an Open Publication-licensed work to its author(s).

VI. LICENSE OPTIONS

The author(s) and/or publisher of an Open Publication-licensed document may elect certain options by appending language to the reference to or copy of the license. These options are considered part of the license instance and must be included with the license (or its incorporation by reference) in derived works.

Distribution of the work or derivative of the work in any standard (paper) book form is prohibited unless prior permission is obtained from the copyright holder.

OPEN PUBLICATION POLICY APPENDIX:

Participants offering Open Publication works are listed <http://www.opencontent.org/>.

From the Author:

In 2003, at a conference attended primarily by law enforcement officers, I watched an agent present a case that involved children who had been tortured in the process of creating child pornography.

Given the option to “deal with it” or do something about it, I decided to investigate the problem further in collaboration with my co-worker, Brenda Czech, at the Protocol Analysis Institute, LLC.

We began researching the issues of Internet safety and almost immediately we were overwhelmed with the information on the topic, but we could not find a clear presentation for adults on the key issues and possible solutions.

We believe that education serves as the greatest protective force on Internet safety issues relating to children and teens.

It appeared to us that, although there were numerous technical tricks available for blocking and filtering communications on the Internet, the key method in protecting these kids would be education. We do not believe that computer or Internet restrictions are the best solution when we want our children to become Internet-savvy leaders in technology.

This course was developed to provide adults with background information on the predators that lurk on the Internet, their methods of luring children into physical contact, the technical options available to protect children and the parental advice defined by a well-established child sex exploitation detective.

We hope that after taking this course you will present it to other adults who could learn, benefit and share this Internet safety knowledge. If your company would like to host this document, please contact us at kids@packet-level.com.

Thank you for your interest in this very important topic.

Laura Chappell
Sr. Protocol/Security Analyst
Protocol Analysis Institute, LLC
lochappell@packet-level.com
www.packet-level.com/kids

Brenda Czech
Project Manager
Protocol Analysis Institute, LLC
bczech@packet-level.com
www.packet-level.com/kids

*This book is dedicated to the
worldwide victims of child sexual exploitation
and the law enforcement officers, government organizations,
private companies and private citizens involved in
the effort to protect our kids.*

SPECIAL THANKS

We wish to acknowledge the organizations who have developed materials referenced in this presentation – specifically Detective James McLaughlin, LiveWires Design, National Center for Missing and Exploited Children, NetSmartz, the High Technology Crime Investigation Association, the Internet Crimes Against Children (ICAC) Task Force, Officer Kim Mercer (SFPD ICACTF), Child Quest International, Officer Chip Wells, and Xavier Von Erck and the team at Perverted-Justice.com..

In addition, special thanks to Altiris Corporation, Hewlett-Packard, Microsoft, Novell and the US Courts, Middle District of Pennsylvania for allowing us to present this material at their conferences (ManageFusion, HP ENSA@Work, TechEd, BrainShare, US Courts Employee Conference).

We truly appreciate all the people who have begun using this material to educate adults in their communities.

Table of Contents

Open Publication License.....	i
From the Author	iii
Dedication	iv
Special Thanks.....	v
Internet Safety for Kids Title	1
Warning.....	2
The Statistics.....	3
Contents Listing	4
Case Review: Kylie Taylor Case	5
Case Review: Sex Solicitation Results in Arrest.....	6
Case Review: S.J. Man Surrenders in Child Sex Case.....	7
Case Review: Man Delivers Live Rape Video.....	8
Case Review: Man Accused of Soliciting a Child.....	9
Case Review: Predator Shopped at myspace.com	10
The Perfect Victim.....	11
Personal Web Pages	12
Is Your Child's Information Online?	13
Technophilia	14
Cyber Child Sex Offender Terminology.....	15
Six Steps to Luring	16
Groomers	17
Befriending Techniques	18
Chat Room Tools	19
Chat Room Session Log #1: Picture Please.....	20
Chat Room Session Log #2: Wanting Young Virgins	21
Chat Room Session Log #3: Cyber Stalker.....	22
Predator Profiles	23
Physical Access is the Goal.....	24
U.S. Child Pornography Law	25
General Internet Safety Tips	26
Advice for Parents.....	27
Monitoring and Restricting Internet Use.....	31
Parental Resources	33
NetSmartz	34
www.netsmartz.org	35
National Center for Missing and Exploited Children (NCMEC).....	36
LiveWires Design.....	37
i-SAFE America	38
Child Quest International	39
Protocol Analysis Institute Kids Project.....	40
What to Do Now	41
Final Thank You	43
Appendix A: Contacts and Resources.....	44
Appendix B: Statistics.....	50
Appendix C: Links List	53
Appendix D: Instructor Resources	55

Internet Safety for Kids

(a presentation for adults)

Who is Most at Risk to Online Predators
Online Victimization Techniques
How to Protect Your Kids
www.packet-level.com/kids
kids@packet-level.com

This presentation keys in on three main areas:

- **Who is most at risk to online predators**
Based on statistics offered by the National Center for Missing and Exploited Children and research documented by Detective James McLaughlin (Keene Police Department), we describe the ideal victim – in age, online characteristics and behavior
- **Online Victimization Techniques**
Examine how predators befriend kids online and the six steps to luring (as defined in the **MISSING** Game developed by LiveWires Design). We define the warning signs of offender manipulation and examine actual chat room sessions in which a 13-year old fictitious victim is approached by various potential predators.
- **How to Protect Your Kids**
The final section of this course provides general advice regarding safe Internet access and specific advice from Detective McLaughlin based on numerous prior cases. In addition, we list and examine the resources available for further training and assistance should your child be solicited with unacceptable material or advances online.

Warning

- ✍ Viewer discretion advised
 - ✍ This is a disturbing topic
 - ✍ This presentation was NOT designed to be viewed by children

This presentation was not designed to be viewed by children – the initial slides depict numerous child pornography, kidnapping, sexual assault and victimization cases.

This can be a painful presentation to experience because of the nature of the materials and viewer discretion is advised.

The Statistics

- ✍ 1 in 5 children are sexually solicited or approached over the Internet in a one-year period of time. **[Online Victimization: A Report on the Nation's Youth]**
- ✍ 20% of violent offenders serving time in state prisons reported having victimized a child. **[Source: U.S. Department of Justice]**

Additional statistics are available online at www.ncmec.org (The National Center for Missing and Exploited Children).

- The “1 in 5” statistic is from a June 2000 report Center for Missing and Exploited Children. The study surveyed over 1500 kids aged 10 to 17. As the rates of pedophilia increase, the statistic is most likely much higher.
- During the development of this course, we created a 13-year old fictitious child and entered a chat room – within 3 hours we had been solicited by 5 individuals and were provided with a link to view a live webcam of a man masturbating. In one case, our character was contacted by a man who felt that 13 might be a bit too old – he explained that he had a particular fondness of 8 to 10 year old girls.

Contents

- ✍ Sample Cases
- ✍ Cold Hard Facts about Technophilia
- ✍ Cyber Child Sex Offender Terminology
- ✍ Six Steps to Luring
- ✍ Cyber Child Sex Offender Profiles
- ✍ Most At-Risk
- ✍ Advice for Parents
- ✍ Resources

This course covers eight areas relating to child sex exploitation and Internet safety:

- **Sample Cases:** Five case studies of children lured over the Internet
- **Cold Hard Facts about Technophilia:** Definition of this term coined by Detective James McLaughlin to describe sexual deviations using computer technology
- **Cyber Child Sex Offender Terminology:** Classifications of sex offenders based on their actions
- **Six Steps to Luring:** Based loosely on the **MISSING** Game, these six steps may be used to obtain the ultimate goal – physical access to the child
- **Cyber Child Sex Offender Profiles:** Review of the background of hundreds of sex offenders indicate varied occupations, number of previous sexual arrests, ages and exposure to children
- **Most At-Risk:** These are the standard characteristics often sought by predators
- **Advice for Parents:** What parent can do to protect and educate their child on Internet safety
- **Resources:** Numerous links to government and private organizations offering assistance and education on Internet safety

Kylie Taylor Case

- ✍ Detectives said Kylie (14) arranged to meet Sadler through Internet chat rooms and phone calls after she left her foster home.
- ✍ Court documents said Kylie was found in a darkened room with video cameras and restraints where he whipped, sexually assaulted her and chained her to a bed when he left the residence.
- ✍ Stanley Scott Sadler, age 47, has been charged with one count of kidnapping in the first degree, three counts of rape of a child in the third degree, and one count of sexual exploitation of a minor.
- ✍ Kylie was located by her mother and an ad hoc group of volunteer pedophile trackers (www.perverted-justice.com).

Stanley Scott Sadler held Kylie hostage, tortured and repeatedly raped Kylie Taylor, a 14-year old he met in an Internet chat room. Kylie's Internet chat sessions with Sadler eventually led to phone conversations (a common trait in Internet luring).

Stanley Scott Sadler is a father of three.

Xavier Von Erck, the Director of Perverted Justice, states that "Kylie herself was as responsible for her recovery as anyone. She was savvy enough to know to click onto sites she was known to visit." Many people were on the alert for her screen name in these other areas – when she appeared, they knew she was alive and they began the traceback. "After her rescue, I complimented her on that practice. She confirmed that was the exact reason she was doing it."

"We believe the Taylor case to be representative and a good lesson for parents that, should the unthinkable happen to their child, they should never give up and just sit back idly by. There are many avenues parents should take if they are not being listened to."

Note: "Perverted Justice" was started by two concerned citizens in July 2002 with a goal of increasing awareness and combating sexual predators online.

Sex Solicitation Results in Arrest

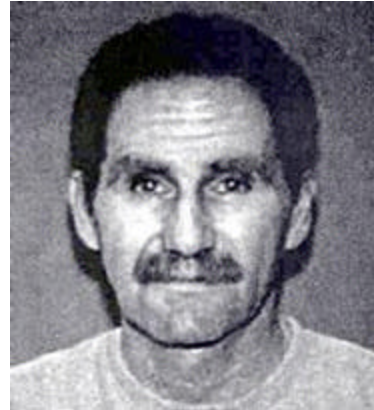
- ✍ A 23-year-old Pueblo man is being held in Douglas County Jail after allegedly soliciting sex with children in an Internet chat room. Lenard James Brown was arrested March 4, according to a press release by the Pueblo County Sheriff's Office.
- ✍ In February, Brown allegedly posted a message in a chat room asking parents to arrange for him to meet privately with their children. The children ranged in age from 1 to 14. A person who saw the message notified authorities.

This case was initiated after Lenard James Brown allegedly posted a message soliciting children ages 1 through 14 for a sexual encounter.

When a Douglas county investigator posed as a 14-year old girl, Brown agreed to meet her at a park and was apprehended.

S.J. Man Surrenders in Child Sex Case

✍ A former Redwood City middle school teacher turned himself in Tuesday at the Santa Clara County Jail after police seized his home computer and allegedly found child pornography. David Joseph Welsh, who most recently taught at the North Star Academy, was charged with a misdemeanor of possessing child pornography and is being held in lieu of \$150,000 bail.



The Cyber Child Sex Offender Profile document presented later in this course illustrates the diverse occupations of sexual predators.

Numerous law enforcement agencies have testified that “there was a significant likelihood that a person in possession of child pornography was also involved in sexually abusing children.” Organized Criminal Pedophile Activity: A Report by the Parliamentary Joint Committee on the National Crime Authority, Australia 1995.

Sixty-seven percent of offenders convicted of Internet-related sex crimes with children were also found to be in possession of child pornography.

(National Center for Missing and Exploited Children)

In addition, pedophiles tend to choose jobs that put them in constant contact with children.

(CrimeLibrary.com)

Man Delivers Live Rape Video

✍ A local man who went on the Internet and offered live video of himself having sex with a 3-year-old girl is behind bars, police say. Paul A. Kraft has been charged with two counts of rape and one count of pandering sexually oriented material involving a minor.



A particularly disturbing case, Kraft was indicted by a grand jury on five counts of rape and twelve counts of pandering sexually-oriented matter involving a juvenile.

Kraft's exploits were discovered when a U.S. Secret Service agent in Florida monitored an Internet chat room on Yahoo.com called "Preteen, Baby and Toddler Sex."

Kraft was married and a student of a technical college at the time of his arrest. Each rape count carries a maximum sentence of life without the possibility of parole.

Man Accused of Soliciting a Child

✍ A 53-year-old accountant who bragged on the Web about molesting children all over the country, was charged Thursday with three counts of soliciting sex from a child using the Internet, authorities said. Roy Mason, of 2009 Highview Fall Place, was arrested Thursday on an Indiana warrant at his home by the Florida Department of Law Enforcement with help from the Hillsborough County Sheriff's Office, said Mike Duffey, an FDLE computer crimes special agent. Authorities are examining the computer found in Mason's home.

This predator bragged about his crimes – fortunately some of these sexual predators talk openly about their actions making them more likely to be caught.

Forensic investigation plays an important role in locating evidence on the computers of the child victims. Forensic investigations require access to the computer system or systems most likely to have been used by the victim or the predator. Examination of evidence in memory, on the local hard drive or on removable drives may assist law enforcement in assisting victimized children. Do not turn off the computer before law enforcement can examine it.

Only 17% of youth and approximately 10% of parents could name a specific authority to which they could make a report (of underage solicitation), although more said they had heard of such places.

(Crimes Against Children Research Center)

If you believe your child has been or is being victimized, contact the CyberTipline at 1-800-843-5678 in the United States. In Europe, visit www.inhope.org for local contact information.

Note: Refer to *Appendix A: Contacts and Resources* for additional resources for various countries.

Predator "Shopped" at *myspace.com*



William Warren Greico, 42, first approached the girl after he saw her posting on *myspace.com* in August. Billing himself as a man named "Tyler," the Seminole High School English teacher sent his picture to the girl and a message asking if she'd like to be friends.

Detectives arranged a sting after Greico suggested that he and the girl meet at an undisclosed location

The teenager, who attends high school in Tampa, told Greico she thought it was strange that he would want to be friends with her since he was so much older than she. She informed her mother about Greico's message who then informed authorities.

Undercover investigators corresponded with Greico over the Internet for four months. In one recent exchange, Greico allegedly made explicit references to oral sex in a message he thought he was sending to the girl, she said.

The Perfect Victim

- ✍ Ideal age: 11-14
- ✍ No or little parental involvement
- ✍ No definite bedtime
- ✍ Can be away from home without anyone knowing where he/she is
- ✍ Has exclusive use of the computer in a private area

This definition of the perfect victim was extracted from *Characteristics of a Fictitious Child Victim: Turning a Sex Offender's Dreams into His Worst Nightmare* by James McLaughlin (International Journal of Communications Law & Policy).

Although the ideal age is listed as 11-14, do not discount the possibility that predators are hunting for younger or older victims.

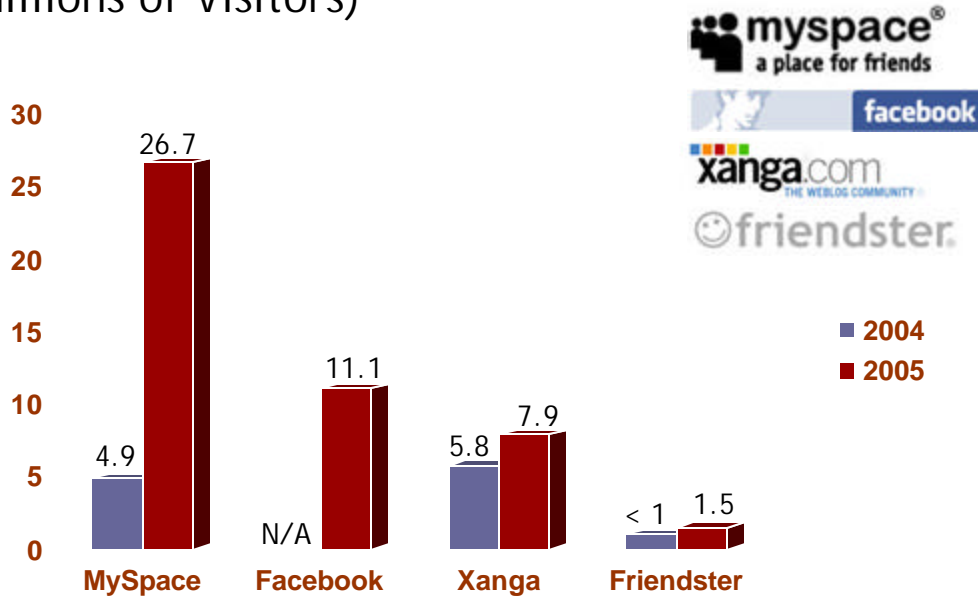
One of the key characteristics of the perfect victim is little or no parental involvement (which can be apparent when the predator obtains information about the victim's bedtime, personal freedom and computer use).

Underage females are targets of solicitation at twice the rate of underage males.

(Crimes Against Children Research Center)

Personal Web Pages

(Millions of Visitors)



As seen in the case of William Warren Greico, personal web sites such as MySpace, Facebook, Xanga and Friendster can be shopping grounds for predators. Kids release a tremendous amount of personal information such as their school name and mascot, hobbies, best friends' names and nicknames, IM screen names, family pets, favorite teams and often quite a bit of sexual detail about themselves.

In some cases, you don't need to have an account to search for someone based on their nickname, interests, location, AOL ID, Yahoo ID, MSN Username or email address (LiveJournal).

Is Your Child's Information Online?

- ✍ Data mining training course entitled “Advanced Internet Research and Intelligence” is online
- ✍ Visit www.htcia.org > Archived Webcasts
- ✍ Registration is free
 - ✍ www.google.com
 - ✍ www.myfamily.com
 - ✍ www.zoominfo.com
 - ✍ www.alltheweb.com
 - ✍ www.zabasearch.com

Predators may put in extensive time to search for the perfect victim and gather information to make the luring process more effective. Does your child belong to a soccer team that maintains a website with photos of the children at their latest meet? These types of sites may provide too much information about your child and should be (at least) password protected.

Consider performing an online reconnaissance operation on your child's name – is their name online somewhere? Determine if their personal information is online (birthdate, school name, teacher name, nickname, home address, home phone number, picture, etc.). One of the key pieces of advice to protect children online is to keep personal information off the Internet.

Varied search engines and data gathering services can be used to look for your child's information online. Consider taking the free webcast training course available online at www.htcia.org. The course is entitled, “Advanced Internet Research and Intelligence.” The instructor, Cynthia Hetherington, is a professional online researcher and excellent presenter.

The High Technology Crime Investigation Association (HTCIA) is a global organization formed to cultivate a cooperative information-sharing environment between law enforcement and private entities.

Technophilia

Term defined by Detective James McLaughlin, Keene County Police Department

“Persons using the computer to engage in sexual deviance”

This term differentiates this disorder from other types of sexual disorders by including the specific reference to computers (“techno”) as the medium for the predatory actions. Recognized as a cognitive distortion, pedophilia may or may not include access to the computer (some pedophiles exchange printed pictures as opposed to digital pictures).

Technophilia is a disorder that is fantasy-fueled – the computer providing access to the materials that the technophiliac obsesses over. Although physical access to the child may be the ultimate goal, in many cases the actual physical contact may fall short of the technophiliac’s fantasy.

Detective James McLaughlin worked with a Child Sex Exploitation team supported by an Internet Crimes Against Children (ICAC) grant.

Consider downloading the documents at www.ci.keene.nh.us/police/task_force.htm. Besides a brief definition of the creation of the Child Sex Exploitation team, this site maintains the child sex offender profile document which is examined later in this course.

Most teens say they do not tell their parents when a stranger contacts them online.
(Teenage Life Online)

Cyber Child Sex Offender Terminology

Travelers	those who manipulate or coerce kids to meet them in person for sexual purposes
Collectors	those involved in collecting child pornography
Manufacturers	those who create child pornography on any type of medium (all manufacturers are collectors)
Chatters	those presenting themselves as trustworthy individuals in chat sessions

These four basic terms separate the types of child sex offenders based on their actions and affinity for child pornography.

Travelers focus on physical contact – that is their ultimate goal. The cases presented at the beginning of this course detailed the downfall of several travelers. These predators may arrange to meet the child victim at a shopping mall, school, soccer field, theater, private home (while the parents are out) or other location.

Collectors may amass huge collections of child pornography. Although they may actively trade images with other collectors, these predators are typically not involved in the creation of these images.

Manufacturers create child pornography using a variety of media (digital pictures, printed pictures, video, etc.). They may actively solicit children through bribery, coercion or force. Manufacturers are always considered collectors.

Chatters may be seen as harmless individuals who may not collect child pornography or seek physical contact with the victim. They are not harmless however – they can expose the child to sexually inappropriate communications and even graphic images depicting sexual images. Chatters may eventually develop into collectors or travelers.

Six Steps to Luring

Based loosely on the **MISSING** Game available online at www.livewwwires.com.

1. Just Like You - Befriending
2. Making the offer
3. Incriminating evidence
4. Contact – the “honeymoon phase”
5. Guilt and threats as coercion
6. The truth emerges

The **MISSING** Game is based on a true story of a boy who was lured through chat room communications.

*Zack spent all his waking hours talking to strangers on the Internet.
Now he has disappeared. Can you find him?*

The purpose of the **MISSING** Game is to prepare children to resist the lures of an on-line predator. It is designed as a prevention tool as well as an educational tool and gives kids an opportunity to see the consequences of unsafe Internet use without having to make those same mistakes in their own lives.

The game box contains a Guide for Parents and Teachers, a videotape, a Detective's Notebook, copies of the **MISSING** Game on CDs, a poster and an Electronic Guide on CD (only included in the Workshop Edition of the game).

After receiving the **MISSING** Game, watch the video documentary first to see an overview of the game and related case studies. The video also provides sample successful conversations with kids – this helps prepare you for follow-up and ongoing discussions about Internet luring.

Note: In real life, the boy was caught on his way out of the house to meet the predator.

Groomers

- ✍ Most Internet luring instances begin with the process of ‘grooming’ – forming a trusting bond with the child. There are several types of groomers including:
 - ✍ Romantic groomers
 - ✍ Aggressive groomers
 - ✍ Monetary/status groomers

The “Six Steps to Luring” on the previous page provides a somewhat simplistic view of the luring process. Not all predators follow the same process or use the same methods. They often do begin with the befriending process however. This process includes “grooming” the child – forming a trusting bond with the child.

- Romantic groomers may woo the child with adulation and romantic fantasies involving the child and predator. For example, this type of groomer may tell the child how they would shower them with flowers and gifts and take them to romantic settings.
- Aggressive groomers may actively show impatience with the child and push the child to meet with them much sooner than the more patient romantic groomer.
- Monetary/status groomers may play on a child’s need for emotional, physical and financial independence.

There are many "types" of groomers. Not all groomers will use guilt and threats to gain power over the child and not all groomers have the same patience level and persistence.

Scott Sadler spent *a full year* grooming Kylie Taylor. Many of his chat communications with Kylie were simply information gathering sessions for future grooming attempts. On the other hand, Benjamin Brown, convicted of raping a 14 year old, worked in a faster, more haphazard manner.

Befriending Techniques

- ✍ Chat room discussions
 - ✍ Portrays same age, same likes, same dislikes
 - ✍ Portrays age-typical awkwardness
 - ✍ Begins to share some secrets
- ✍ Telephone
- ✍ Email
- ✍ Webcamming
- ✍ Verbal Chat on Internet (Microphone)

Spending just a few hours online as a fictitious child enables you to witness the befriending process first hand.

Predators may review the child's online profile and ask a series of personal questions to get a better feel for the child's weaknesses and insecurities. What are the child's hobbies? Does the child like/dislike their parents, brothers, sisters, school, etc.? Is the child curious about sex? Is the child currently engaged in any sexual activities?

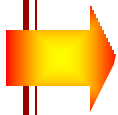
As you will see later in this presentation, we set up a fictitious child victim online and were immediately asked for photos and a phone number. The predators also wanted to know if our victim had a webcam so they could see our victim. In many cases, the predators provided access to their webcam so they could fuel their exhibitionist needs.

This type of contact is not just limited to chat rooms – some Internet multiplayer games allow you to have live communications with other players.

Fifty-four percent of girls claim the ability to carry on a cyber-romance.
(Girls Scout Research Institute)

Chat Room Tools

- ✎ MSN Messenger
- ✎ ICQ (“I seek you”)
- ✎ AOL Instant Messenger
- ✎ Yahoo! Messenger & Yahoo Chat
- ✎ mIRC (many Internet Relay Chat)



Recommendation: Tracking Teresa from NetSmartz (www.netsmartz.org)

The list above only shows some of the chat room options available online. Other IM (Instant Messenger) sites offering chat rooms include:

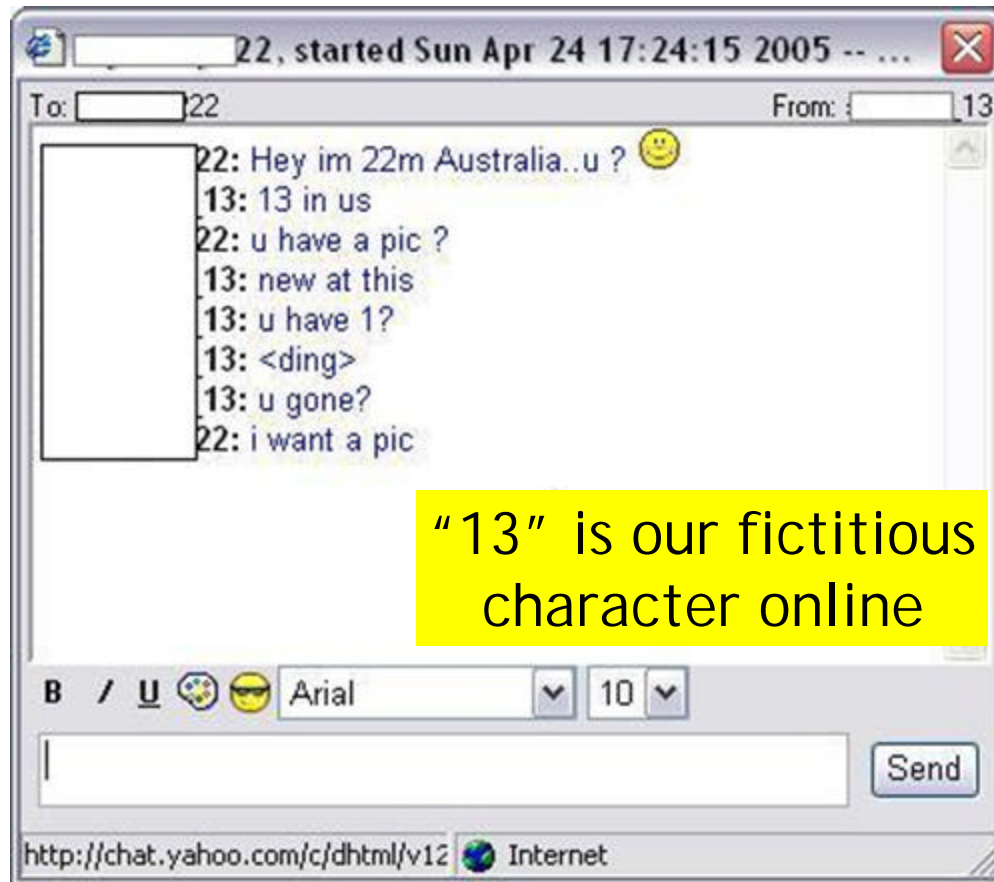
- www.talkcity.com
- www.spinchat.com
- www.boldchat.com

In addition, www.myspace.com has become VERY popular as a free site for setting up a personal web page and blog (information that is immediately published on a web site as a biographical log). People setting up pages on www.myspace.com often provide detailed information about themselves including their likes/dislikes, friends' names, school information, hobbies and family member details.

The Tracking Teresa presentation depicts a chat session with a predator who is researching the child on the side while the chat is taking place. This is a very interesting presentation offered by NetSmartz.

Seventeen percent of parents believe their children are posting online profiles compared to forty-five percent of children who report doing this.

(Web Savvy and Safety)



To get a feel for being a child victim online and the frequency and speed of a sexual encounter online, we established a Yahoo account as a 13-year old girl who lives in California. We were online less than 10 minutes when the first IM window appeared.

The graphic shows the typical reaction we received to our 13-year old fictitious child in the Yahoo chat rooms. We always stated immediately that our character was only 13 years old – this person was very insistent on getting a photo and did not appear concerned that our character was only 13.

Note: Screen names have been intentionally blocked.

More than half (fifty-six percent) of online teens have more than one e-mail address or screen name. Half of online girls have more than one screen name or email account and nearly one in five girls have more than four identities.

(Teenage Life Online)



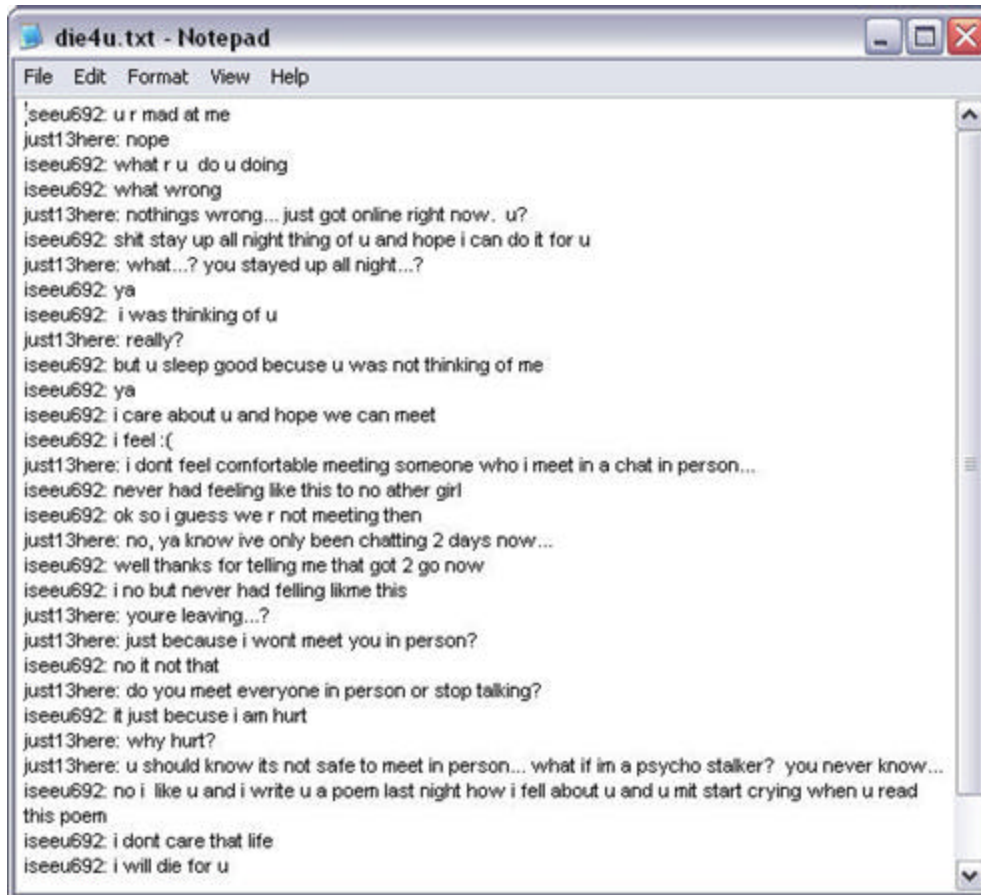
We were constantly bombarded with IM sessions asking for “as/” – age, sex and location (or “a/s” in this case).

This character moved right into the personal questions and eventually toyed with the idea of coming from the Philippines for a “visit” with our 13-year old virgin character. He immediately asked personal questions to see how experienced our character was with sex and what her body dimensions were.

At times, we could not keep up with all the IM sessions and some predators would become impatient with our slow responses. When we used a “little sister barging into the room” as an excuse for slow responses, this predator immediately began asking the name, age and body dimensions of our fictitious little sister. He was thrilled to learn that our character had an 8-year old sister.

This predator expressed an interest in 8 and 10 year old virgins and felt 13 might be a bit too old for him.

Note: Screen names have been intentionally blocked.



We were bombarded with emails and IM sessions from iseeu692 over several days – our first cyberstalker. As you can tell from the chat session log shown above, iseeu692 professed his commitment to our 13-year old character (he stated that he was in his “mid-30s but very fit”).

He stated that he stayed up all night long writing poetry to our character (a cursory review of the time/date stamp on his email headers verified that he didn’t get much sleep).

He wanted to push our 13-year old into a deep online relationship and then move forward. As you can see from the log above, he was already in “stalking mode” after our character had only been online 2 days.

In the last line of this log, iseeu692 states “I will die for u” to our fictitious victim. That type of devotion could be very powerful over a young girl who may feel insecure and unloved as she heads into the teenage years.

Note: Screen names have been altered.

Predator Profiles

<http://www.ci.keene.nh.us/police/offender1.htm>

Occupations	Involvement with children	Age	Locations	Past sex arrest
Engineer	On parole/in therapy	46	NH	Yes
GM/Radio Station		44	NH	No
Computer Tech.	Mother of two	38	NH	No
College student		18	IA	No
Factory worker		39	SC	No
Nurse	Mother of one	31	OK	No
Fast food worker		24	NH	No
Gas station worker	Worked as nanny	29	NY	No
Computer Tech.		32	CANADA	No
Air Port worker		32	GA	No
	10			
Unemployed		38	NH	Yes

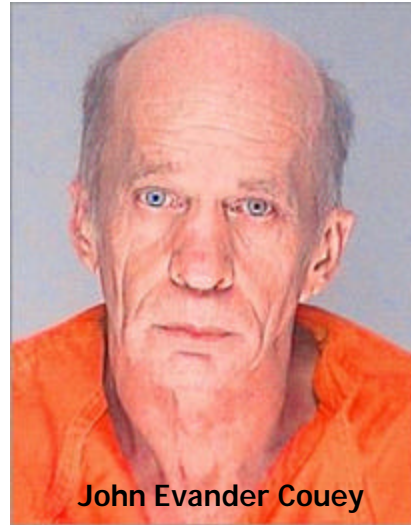
In 1998, the Portsmouth, NH and Keene, NH Police Departments along with the Education Development Center, Inc. of Newton, Massachusetts, were awarded a \$300,000 grant from the Justice Department to combat Internet child sexual exploitation. This grant was awarded by the Justice Department's Office of Juvenile Justice and Delinquency Prevention (OJJDP) under its Internet Crimes Against Children (ICAC) program.

One of their goals was to examine over 260 sexual exploitation cases they were involved with to collect descriptive characteristics of the offenders who had committed sexual exploitation using a computer. The result is the Offender Profile document available online at www.ci.keene.nh.us/police.offender.htm.

This document often shocks parents who don't picture a predator as someone who works with or parents children.

Physical Access is the Goal

- ✂ John Evander Couey was a registered sex offender that was living just 150 yards away from Jessica Lunsford's home.
- ✂ Please check the database of sex offenders in your area. Megan's Law was signed into federal law on May 17, 1996.
- ✂ Access the Megan's Law database from www.ncmec.org
www.fbi.gov/hq/cid/cac/states.htm



John Evander Couey

It is important to acknowledge that luring and abductions happen in the purely physical world as well. Recent cases, such as the Jessica Lunsford case illustrates the need to be aware of sexual predators living near homes and schools. Jessica was abducted from her home by John Evander Couey, sexually assaulted and buried alive in March 2005.

Unfortunately, the online registered sex offender database is typically far from accurate – it is approximately 25% inaccurate in fact. In one neighborhood in California, however, over 50% of the offenders listed were unaccounted for because they had not checked in recently.

On May 17, 1996, President Clinton signed Megan's Law, written in response to the brutal 1994 rape and murder of Megan Kanka. Megan's Law requires sex offender registration and community notification.

US Child Protection Law

United States Code

TITLE 18 - CRIMES AND CRIMINAL PROCEDURE

PART I - CRIMES

CHAPTER 110 - SEXUAL EXPLOITATION AND OTHER ABUSE OF CHILDREN

Section 2251. Sexual Exploitation Of Children

Section 2251A. Selling Or Buying Of Children

Section 2252. Certain Activities Relating To Material Involving The Sexual Exploitation Of Minors

Section 2252A. Certain Activities Relating To Material Constituting Or Containing Child Pornography

Section 2253. Criminal Forfeiture

Section 2254. Civil Forfeiture

Section 2255. Civil Remedy For Personal Injuries

Section 2256. Definitions For Chapter

Section 2257. Record Keeping Requirements

Section 2258. Failure To Report Child Abuse

Section 2259. Mandatory Restitution

Section 2260. Production Of Sexually Explicit Depictions Of A Minor For Importation Into The United States

Every country has some legal restriction on child pornography and child sexual exploitation. Chapter 110 of Title 18 of the US Code addresses child sexual exploitation and abuse.

Visit the Facts by Country section at www.inhope.org for information on the age of consent and legislation issues for numerous countries. This site, www.inhope.org also details issues facing law enforcement in combating child sex exploitation.

Note: Appendix A: Contacts and Resources provides additional international links.

General Internet Safety Tips

1. Place the computer in a central location in the home, not in the kid's room.
2. Learn who your kids are chatting with online (take the "don't talk to strangers" message into the digital world).
3. Define your personal standard regarding your child's privacy.
4. Become familiar with chatting and search tools used by your kids.

Keeping the computer in a central location may alert you to suspicious online activity. Be alert to sudden screen switching when you walk by. Periodically show interest in what your kid is doing online.

Most parents grew up with the "don't talk to strangers" message ingrained in their psyche. That message also applies to the digital world.

How do you feel about tracking your child's online activity? Eavesdropping on your child's online activity could be very harmful to a parent-child relationship that is based on trust. This is an issue that you must resolve for yourself – possibly in an open forum with your child. Some parents feel justified looking into their child's online activity after setting up a background image that states "We may periodically examine or track your online activity as it relates to your safety. If you feel uncomfortable or threatened by any online activity, please turn off the monitor and come talk with us immediately."

Basic awareness of the tools your child uses online may help alert you to potential dangers. For example, knowing the type of content that may be found at www.myspace.com might cause you to rethink your 11-year old child's access to that site.

Advice for Parents

- **Detective James McLaughlin, Child Sexual Abuse and Exploitation, Keene Police Department**

1. Know who is most “at risk.”
2. Set up an agreement with your child about computer use (hours, access to chat lines, revealing personal information/photographs)

These next two pages include parental advice defined by Detective James McLaughlin who has worked hundreds of child sex exploitation cases with the Keene Police Department.

Earlier in this presentation we covered the most “at risk” age group (11-14) and we defined some of the characteristics that predators value in potential victims.

Ideally, we want to ensure our children have safe access to all the advantages that the Internet offers. Detective McLaughlin recommends talking with your child about their Internet use and setting up some guidelines related to Internet access hours, chat line use and revealing personal information online.

Advice for Parents

3. Don't rely solely on software to block/filter content.
4. Let your child know that reporting unwanted or suspicious solicitations won't lead to restrictions on computer use.

There are numerous software packages available to block and filter out web sites and content. Many computer-savvy kids know how to thwart these filters. In addition, other computers they access most likely won't have these filtering programs installed.

Teaching kids to recognize online predatory behavior and befriending techniques enable them to protect themselves regardless of the computer they are using.

It is important to maintain an open dialogue regarding online sexual exploitation. It is not the fault of the child that they are being sought out online.

Advice for Parents

5. Know that restricting communications to a specific list of friends may not guarantee safe communications.
6. Be aware of restrictions at other computer locations – school, library, friends' homes.

Online anonymity enables anyone to pose as anyone they wish. Your child may believe they are talking to a kid at another local school, when in fact they are talking with a 43-year old predator located thousands of miles away.

Currently most school children have access to computers at school (in the classroom or in a computer lab or library), at the city libraries and friends' homes. Empowering your kids with the knowledge required to protect themselves enables them to work on a variety of computer systems while following the same guidelines for Internet safety.

Advice for Parents

7. Look for the warning signs of offender manipulation – secretive behavior, histories being deleted, unexplained telephone charges, hang-up calls, unexpected mail, indications that the home is under surveillance.
8. Know how to monitor Internet use in a variety of ways.

It is imperative that parents pay attention to their child's behavior – there are several warning signs of offender manipulation:

- Secretive behavior such as switching the computer screen whenever someone walks near the computer
- Histories and cache (data saved in computer memory) being deleted so you can't tell what web sites they have been visiting
- Unexplained telephone charges may indicate that an off-line communication channel has started between your child and a predator
- Hang-up calls may indicate that your child has given out your home phone number to someone who hangs up when an adult answers the phone
- Unexpected mail may indicate that your child has given out your home address to someone – in some cases, predators have sent print photos of themselves to the child victim's home
- Someone may also begin surveillance on your home if your child has provided your home address – they may track when people come and go from the home to establish a time to meet with your child at your home

Knowing how to monitor your child's Internet use may negatively affect your parent-child relationship. If your child is missing, however, this log information can be vital to law enforcement officers in their efforts to locate them.

Monitoring and Restricting Internet Use

- ✎ Internet Explorer's Content Advisor
- ✎ Content Protect, NetNanny, CYBERsitter, CyberPatrol, Cyber Sentinel, FilterPak, Cyber Snoop, etc.
- ✎ Single Password
- ✎ Cache and history

Internet Explorer's Content Advisor is disabled by default. To enable Content Advisor, select Tools > Internet > Content and click the Enable button under the Content Advisor section. Content Advisor offers four categories where you can set ratings for language (offensive language, profanity), nudity, sex and violence (aggressive violence, natural or accidental violence)

Evaluate the filtering software listed in this slide before implementing it. Keep in mind that these packages can be circumvented by clever computer-savvy kids.

The following lists several filtering software vendors and their web sites:

Content Protect (www.contentwatch.com)	Cyber Sentinel (www.securitysoft.com)
NetNanny (www.netnanny.com)	FilterPak (www.surfguardian.net)
CYBERsitter (www.cybersitter.com)	Cyber Snoop (www.pearlsw.com)
CyberPatrol (www.cyberpatrol.com)	

A single login password may help ensure your child is not on the computer while you are away or not directly supervising their activities.

Examining computer cache and history information can provide a glimpse into your child's Internet travels.

Parental Resources

✍ Often focusing on a particular age group with the following typical grade groupings:

- ✍ **K-3** **Children (age 6-9)**
- ✍ **4-8** **Kids (age 10-14)**
- ✍ **9-12** **Youth (age 15-18)**

As you peruse through the parental resources listed on the following pages, you will notice that they are often divided into three distinct categories by age. You wouldn't present cartoon-based materials to a teenager and you wouldn't scare younger children with the case studies presented in this course.

As you can tell by this listing, the most "at risk" kids are contained in the second category encompassing grades 4 through 8 (ages 10-14).

We recommend that you review the sites listed on the following pages to get a general feel for the target age group. Be sure to fully review online classes and materials before providing them to your child.

www.NetSmartz.org

✎ Created by the National Center for Missing and Exploited Children (NCMEC)

✎ Age-grouped materials for K-3, 4-8 and 9-12

✎ Age-grouped pledge sheets for online use



 (see www.netsmartz.org/education/ut/)

NetSmartz was founded by the National Center for Missing and Exploited Children (NCMEC). This site has numerous presentations and resources available for online viewing.

You can also download the **I-360** presentation set online from www.netsmartz.org/education/ut/ enabling you to review the course materials offline.

I-360 contains the following courses:

- Amy's Choice (teen who was lured)
- Tracking Teresa (tracing back from a chat session)
- Angela's Experience (online bullying)
- Keisha's Crime (strange online bullying)
- Damon's Game (online racism)
- Online Shopping (online scams; credit card fraud)
- Downloads (copyright infringement)
- Research & Citing Sources (plagiarism)
- Online Gambling (online gambling laws)
- Internet Use Tips (hints to avoid being a financial victim)

Note: In the I-360 program, you must open and view the courses in a specific order. Once you have completed going through all the materials you can visit them again in any order as long as you use the same login name.

www.NetSmartz.org

✍ **Julie's Journey:** Julie left home for three weeks with a convicted murderer she had developed a relationship with online.

✍ **Amy's Choice:** At 15, Amy left home to meet in person with a man she first met online. You can also read "Amy's Story" as told by her mother.



Tracking Teresa: Even though Teresa has tried not to reveal personal information online, she's left enough clues that she could find herself in danger.

Each of these presentations is geared toward a teenage and adult audience.

We recommend Tracking Teresa for non-technical and technical adults. It is a good example of how kids are traced back from their online comments.

Amy's Choice and Tracking Teresa are available on the I-360 program that you can download from www.netsmartz.org/education/ut.


www.ncmec.org

✍ **National Center for Missing and Exploited Children (NetSmartz was created by the NCMEC)**

✍ **Online safety quiz for adults and children**

✍ **Online terminology listing**

✍ **CyberTipline – www.cybertipline.com**

 **1-800-843-5678**

At www.ncmec.org, check out the “Types of Child Sexual Exploitation” section that provides information on the following:

- Possession, manufacture, and distribution of child pornography
- 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
- Misleading domain names

The CyberTipline is available in the US only.

Note: Appendix A provides a list of International contacts for child sex exploitation information and reporting.

www.livewwwires.com (Intl)
www.webwisekids.org (US only)

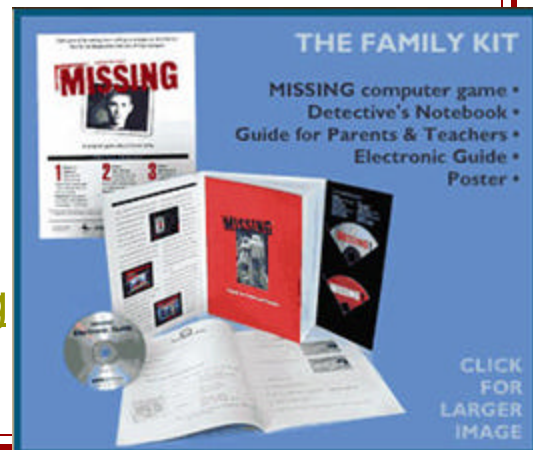
✎ The **MISSING** Game

- ✎ Family kit (single CD)
- ✎ Workshop kit (multiple-CD set)

✎ International orders filled by LiveWires Design

✎ US orders filled at

✎ www.webwisekids.org



Based on a true story, the **MISSING** Game offers kids ages 11-14 a chance to watch as a child, Zack, strikes up a conversation with an online predator. Players learn the six steps to luring and use their investigative skills to help locate Zack's whereabouts when he goes missing.

The Family Kit includes one set of CDs for a single group of players. The Workshop Kit contains 10 CD sets and is designed to be run in a moderated setting, such as a computer lab.

Officer Kim Mercer of the San Francisco Police Department and the Internet Crimes Against Children (ICAC) Task Force has moderated numerous **MISSING** Game labs in various schools. The game was very well-developed and contains a variety of activities to attract a large age range.

www.iSafe.org

- ✍ Designated as a non-profit and formed in 1998 to bring internet safety and education to the youth of the US
 - ✍ Classroom curriculum
 - ✍ Community outreach
 - ✍ Youth empowerment program
 - ✍ Visible in all 50 states

i-SAFE America, referred to typically as i-SAFE, offers free training courses and curriculum throughout the United States. In addition, i-SAFE created *Dig Deeper*, an ongoing series of articles examining the latest Internet safety issues.

i-SAFE's curriculum is designed to support peer-to-peer learning methods. The curriculum is varied and includes subjects such as:

- Cyber Community Citizenship
- Cyber Security
- Personal Safety
- Predator Identification
- Cyber Bullying
- Plagiarism and Theft of Intellectual Property
- Privacy and the Internet
- Malicious Code
- Technology and the Computer Virus

i-SAFE offers courses and support for local Community Action Teams who are involved in raising awareness of Internet safety issues in their local communities.

www.ChildQuest.org



- ✍ Child Quest has assisted in the safe return of over **2,900** individuals. They are recognized by local and national law enforcement agencies as an important element in the recovery effort.
- ✍ Child Quest maintains an Internet Safety document online. For additional information, call CHILD QUEST INTERNATIONAL at (408) 287-4673. Printed booklets, educational materials and learning aids are available.
- ✍ We also highly recommend **Milk Cartons: The Way Back Home** video which addresses predator tactics and child protection methods.

We met personally with the Child Quest group in California and were VERY impressed with their organization. They teach the MISSING game at various schools and are tied in with law enforcement to help recover missing children.

We highly recommend ordering "Milk Cartons: The Way Back Home" video that shows how children can be lured by predators in the physical world.

www.packet-level.com/kids

- ✍ Protocol Analysis Institute **Kids Project**
- ✍ Providing educational resources and presentation materials to parents and leaders for regionalized delivery of Internet Safety for Kids presentations



At the Protocol Analysis Institute, we created the *Internet Safety for Kids* program (also referred to as the *Kids Project*) in March 2005.

Our primary goal is to provide educational resources to support parents and leaders who share information on Internet safety issues in their local communities.

We believe that education serves as the greatest protective force on Internet safety issues relating to children and teens.

Resources online at www.packet-level.com/kids include the slide deck that accompanies this presentation, an audio Train-the-Leader presentation, course description document, instructor-led course invitations, links listing, etc.

Contact us directly at kids@packet-level.com with any questions, comments or suggestions related to this project.

What To Do Now

- ✍ Download and review the presentation material available online at www.packet-level.com/kids
- ✍ Register for and take the online course “Advanced Internet Research and Intelligence” at www.htcia.org – use the techniques to perform reconnaissance on your child

As mentioned on the previous page, the Internet Safety for Kids project materials are available online at www.packet-level.com/kids. If your company would like to host these materials on your website, please contact us at kids@packet-level.com.

The High Technology Crime Investigation Association maintains numerous webcast archives. You may be surprised to learn that your child’s information may already be scattered about the Internet.

What To Do Now

- ✍ Visit the resources listed in this presentation
- ✍ Educate your kids on this issue
- ✍ Consider presenting this information to other parents/educators, etc.
- ✍ Email kids@packet-level.com if you have additional resources

Talking openly with your children about Internet luring and the need to avoid sharing personal information online may help keep them safe online.

We hope you use this information and the materials provided to educate others at school meetings, church gatherings, community center meetings, etc.

We are interested in your feedback and resource information. Contact us directly at kids@packet-level.com.

Thank You

- ✍ If you have received a course survey form, please fill it out and return it to the presenter

Thank you very much for your time.

If you read this material as part of a course, please fill out the course survey form and return it to the presenter.

If you have taken the audio or video course online at www.packet-level.com/kids, please fill out the online or downloadable course evaluation forms and return them to us (instructions are printed on the downloadable course evaluation forms) so we may improve this material further in accordance with your feedback.

Appendix A: Contacts and Resources

General Resources

American Library Association

www.ala.org/cipa

Calgary Police Service

<http://www.calgarypolice.ca/crimeprev/frame1.html>

Child Lures Prevention

www.childlures.com

The Children's Partnership

www.childrenspartnership.org

Counter Pedophilia Investigative Unit

www.cpiu.us

Crimes Against Children Research Center

<http://www.unh.edu/ccrc/>

Cyberlaw Enforcement Organization (affiliated with Wired Safety)

www.wiredcops.org

CyberSmart

www.cybersmart.org

Detective James McLaughlin

Child Sexual Abuse and Exploitation Agent

Keene County Police Department

www.ci.keene.nh.us/police/task_force.htm

Disney

<http://disney.go.com/surfswell/index.html>

DMOZ Open Directory Project (*Note: This link offers several additional sites for internet safety directed specifically at kids and teens).

http://dmoz.org/Kids_and_Teens/Computers/Internet/Safety/

Enough is Enough

www.enough.org

www.protectkids.com (sister site to EIE)

Family Trusted

www.familytrusted.com

Federal Bureau of Investigation Crimes Against Children

<http://www.fbi.gov/hq/cid/cac/crimesmain.htm>

Federal Bureau of Investigation State Sex Offender Registry List
<http://www.fbi.gov/hq/cid/cac/states.htm>

GetNetWise
www.getnetwise.org

High Technology Crime Investigation Association (HTCIA)
Internet Safety for Children Program
www.htcia.org/isfc

Internet Keep Safe Coalition
www.ikeepsafe.com

i-SAFE America
www.isafe.org

Kidz Privacy sponsored by The US Federal Trade Commission
<http://www.ftc.gov/bcp/online/edcams/kidzprivacy/index.html>

Laws Concerning the Exploitation of Children (NCMEC)
http://www.ncmec.org/missingkids/servlet/PageServlet?LanguageCountry=en_US&PageId=1481

LiveWires Design, LTD
www.livewwwires.com

Media Awareness Network
http://www.media-awareness.ca/english/parents/internet/safe_passage_parents/

Megan's Law
www.meganslaw.ca.gov

National Center for Missing and Exploited Children (NCMEC)
www.ncmec.org
www.netsmartz.org
www.cybertipline.com

The Office for Victims of Crime
<http://www.ojp.usdoj.gov/ovc/welcovc/welcome.html>

The Internet Safety for Kids Project
The Protocol Analysis Institute, LLC
www.packet-level.com/kids

Perverted-Justice
www.perverted-justice.com

SafeKids.com
www.safekids.com

SafeTeens.com
www.safeteens.com

Safer Use of Services on the Internet (SUSI)
www.besafeonline.org

U.S. Dept of Justice Internet Crimes Against Children (ICAC)
www.ojp.usdoj.gov/ovc

U.S. Immigration and Customs Enforcement (ICE)
Operation Predator Division
www.ice.gov/predator

Web Wise Kids
www.webwisekids.com (works with Livewires and the **MISSING** Game)

Wired Safety (affiliated with www.wiredcops.org)
www.wiredsafety.org

World Kids Network
<http://worldkids.net/school/safety/internet/>

International Sites

Chatdanger – Kids interactive site - Produced by Childnet International
www.chatdanger.com

Childnet International
<http://www.childnet-int.org/>

Child Quest International Inc.
www.childquest.org

ECPAT - End Child Prostitution, Child Pornography and Trafficking of Children
for Sexual Purposes
<http://www.ecpat.net/eng/index.asp>

NetAlert - CyberSafe Schools
www.netalert.net.au/schools
www.cyberquoll.com.au – Kids interactive site Produced by NetAlert
www.nettysworld.com.au – Kids interactive site Produced by NetAlert

NetSafe – The Internet Safety Group
www.netsafe.org.nz

ThinkUknow
<http://www.thinkuknow.co.uk/home.htm>

United Nations Educational, Scientific and Cultural Organization
http://www.unesco.org/webworld/highlights/innocence_010799.html

Virtual Global Taskforce
<http://www.virtualglobaltaskforce.com/>

International Hotlines

ABA in Australia
<http://www.aba.gov.au/>

ACPI in Spain
<http://www.protegeles.com/>

AFA Point de Contact in France
<http://www.pointdecontact.net/>

Barnaheill in Iceland
<http://www.abotinn.is/barnaheill/index1.htm>

Child Focus in Belgium
<http://www.childfocus.org/>

CyberTipline in USA
<http://www.cybertipline.com>

Freiwillige Selbstkontrolle Multimedia in Germany
<http://www.fsm.de>

Hotline in Ireland
<https://www.hotline.ie/>

Inhope - facilitates co-operation between Internet Hotline providers
www.inhope.org

Internet Watch Foundation in UK
<http://www.iwf.org.uk/index.html>

Jugendschutz in Germany
<http://www.eco.de/servlet/PB/menu/-1/index.html>

Meldpunt in the Netherlands
<http://meldpunt.org/>

Radda Barnen in Sweden
<http://www.rb.se/hotline/index.htm>

Red Barnet in Denmark
<http://www.redbarnet.dk/>

Stopline in Austria
<http://stopline.at>

Internet Chat Lingo/Acronyms

AcronymFinder
www.acronymfinder.com

ComputerUser High-Tech Dictionary
<http://www.computeruser.com/resources/dictionary/chat.html>

National Center for Missing & Exploited Children (NCMEC)
<http://www.missingkids.com/adccouncil/lingo.html>

NetLingo
<http://www.netlingo.com/emailsh.cfm>

Internet Filter Resources

Bsafe Online
www.bsafehome.com

Computer Cop
www.computercop.com

ContentProtect
www.contentwatch.com

CyberPatrol
www.cyberpatrol.com

Cyber Sentinel
www.securitysoft.com

CYBERSitter
www.cybersitter.com

Cyber Snoop
www.pearlsw.com

FilterPak
www.surfguardian.net

Internet Guardian
www.internet-guardian.com

Netmop
www.netmop.com

NetNanny
www.netnanny.com

Parental Guidance
<http://www.parentalguidance.org/>

Safe2Read
www.safe2read.com

Software 4 Parents
www.software4parents.com

Trustworthy Communication, LLC.
www.kidmail.com

Appendix B: Statistics

Between 1998 and 2000, online pedophilia cases dealt with by the FBI rose over 400%

Source: Newsweek

Between 1% and 6% of American men are pedophiles; for unknown reasons, very few women have the disorder.

Source: American Psychiatric Association

Two-thirds of all prisoners convicted of rape or sexual assault committed their crime against a child.

Source: U.S. Department of Justice

Nationally, there were an estimated 2,577 arrests for internet sex crimes against minors in the 12-month period beginning July 1st, 2000.

Source: National Center for Missing & Exploited Children

In 65% of incidents, the youth ran across the sexual solicitation in a chat room, 24% of episodes occurred through instant messages.

Source: Crimes Against Children Research Center

20% of violent offenders serving time in state prisons reported having victimized a child.

Source: U.S. Department of Justice

California's neglected Sex Offender Registry has an error rate that hovers at nearly 25%.

Source: San Jose Mercury News

Studies show that over 17% of convicted sex offenders strike again.

Source: FOX News

The average prison term for those convicted of sexual crimes against children is just over 10 years.

Source: U.S. Department of Justice

67% of offenders convicted of internet-related sex crimes against children were also found to be in possession of child pornography.

Source: National Center for Missing & Exploited Children

Pedophiles tend to chose jobs that put them into constant contact with children.

Source: CrimeLibrary.com

3 out of 10 child victimizers report that they have committed their crimes against multiple victims.

Source: U.S. Department of Justice

An estimated 12% of sexually abused children grow up to become abusers themselves.

Source: USA Today

Between the years of 2002-'03, the number of websites featuring child pornography more than doubled.

Source: National Criminal Intelligence Service

In almost half of the solicitations in the survey, the youth did not tell anyone about the occurrence.

Source: Crimes Against Children Research Center

A survey of 453 pedophiles found that they were collectively responsible for the molestation of over 67,000 children in a 1994 study.

Source: KidSafeNetwork.com

In 1997, an FBI grand jury investigating internet child predators had a list of nearly 4,000 suspects.

Source: CNN

Less than 10% of sexual solicitations were reported to authorities such as a legal agency, an internet service provider, or a hotline.

Source: Crimes Against Children Research Center

Of those imprisoned for crimes against children, 7 in 10 report that they are incarcerated for rape or sexual assault.

Source: U.S. Department of Justice

Sexually victimized children are four times as likely to develop a severe psychiatric disorder, and three times as likely to fall victim to substance abuse as their unmolested counterparts.

Source: American Psychologist

Only 17% of youth and approximately 10% of parents could name a specific authority to which they could make a report (of underage solicitation), although more said they had "heard of" such places.

Source: Crimes Against Children Research Center

Nearly 1,500 Catholic priests have been accused of molesting children since 1994 - just over 2% of the nation's total.

Source: The Washington Post

Criminals who victimize children are nearly 13% less likely to have a prior criminal record than those who commit crimes against adults.

Source: U.S. Department of Justice

Underage females are targets of solicitation at twice the rate of underage males.

Source: Crimes Against Children Research Center

The U.S. Department of Health and Human services estimates that 93,000 children were sexually abused in this country in 1999 alone.

Source: TIME Magazine

Appendix C: Links List

These are the key links listed in the Internet Safety for Kids presentation.

www.ci.keene.nh.us/police/offender1.htm	Offender profile document compiled by the Keene Police Department; recommended review by all parents; lists occupation, involvement with children, age, location and past sex arrests
www.ci.keene.nh.us/police/task_force.htm	Keene Country police department task force on child exploitation; Detective McLaughlin's Advice for Parents; Offender Profile document
www.cybertipline.com	Direct access to the NCMEC CyberTipline for leads relating to child sexual exploitation; phone number is 1-800-843-5678
www.fbi.gov/hq/cid/cac/states.htm	State Sex Offender Registry Web Site entry point; contains links to additional resources relating to child pornography, kidnappings, and federal statutes
www.htcia.org	High Technology Crime Investigation Association – group of law enforcement officers and private citizens working together on high-tech crime issues; webcast archives offer free training (recommended: the Data Mining course)
www.isafe.org	Organization formed to develop and deliver education (K-12) on internet safety and responsible use of the Internet; i-Parent courses and certified instructor program in place
www.livewwwires.com	LiveWires Design – group that developed the MISSING Game (available in family and workshop editions; recommended for ages 11-14) – to order the game within the U.S., visit www.webwisekids.org .
www.ncmec.org	National Center for Missing and Exploited Children (NCMEC) – maintains the CyberTipline for reporting incidents, numerous resource materials and studies online

www.netsmartz.org

NetSmartz Group (sponsored by NCMEC) – provides instruction on Internet safety for a range of age groups; games and quizzes; interviews with teens who have been abducted (Julie’s Journey, Amy’s Choice); visit www.netsmartz.org/education/ut to download the i360 program for off-line viewing of educational materials

www.packet-level.com/kids

Location of the Internet Safety for Kids audio presentation, slide set, handouts, resource list and instructor/parent supplements

www.perverted-justice.com

Perverted Justice Group - Ad-hoc group that poses as underage children in chat rooms to identify predators

This list only covers the key sites mentioned in the Internet Safety for Kids presentation. For additional links and resources, please visit www.packet-level.com/kids.

Appendix D: Instructor Resources

Instructor resources are available online at www.packet-level.com/kids if you want to present this material to other adults. We have included the course information sheet and invitation flyer for your reference.



Internet Safety for Kids - a Presentation for Adults

“1 in 5 children are sexually solicited or approached over the Internet in a one-year period of time.” [Online Victimization: A Report on the Nation’s Youth]

This 1-hour course focuses on Internet risks, predators and advice on making the Internet experience safer for our children.

Topics include:

- Case studies of Internet luring
- Who is most at risk (“The Perfect Victim”)
- How to find if your child’s information is online
- Predator terminology and classifications
- Six steps to luring and befriending techniques
- Chat room tools and logs of predatory communications
- Offender profiles
- Physical access to your child is the goal/Megan’s Law
- US child pornography laws
- General Internet safety tips and advice for parents
- Tips from a sex exploitation unit law enforcement officer
- Internet monitoring and use restriction tools
- Parental resources

This presentation is part of the Internet Safety for Kids (ISK) Program launched by the Protocol Analysis Institute in March 2005. For more information, please visit www.packet-level.com/kids.

Presenter: Laura Chappell, Sr. Protocol/Security Analyst
Protocol Analysis Institute, LLC
Ms. Chappell is a member of the High Technology Crime Investigation Association (HTCIA) and the Institute for Electrical and Electronic Engineers (IEEE). In addition to authoring two best-selling technical books, writing numerous articles on network troubleshooting and security, taping hundreds of hours of self-study courses (“Laura Chappell Master Library”), Ms. Chappell is the mother of two grade-school children. Recently, Ms. Chappell received the Most Innovative Networking Project or Implementation Award from the Network Professionals Association for her work founding the Internet Safety Program.

For more information, please contact kids@packet-level.com.

NOTE: This presentation is for adults only – no children will be permitted to attend due to the graphic nature of the materials.



You are invited to attend a free 1-hour **Internet Safety for Kids - a Presentation for Adults**

"1 in 5 children are sexually solicited or approached over the Internet in a one-year period of time." [Online Victimization: A Report on the Nation's Youth]

Please join us for this free 1-hour course focusing on Internet risks, predators and ideas on how to make the Internet experience safer for our children.

Topics include:

- Case studies of Internet luring
- Who is most at risk ("The Perfect Victim")
- How to find if your child's information is online
- Predator terminology and classifications
- Six steps to luring and befriending techniques
- Chat room tools and logs of predatory communications
- Offender profiles
- Physical access to your child is the goal/Megan's Law
- US child pornography laws
- General Internet safety tips and advice for parents
- Tips from a sex exploitation unit law enforcement officer
- Internet monitoring and use restriction tools
- Parental resources

Time: _____

Date: _____

Location: _____

For more information, contact: _____

NOTE: This presentation is for adults only – no children will be permitted to attend due to the graphic nature of the materials.