

Online Safety: *A Parent's Guide*



Version 7.0 – 8/2010



- Predators will use information obtained from children to gain trust and friendship (*her mother's death*).
- Unless you know someone in person, you don't really know who they are on the Internet (*predator portrayed himself as 18 yr old*).
- Anyone is vulnerable (*father was police officer, lived in small town*).

Kacie Rene Woody was a typical 13-year-old girl. She was a good student, a member of the school band and liked going online. Kacie met 18 year old David Fagan in a Christian chat room for teens. She didn't doubt his identity because the picture posted in David's profile was of a brown hair, blue eye teenage boy. What Kacie didn't know was that David Fagan didn't really exist.

(Click mouse) She was really talking to 47 year old David Fuller. He had used a photo of a nephew in his profile. Fuller was an Internet predator who had set his sights on Kacie. She made the fatal mistake of sharing personal information with him. Fuller tracked Kacie from his home in San Diego, California to the small town in Arkansas where she lived. He abducted and then killed her before committing suicide.

This is a tragic story and we should all learn something from such a tragedy.

(Click mouse)

Predators will use information obtained from children to gain trust and friendship - *When Kacie told Fuller about witnessing her mother's death in a traffic accident, Fuller told Kacie that he had an aunt that lived in Arkansas who had also been in a traffic accident, was in a coma and expected to die soon. This is one way he established a bond of trust and friendship.*

Unless you know someone in person, you don't really know who they are on the Internet. *Fuller portrayed himself as 18 years old and Kacie believed him.*

Anyone is vulnerable - *Kacie's father was a police officer and she lived in small town, but once she logged onto the world wide web, she was no longer just a part of the small community she physically lived in.*

Introduction

- “Food for thought” for parents ... You must decide your strategy.
- Some material may be “unsettling,” but this is unavoidable.
- Philosophy: “Instill a sense of caution, not a sense of fear.”
- The good does outweigh the bad.
- Ask questions ... offer thoughts.



Children need instruction and rules throughout life – including using the Internet. We don't just give our children keys to the car when they are old enough to drive – they receive lessons and learn the rules of the road. The same is true when traveling the information highway – the Internet. Children need instruction and rules in order to proceed safely.

Rules and safety tips are some of the topics we will be addressing.

Targeting Kids Online

How Hard Is It To Target
Kids Online?

- *View Video: Tracking Theresa*

(00:05:08)

© 2010 - NYS Internet Crimes Against Children Task Force

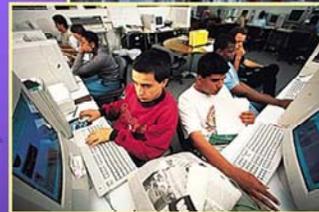
4

Targeting Teresa demonstrates just how easy it can be to track someone online.

Play Video

The Technologies: How do they get there?

- Desktop and laptop computers located at home, friend's homes, work, libraries, stores, schools, "Internet cafes"...wireless connections.
- PDA/BlackBerry.
- Cell phones.
- Internet capable games (i.e., Xbox, Playstation).



Parents need to keep in mind the many different ways that children access the Internet, through computers located outside the home, on cell phones and gaming platforms.

Kids in the U.S.

- 94% of teens aged 12 – 17 use the Internet.
- 84% of online teens have a social networking profile. 46% have open access to their online profile information.
- 84% of teens have cell phones and are texting.
- 43% of teens have been victims of cyberbullying.



Risks Involving Children Are Real

- **Online enticement.**
- **Sexting.**
- **Access by children to pornography.**
- **Distribution of child pornography.**
- **Cyberbullying.**

© 2010 - NYS Internet Crimes Against Children Task Force

7

Along with the ever increasing number of children accessing the Internet, comes the growing number of children at risk to online dangers.

Sexting among teens is on the increase and has had negative consequences that some teens never expected.

Pedophiles and other child exploiters have direct one-to-one access to children online, especially through the use of “blogs” and chatrooms.

Pornography which is legally restricted to adults can easily be accessed by children online.

Cyberbullying is becoming an increasing problem at home as well as at schools.

While there many online risks, such as viruses, identity theft, illegal downloading of materials, these are the three we will focus on.

Online Victimization of Youth: Five Years Later (2006)



- 1 in 7 children (13%) received sexual solicitation or were approached within the last year.
- 1 in 3 (34%) had an unwanted exposure to pictures of naked people or people having sex.
- 1 in 11 (9%) was threatened or harassed.
- 1 in 25 (4%) received an “aggressive” sexual solicitation - A solicitor who: asked to meet them somewhere; called them on the telephone; or sent them regular mail, money or gifts.

© 2010 - NYS Internet Crimes Against Children Task Force

8

A study in 2006 showed that 1 in 7 children received a sexual solicitation or were approached within the last year.

1 in 3 children had an unwanted exposure to pictures of naked people or people having sex. The average age of a child first being exposed to Internet pornography is age eleven.

1 in 11 was threatened or harassed. Unfortunately, very few children ever report this type of experience to a grownup.

1 in 25 received an “aggressive” sexual solicitation. This means it came from someone who actually wanted to meet the child, called them on the telephone or sent them regular mail, money or gifts.

Online Enticement

- Through use of chat rooms, e-mail, instant messaging, "blogs" and even on-line games, adult strangers can establish direct one-to-one access to children.
 - "Distance" and children's natural trust can lead them to forget that these people are strangers ... and many of them are very good at misrepresenting who they are.

- "There was one guy who kept telling me I was beautiful, sexy and hot, and that he wanted to meet me. Even though I kept saying no, he kept giving me his pager number and telling me to call him" (Age 14)



© 2010 - NYS Internet Crimes Against Children Task Force

9

Children make ideal victims because they are naturally curious, they sometimes have a desire to rebel against parents and seek attention and affection.

In a Rochester Institute of Technology Cybercrime study released in 2008, 42% of middle school students surveyed indicated that they had communicated with at least one stranger within the past year.

Who are these people?

DATeline BOOKMARK THIS PAGE | ABOUT THE SHOW | E-MAIL US

On the hunt for Internet sex predators

Respected members of the community have a potentially criminal secret — one involving the possible sexual exploitation of children. What happened to these men after the first 'Dateline' report?



- *View Video: "On Line Sexual Predators - Adults Targeting Children"*

© 2010 - NYS Internet Crimes Against Children Task Force

11

Dateline NBC conducted an undercover investigation into Internet predators. You might be surprised when you learn just who these people are: business professionals, religious leaders, educators, police officers, elected officials, someone's neighbor – people you would never suspect.

Play video.

Where are children going online?



- *View Video: Future Consequences (0:30)*

Children access the Internet through many different types of media, they are posting pictures on Flickr, Skyping, and micro-blogging on Twitter. They are chatting online, IMing, and practically living their lives on Facebook. Let's take a closer look at what this all means.

Chat rooms

- Chat rooms are places on the Internet where you can have live, real-time conversations with many people at the same time.
- Everyone in the chat room can see what everyone else writes, but you can still be as anonymous as you want.



Chat rooms are just one place where sexual predators attempt to lure children.

- **While chat rooms can be dynamic meeting places for people with similar interests:**

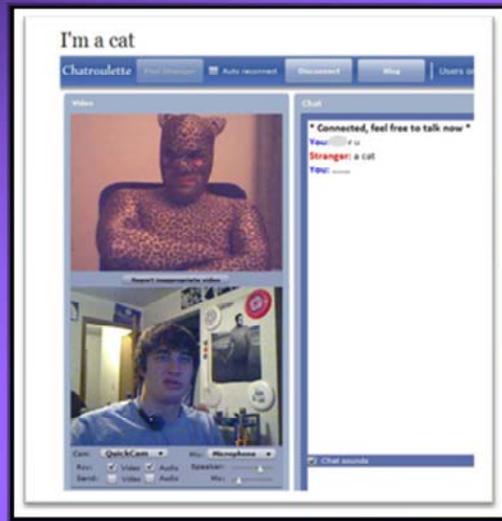
- Children can be easily misled to do things that they ordinarily would not do.
- It is easy for a child to reveal more, sometimes much more, than they should.
- They are cruising grounds for predators.



- If a person unknown to you was speaking to your child in your front yard, what would you do? If your child was communicating with the same stranger on-line, what would you do?

Children's use of chat rooms should be monitored because chat rooms can be "cruising grounds" for predators. Before allowing your child to enter a chat room, you may want to explore the use of an age appropriate, monitored chat room.

Chatroulette



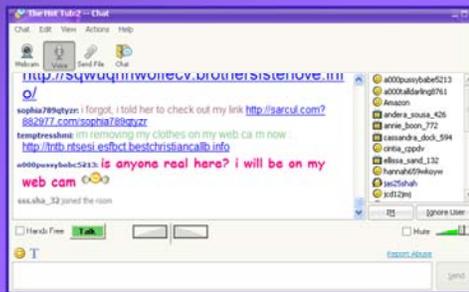
- *View Video: Chat Roulette (5:47)*

Chatroulette is the latest craze on the Internet. Here is a video which provides a better understanding of what Chatroulette is.

Play video.

Instant Messaging (IM).

- IM is a form of Internet communication that combines the live nature of real time chat with the personal contact of email. Benefits include:
 - A safer environment than chat rooms since contact lists can be better controlled.



© 2010 - NYS Internet Crimes Against Children Task Force

16

Instant messaging is a form of Internet communication that combines the live nature of real time chat with the personal contact of email.

One survey indicates that 62% of IM using teens have posted a personalized away message. 28% have listed a phone number where they can be reached in an away message.

- **IM software allows users to create a detailed personal profile including: name, email address, age, home address, phone number, school and hobbies.**
 - If children aren't careful during the sign-up process, they can reveal more than they should.
 - Easy accessible profiles can allow anyone to contact them.
 - Some IM programs offer users the option of joining in chat with strangers.
 - The reach of IM can encourage gossiping and bullying.
 - Children can receive pornographic "spam" through IM.

© 2010 - NYS Internet Crimes Against Children Task Force

17

Children should use instant messaging privacy preferences. For example, allowing only users on their buddy list to contact them, and preventing users from seeing when the child is logged in.

Social Networking Sites.



- "Kids are becoming stars of their own online television reality shows" in front of an audience of millions of Internet users.

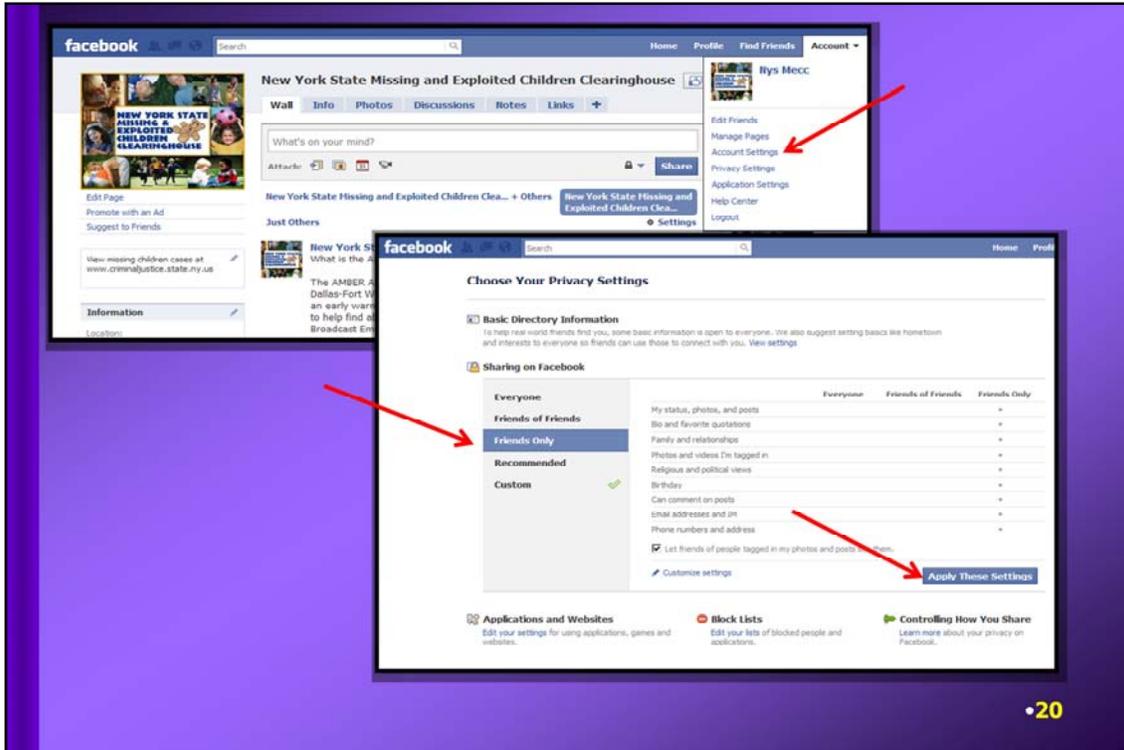
• *View Video "Dateline - MySpace"*

Social networking sites have become a significant part of children's lives. While young children should not use social networking sites at all, teens are going to use them. This is why it is so important for them to be taught how to safely use these sites.

Other social networking sites include – Yahoo 360, Friendster, Bebo, Facebook, Xanga, Melodramatic....

- **A blog is basically a journal that is available on the web - the term is a shortened form of web log.**
 - Blogs are typically updated daily using software that allows people with little or no technical background to maintain the blog.
 - Postings on a blog are almost always arranged in chronological order with the most recent additions featured most prominently.
 - Blogs usually include profiles, text, photographs, and links between “friends” and interests - and may include video or audio files.

Many social networking sites allow children to blog. A blog is basically an online journal. Blogging can allow children to express their thoughts, ideas and creativity, but they must be careful not to reveal too much personal information and to protect their reputation. This is important because many colleges and employers now conduct online searches of prospective students and employees. The consequences of inappropriate blogging could negatively effect a persons academic or career future.



To make your Facebook viewable to friends only, do the following:

1. Click on Account.
2. Click on Privacy Settings.
3. Choose Friends Only.
4. Click on Apply These Settings.

Message Boards

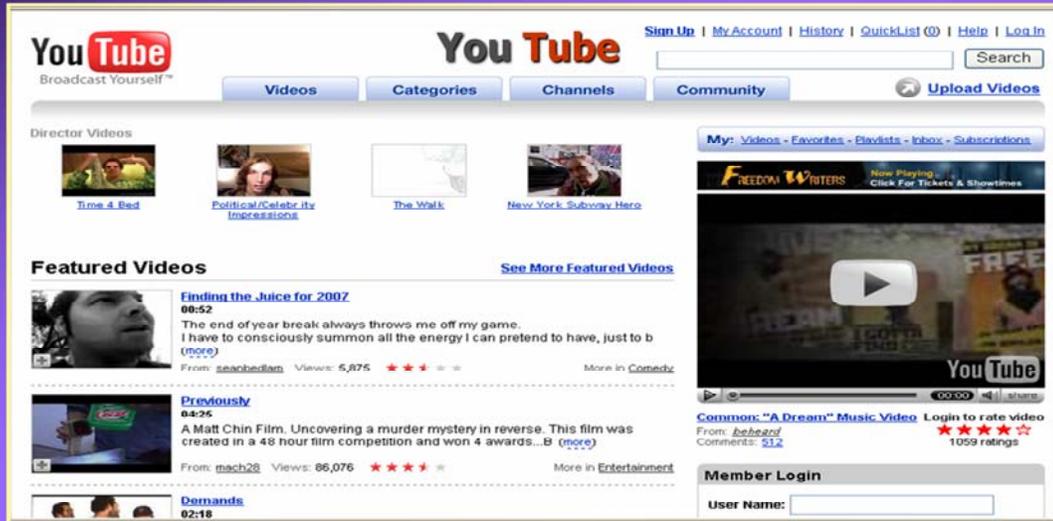


© 2010 - NYS Internet Crimes Against Children Task Force

21

Many people believe they can be anonymous on message boards, but there are plenty of creepy losers out there who have the skills and time to figure out who you are, and then harass and make your life very difficult. Teens should be cautious of what and where they are posting on message boards. Also, beware of the many scams published on messages boards. Unfortunately, there are many messages and ads that try to take advantage of people.

Video Networking



© 2010 - NYS Internet Crimes Against Children Task Force

22

Video networking has become very popular. It is important for parents to be aware of what videos their children are viewing and posting online.

Video Networking

- **Registration is almost always free.**
- **Identity verification is not always required to become a member – children can access “adult” material.**
- **Graphic and explicit videos – pornography, violence, pedophilia.**
- **Cyberbullying, Internet predators.**

Children can view extremely violent and graphic videos, such as a beheading in Iraq, explicit pornography and after school fights between children.



It is important for children to be careful about the types of text messages, pictures and videos they send over their cell phone. The consequences of sending sexually explicit messages or images can be staggering. Many kids can end up being the target of bullying, harassment and some can even face criminal charges.

Sexting is the sending of sexual messages, pictures, or videos through cell phones. Sometimes sexting is considered child pornography, which is a crime. Even teenagers can be registered as sex offenders for sexting.

•Sexting – Serious Consequences

'Sexting' surprise: Teens face child porn charges
 6 Pa. high school students busted after sharing

By Mike Project
msnbc
update

Top News

Sexting at middle school investi

Mike B

New trouble
By Lauren L

Teens use th
also includ

The trend can be criminal for teens

HENRICO, Va., are investigat
a middle school

Administrator
Henrico found
including some
school, the R
reported Frid

Warrants filed April 1 in Bedford County
investigating threatening text message
officials found two pictures of a partial

Investigators with the Bedford County
them to a second suspect, the warrant
cellphone and investigators found 11

Two cellphones were seized during the

Do your kids know sexting could bring criminal charges?
 Posted: May 6, 2009 09:07 PM EDT
 Updated: May 8, 2009 11:25 PM EDT

By Becky Graham - bio | email | Twitter
 Posted by Sarah Harlan - email

Video Gallery

Two Mason Teenagers Charged In 'Sexting' Case
Third Subject In Case Not Charged

POSTED: 5:21 pm EST March 4, 2009
 UPDATED: 11:35 pm EST March 4, 2009

MASON, Ohio -- Two Mason teenagers were charged Wednesday after nude pictures of their classmates were allegedly found on a cell phone, a practice growing in popularity among teenagers called "sexting."

The Warren County prosecutor's office charged the two juveniles with contributing to the delinquency of a minor, a first-degree misdemeanor.

© 2010 - NYS Internet Crimes Against Children Task Force 25

Listen to this true story: A 14-year-old girl took a nude picture on her cell phone and sent it to a few friends as a joke. Those friends sent it to a few of their friends, and then a few of theirs, until as many as 200 people had seen it. Not only was she humiliated, she was arrested for creating child pornography.

Even if your child is not the one taking the picture, he or she could still be arrested for forwarding it to friends, like six boys were in Massachusetts.



Emily was a student at Eisenhower High School in New Berlin, Wisconsin, a suburb of Milwaukee. Like many girls her age, she had lots of friends on Facebook and was especially popular with the boys. Unfortunately, Emily didn't really exist and was the creation of this boy, (click mouse) 18 year old Anthony Stancl. Stancl had an elaborate scheme where he convinced other boys at Eisenhower High School to send sexually explicit photos of themselves. The boys believed they were sharing the pictures with Emily. Stancl then extorted the boys into sexual acts with him by threatening to circulate the pictures to their families and other students through out the school. Even though the boys did not actually know Emily from school, it was a large school and the perpetrator used a last name that was known at the school. Once a boy would see other kids he knew on "Emily's" friends list, he thought it was okay to accept her friend request. In the end, 39 boys were victimized and seven of them were actually sexually assaulted. Stancl was charged with 12 felonies, he pleaded guilty to two of the most serious charges and the others were dismissed. He was sentenced to 15 years in prison and 13 years of extended supervision.

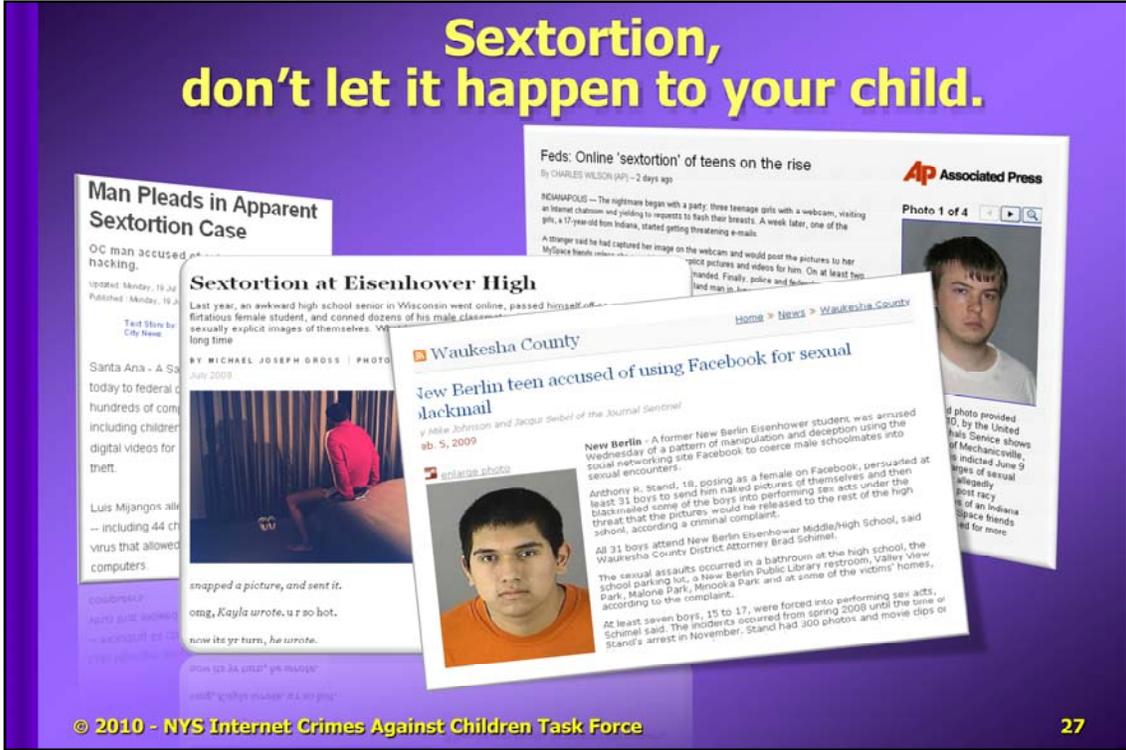
What can we learn about this: it is imperative to talk to children about the dangers of the Internet.

Predators will use information to gain their trust and friendship and then use it against them.

It doesn't matter how long you've known someone online, if you don't know them in real life, you really don't know who they are.

Anyone is vulnerable, boys as well as girls. It can happen in any town, any school and any family.

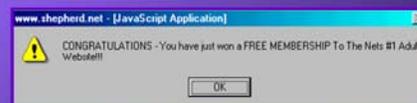
Sextortion, don't let it happen to your child.



Blackmailers using compromising photos attempt to force children and teens to take more explicit photos, perform on webcams, or to actually meet them for inappropriate contact. There have even been cases where hackers have accessed computers through peer-to-peer file sharing sites and using malicious software, obtained photos stored on the computer and other information such as credit cards, websites and accounts. Some have even taken over the computer, activating the webcam without the owners knowledge.

Access by Children to Pornography

- **Pornography which is legally restricted to adults can easily be accessed by children online.**
 - A child who can't browse through a sexually explicit magazine in a store can easily view explicit images and video online.
 - Also, obscene materials which are illegal even for adults can easily be accessed online.



© 2010 - NYS Internet Crimes Against Children Task Force

28

Children accessing pornography online is another concern.

Surveys have indicated that 90% of children age 8 – 16 have viewed pornography online (many while doing homework).

- **Unintentional**

Even “innocent” website addresses can lead directly to pornography.

The screenshot shows a Netscape browser window with the address bar set to <http://www.fun.com/>. The main content area displays a large red "WARNING" and "ADULTS ONLY" text. Below this, it states: "The following site contains nudity and sexually explicit material. You must be 18 years of age or older to enter this site. If you are under 18 or you do not wish to view this explicit material, please leave now." At the bottom of the warning, there are "ENTER" and "EXIT" buttons. To the right of the warning, there is a link to www.teen.com. Below the warning, there is a small icon for "net effect" and a quote: "It is like a car crash. You want to look away but can't." (Age 14)

Children can innocently access a pornographic website. As one teenager said, “It is like a car crash. You want to look away, but can’t.”

URL's (Uniform Resource Locators) ...The incorrect one can take you to a sexually explicit site. How?

- Assumptions
 - You're "certain" that you know the URL
- Mistaken
 - Use of ".com" versus ".org" etc...
- Spelling errors
 - Transposing characters

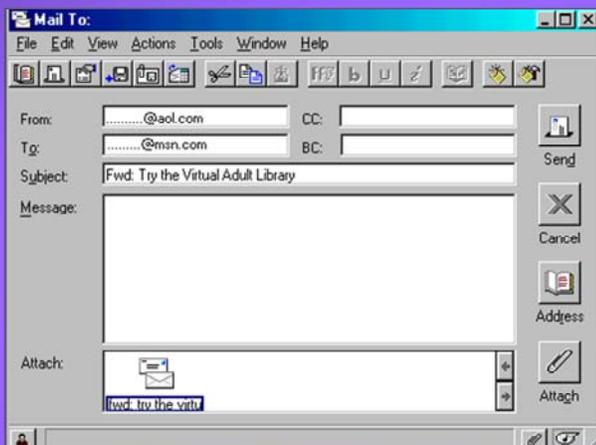


© 2010 - NYS Internet Crimes Against Children Task Force

30

The mistaken use of ".com" versus ".org" or a spelling error can bring a child to a pornographic website.

- **Unsolicited “push” pornography and e-mail links are very prevalent and are sent to everyone – including children.**



© 2010 - NYS Internet Crimes Against Children Task Force

31

Adults as well as children receive unsolicited email attempting to redirect them to a pornographic site.

• “Keyword Searches”

- Children using search engines to locate legitimate information can receive links to pornographic sites.



A simple keyword search can bring a child to a pornographic website. There are 26 children’s characters, including Pokeman and Action Man, which are linked to thousands of pornographic websites.

Intentional



Curiosity in children is natural, but learning about sexuality on-line is not usually the best place.



**TO MOST ADOLESCENTS...
THIS IS AN INVITATION.**

Sometimes, accessing online pornography is intentional. Curiosity is natural, but learning about sexuality online is not the best place.

“Porn” Among Top Search Terms for Kids

Top Searches: Teens, Tweens and Under 7s

	Teen (13-18)	Tween (8-12)	7 & Under
1	Youtube	Youtube	Youtube
2	Facebook	Google	Google
3	Google	Facebook	Facebook
4	Sex	Sex	Porn
5	MySpace	Club Penguin	Club Penguin
6	Porn	Youtube.com	Yahoo
7	Yahoo	You Tube	Webkinz
8	Youtube.com	Miniclip	You Tube
9	eBay	Yahoo	Games
10	Wikipedia	eBay	Miniclip

<http://mashable.com/2009/12/19/porn-toddlers/>

It is not surprising that the fourth top search term among kids 8-18 is sex, but what is shocking is the fourth ranked search term for children 7 and under is “porn.”

Distribution of Child Pornography.

- The Internet has provided child pornographers with a powerful and anonymous distribution vehicle.
- Possession and distribution of child pornography is illegal under state and Federal laws.

Spanky the clown arrested on porn charges

From Terry Frieden
CNN Washington Bureau
Tuesday, May 25, 2004 7:40 PM EDT (2246:1647)

WASHINGTON (CNN) — Spanky, a clown with the renowned Ringling Brothers and Barnum & Bailey Circus, has been arrested on charges stemming from a child pornography investigation, law enforcement officials said Tuesday.

Spanky, whose real name is Thomas Allen Riccio, 23, of Jacksonville, Florida, made his first state road appearance Monday in Fayetteville, North Carolina, where he was traveling with the circus, the officials said.



Tech

• Email this story • Subscribe to this newspaper • Sign up for special news

BYRONNE - Updated 12:04 PM ET

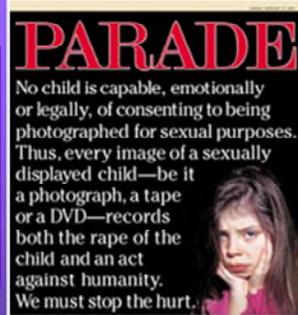
FBI arrests 40 in child porn sting

By Kevin Johnson, USA TODAY

WASHINGTON — Federal authorities investigating an Internet-based child pornography ring have arrested 40 people in 20 states, including two Catholic priests, youth baseball coaches, a civilian law enforcement employee and a teacher's aide, Justice Department officials said Monday.



By Tim Shirk, APF



- *View Video: Dr Sharon (1:47)*

© 2010 - NYS Internet Crimes Against Children Task Force

There are many websites that offer child pornography. Keep in mind, most is traded/sold through non-public “enterprises”, email, etc...

Dr. Sharon summarizes the pornography risks for us.

Play video.

“Cyberbullying” - Any Device, Anytime...



© 2010 - NYS Internet Crimes Against Children Task Force

36

Cyberbullying has rapidly become a problem that is difficult to deal with. Technology now allows for bullying at any time, any place.

- **There are several ways that children threaten and/or harass others online. They may:**

- Send e-mails or instant messages containing insults or threats directly to a person.
- Spread hurtful comments about a person to others through e-mail, instant messaging or postings on web sites and blogs.
- Steal passwords and send out threatening e-mails or instant messages using an assumed identity.

School suspends 20 over MySpace posting

Calif. middle-school student faces expulsion over alleged threat on Web site

Cyber bullying can happen in several ways; through email or instant messages sent directly to a child, hurtful comments sent or posted about a person or assuming a person's identity.

One third of online teens report writing a comment in IM that they wouldn't say to someone's face.

- Build web sites, often with password protection, to target people - students or even teachers.
- Increasingly, kids are being bullied by text messages sent through their cell phones.
- Built-in digital cameras in cell phones have added a new dimension to the problem.

WELCOME TO THE PAGE
THAT MAKES FUN OF
DAVE KNIGHT

"A kid from school sent me a message on the Internet saying, 'Hey Dave, look at this website'" says David. "I went there and sure enough, there's my photo on this website saying 'Welcome to the website that makes fun of Dave Knight' and just pages of hateful comments directed at me and everyone in my family."



© 2010 - NYS Internet Crimes Against Children Task Force

38

Build web sites, often with password protection, to target people - students or even teachers.

Increasingly, kids are being bullied by text messages sent through their cell phones.

Built-in digital cameras in cell phones have added a new dimension to the problem. There have been many reported instances of children taking pictures of classmates in the locker room shower and distributing the photo throughout the school.

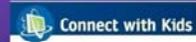
Consequences of Cyber Bullying!



From hurt feelings to...suicide.

View Videos: Ryan Halligan's Story and Ryan Halligan's father speaks with teens

© 2010 - NYS Internet Crimes Against Children Task Force



39

Unfortunately, the consequences of cyber bullying can range from hurt feeling to suicide.

- **Possible warning signs of children being bullied or bullying other children.**

- Complaining that other children or a group of children do not like them.
- Preoccupation with friendship concerns.
- Poor self-esteem. Feeling they are not as good as others.
- Not wanting to go to school or other activities.
- Spending a great deal of time on the computer.
- Being secretive about online activities.

Parents should be aware of possible warning signs that a child is being bullied or is bullying other children.

- Complaining that other children or a group of children do not like them.
- Preoccupation with friendship concerns.
- Poor self-esteem. Feeling they are not as good as others.
- Not wanting to go to school or other activities.
- Spending a great deal of time on the computer.
- Being secretive about online activities.

- Lacking interest and involvement with other kids.
- Acting like their group (clique) is superior.
- Bragging that they use the Internet to play practical jokes or steal other kids' passwords as a joke.
- Continuing to make fun of other kids.
- Getting in trouble at school or in the community for inappropriate computer use.

Adapted from Powertolearn.com

- Lacking interest and involvement with other kids.
- Acting like their group (clique) is superior.
- Bragging that they use the Internet to play practical jokes or steal other kids' passwords as a joke.
- Continuing to make fun of other kids.
- Getting in trouble at school or in the community for inappropriate computer use.

• Dealing with Cyberbullying

- Preserve evidence – this is crucial for identifying the bully and making a case.
- Attempt to enlist assistance from the service provider.
- If able to identify the bully, contact him or her and/or parents.
- Use available blocking technology (i.e., block the user on IM, email and chat.)
- In serious cases, seek assistance from the police (i.e., threats of physical harm, unrelenting or unable to stop.)

© 2010 - NYS Internet Crimes Against Children Task Force

42

Here are some tips for parents on how to deal with cyber bullying.

Preserve evidence – this is crucial for identifying the bully and making a case.

Attempt to enlist assistance from the service provider.

If able to identify the bully, contact him or her and/or parents. Contacting the bully or parent is a judgment call, if you are unfamiliar with the family, perhaps you should contact your child's school to ask for assistance.

Use available blocking technology, for example block the user on IM, email and chat.

In serious cases, seek assistance from the police, especially if anyone ever physically threatens a child.

So... What Should Parents Do?



We have talked about several online risks for children. So what should parents do? Immediately “pulling the plug” is probably not the answer. Teaching children rules and proper netiquette is very important.

1. Learn everything you can about computers, the Internet and related technology -

- Develop and maintain proficiency through use.
- Ask children to demonstrate.

2. Communicate with your children.

- Take time to discuss concerns; agree on ground rules.
- Understand their needs.
- Set reasonable expectations.

3. Place the computer in a “well-trafficked” area, not a child’s bedroom or a secluded area.

© 2010 - NYS Internet Crimes Against Children Task Force

44

As a parent learn everything you can about computers, the Internet and related technology, including hardware, software and terminology, misuse and risks, and tools such as filtering software, browser settings and “reliable” websites.

Communicate with your children. Try to understand their needs, interest and curiosity. Be trusting and set reasonable expectations. Be specific about your expectations. For example, acceptable websites, selection and use of chat rooms, “buddies,” divulging personal information, and time limits. Ensure that your expectations are respected; take appropriate action if they are not.

Place the computer in a “well-trafficked” area. Have the monitor facing out, so that when you walk past, you can see the activity on the screen.

4. Ensure that they do not divulge detailed personal information when completing “profiles” and minimize dissemination.

5. Keep ALL accounts in your name.

6. Know your child’s password(s) and screen name(s).

- Ensure that screen names do not provide information about his or her identity (e.g., Sarahsweet16.)



The screenshot shows a web form titled "Create a Screen Name" with a "Help" link. It includes a note: "* Indicates a required field". The form has four main input fields: "Desired Screen Name" (with a note: "3-16 letters or numbers. It must start with a letter."), "Password" (with a note: "4-16 letters or numbers. [Help](#) for creating a secure password."), "Re-Type Password", and "Display Name" (with a note: "This is the way you are greeted each time you sign in.").

Ensure that they do not divulge detailed personal information when completing “profiles” and minimize dissemination.

Teach children to protect their “online” reputation.

It is very important to keep accounts in your name, not the child’s. For example, time is critical in the case of a missing child. If accounts are in your child’s name, police are required to obtain a subpoena to access the accounts.

Know your child’s passwords and screen names. Ensure that screen names do not provide information about his or her identity.

7. Consider Use of Computer/Internet Management Software:

- Age-based access levels – Allows for various levels of access for different family members.
- Filtering and Blocking (incoming and outgoing.)
- Time Restrictions.
- Activity Logs - Parents can view logs that list web sites visited, web sites blocked, chat sessions... Software can even capture screen shots and email messages to you if a rule is violated!



- "Girls are aware of the varied dangers of the Internet, but want more proactive involvement rather than prohibitive don'ts from parents."



© 2010 - NYS Internet Crimes Against Children Task Force

46

Consider the use of computer and Internet management software. More specific information on this type of software can be found on the New York State Division of Criminal Justice Services website at www.criminaljustice.state.ny.us.

Monitoring Software Information

TopTenREVIEWS™
We Do the Research So You Don't Have To.

Legend:
 ■■■■ Excellent
 ■■■ Very Good
 ■■ Good
 ■ Fair
 □ Poor

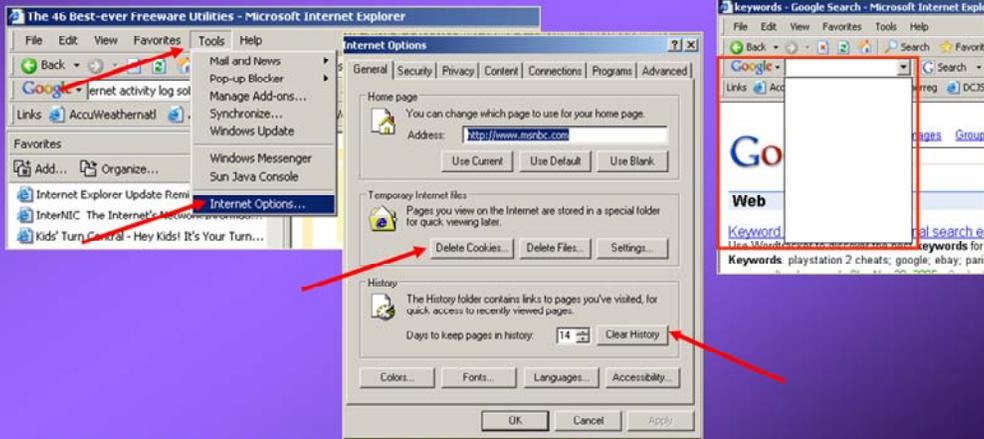
Rank	1	2	3	4	5	6	7	8	9	10
Product	Spector Pro	SpyAgent	ImageBrother	eBlaster	Golden Eye	Coachman Monitor	Invisible Keylogger	007 Spy Software	Spy Buddy	Keylogger Pro
Reviewer Comments	READ REVIEW	READ REVIEW	READ REVIEW	READ REVIEW	READ REVIEW	READ REVIEW	READ REVIEW	READ REVIEW	READ REVIEW	READ REVIEW
Lowest Price	BUY \$99.95	BUY \$79.95	BUY \$29.95	BUY \$99.95	BUY \$29.95	BUY \$39.95	BUY \$39.99	BUY \$39.95	BUY \$69.99	BUY \$39.99
Overall Rating	■■■■	■■■■	■■■■	■■■■	■■■■	■■■■	■■■■	■■■■	■■■■	■■■■
Ratings										
Feature Set	■■■■	■■■■	■■■■	■■■■	■■■■	■■■■	■■■■	■■■■	■■■■	■■■■
Ease of Use	■■■■	■■■■	■■■■	■■■■	■■■■	■■■■	■■■■	■■■■	■■■■	■■■■
Ease of Installation/Setup	■■■■	■■■■	■■■■	■■■■	■■■■	■■■■	■■■■	■■■■	■■■■	■■■■
Monitoring Effectiveness	■■■■	■■■■	■■■■	■■■■	■■■■	■■■■	■■■■	■■■■	■■■■	■■■■
Help/Documentation	■■■■	■■■■	■■■■	■■■■	■■■■	■■■■	■■■■	■■■■	■■■■	■■■■
RECORDING/LOGGING										
Keystroke Recording	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Web Surfing Recording (HTTP)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Chat Messenger Recording	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
File Transfer Recording (FTP)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
P2P Download Recording	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Email Logging	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓

© 2010 - NYS Internet Crimes Against Children Task Force

47

TopTenReviews.com can be helpful when deciding what type of monitoring software to use. The brand, features and price are provided for comparison.

8. Periodically review Internet bookmarks, history files, temporary Internet files and keyword searches. Also ... what can it mean if history, keyword or temporary Internet files are cleared?



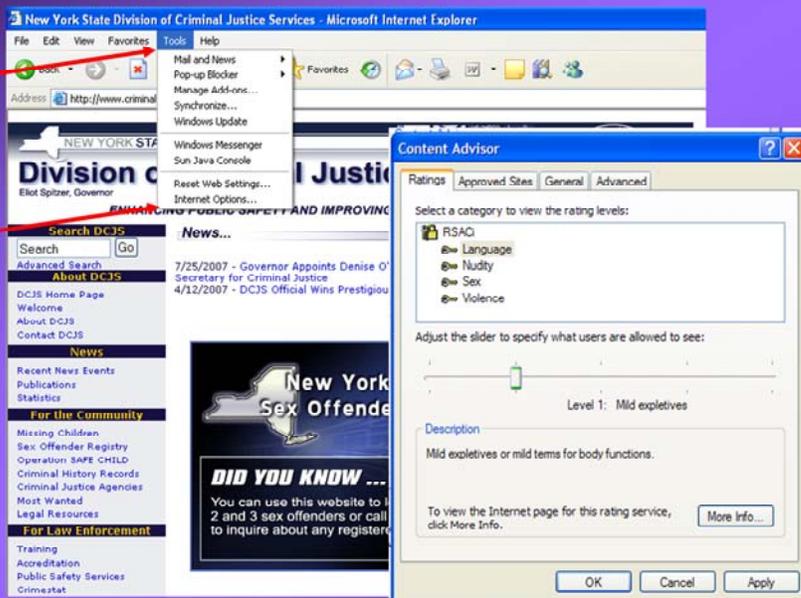
© 2010 - NYS Internet Crimes Against Children Task Force

48

Periodically review Internet bookmarks, history files, temporary Internet files and keyword searches. Also ... what can it mean if history, keyword or temporary Internet files are cleared?

Perhaps the child is trying to stay one step ahead of mom and dad?

Set Parental Controls



Use available parental controls on computers, cell phones and gaming platforms.

Acronyms, Text Shorthand and Emoticons



View Video: "My bff jill" (0:20)

netling.com

noslang.com

acronymfinder.com

© 2010 - NYS Internet Crimes Against Children Task Force

50

If you are finding it difficult to understand your child due to their use of acronyms and other online slang, netling.com, noslang.com and acronymfinder.com may be useful resources for you.

Blogs, IM, Chatrooms, Email: What is reasonable?

- **Under 8** - Children shouldn't be using IM, chat rooms or blogs - period. Email should be restricted to only approved senders.
- **8-10** - If you add IM or chat, make sure only pre-approved senders can send to your child. No blogs!
- **10-12** - Give them more privacy, as long as it is with people you trust. Block all but pre-approved senders. Still no blogs!



© 2010 - NYS Internet Crimes Against Children Task Force

51

When it comes to instant messaging, chatrooms and email, what is reasonable?

Under 8 - Children shouldn't be using IM, chat rooms or blogs - period. Email should be restricted to only approved senders.

Ages 8-10 - If you add IM or chat, make sure only pre-approved senders can send to your child. No blogs!

Ages 10-12 - Give them more privacy, as long as it is with people you trust. Block all but pre-approved senders. Still no blogs!

- **13-15** - Respect their privacy even more. Give them more leeway regarding IM, e-mail, chat and blogs. But check and account for everyone, in real life, on their buddy lists. No friends of friends!
- **16 and over** - Parental involvement becomes difficult at best – if good judgment and communication have not been firmly established by now ... all bets are off.
 - If they have earned your trust, give it to them.
 - If not, unplug the computer and take away their cell phones and interactive gaming devices.

Teens 13-15 - Respect their privacy even more. Give them more leeway regarding IM, e-mail, chat and blogs. But check and account for everyone, in real life, on their buddy lists. No friends of friends!

Age 16 and over - Parental involvement becomes difficult at best – if good judgment and communication have not been firmly established by now ... all bets are off.

If they have earned your trust, give it to them.

If not, unplug the computer and take away their cell phones and interactive gaming devices.

- **Warning signs. Elevate concern if your child:**

- Significantly increases on-line time.
- Receives phone calls, email, mail or packages from someone you don't know.
- Quickly exits IM, chat, email, websites and other activities when you are near.
- Increases use of new slang words, inappropriate sexual knowledge, withdraws from family and friends.
- Begins using new screen names, an online account belonging to someone else, etc.
- Is reluctant to discuss activities or your concerns.

© 2010 - NYS Internet Crimes Against Children Task Force

53

Be aware of warning signs.

Elevate your concern if your child:

- Significantly increases on-line time.
- Receives phone calls, email, mail or packages from someone you don't know.
- Quickly exits IM, chat, email, websites and other activities when you are near.
- Increases use of new slang words, inappropriate sexual knowledge, withdraws from family and friends.
- Begins using new screen names, an online account belonging to someone else, etc.
- Is reluctant to discuss activities or your concerns.

Remember that good communication between you and your child is the best defense to your child's safety.

Always Keep In Mind ... The "Good" Really Does Outweigh The "Bad!"



© 2010 - NYS Internet Crimes Against Children Task Force 54

Even though we have talked about a lot of negative aspects of the Internet, it is important to remember that there are many good websites. The Internet is a great educational and communication tool. It is up to us as parents, teachers, and law enforcement to show children how to find the good things and avoid the bad. One way to teach them how to be safer online is to teach them the "4 R's".

Teach Children to Remember the 4 R's ...

- **Recognize** techniques used by online predators to deceive their victims.
- **Refuse** requests for personal information.
- **Respond** assertively if you are ever in an uncomfortable situation while online. Exit the program, log off or turn off the computer...
- **Report**, to a parent or other trusted adult, any suspicious or dangerous contact that makes you uncomfortable.

The New York State Internet Crimes Against Children (ICAC) Task Force

- Established in 1998 in response to the rapidly escalating problem of Internet crimes involving children.
- Formally combined efforts of the New York State Police, NYS Attorney General's Office, NYS Division of Criminal Justice Services and regional affiliates.
- It is one of over 50 nationwide, which has strengthened information sharing between police agencies.



- Efforts:

- The New York State Police conduct well coordinated investigations and forensic examination of computers seized as evidence.
- The NYS Attorney General prosecutes or assists with the prosecution of offenders.
- NYS DCJS is responsible for providing training and education to both the public and law enforcement.

Your kids can fill in the blanks. Can you?

LOL: laughing out loud
BRB: _____
MUSM: _____
A/S/L: _____
BF: _____
TAW: _____
LULAS: _____
POS: _____
WTGP: _____?
LMIRL: _____

Protect your child's online life.
HOOP: help delete online predators

To learn more, visit
www.criminaljustice.state.ny.us/rttraining/index.htm
www.nysaog.edu
www.NetSmartz.org

To report an incident, call 1-877-434-6263, 1-800-NY-4953 or visit cyber.tipsline.com





NYS Internet Crimes Against Children Task Force

www.nysicac.org

1-877-474-KIDS (5437)

nysicac@troopers.state.ny.us

**NYS Division of Criminal Justice Services
Missing and Exploited Children Clearinghouse**

www.criminaljustice.state.ny.us

1-800-FIND-KID (346-3543)

missingchildren@dcjs.state.ny.us