



Empowering young people to be safe on the Internet

Information for parents, teachers and community members



Celebration of Service

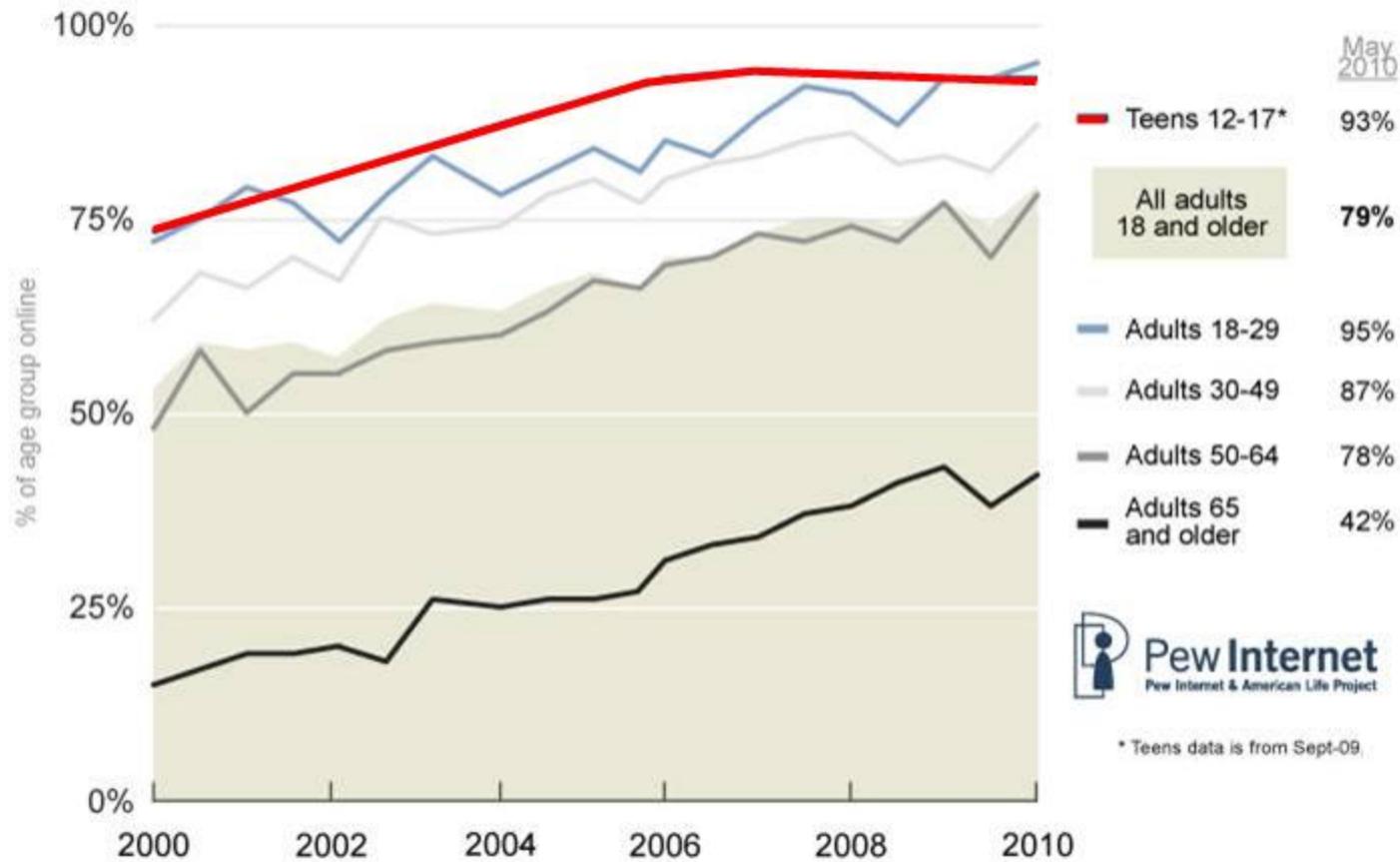
Empowering parents, teachers, & community members

- IBM is providing the following information only as an introduction to Internet safety.
- You should decide what other resources you need to help make children's Internet use a safe and enjoyable experience.

Developed in partnership with the Center for Technology, Innovation, and Community Engagement at the Columbia University School of Engineering and Applied Science



Change in Internet usage by age, 2000-2010



Generational differences in online activities

Activity	Online Teens (12-17)	All Online Adults
Use e-mail	73%	91%
Get news	63%	70%
Buy something online	38%	71%
Use social networking sites	65%	35%
Watch videos online	57%	52%
Send instant messages	68%	38%
Play games online	78%	35%
Read blogs (online diaries)	49%	32%
Download music	59%	37%

Internet safety: More important than you think!

- Earlier studies raise concerns:
 - In 2005, one in seven children who used the Internet had been sexually solicited. *Internet Filter Review*
 - In 2006, 79% of unwanted exposure to pornography by youth occurred in the home. *Online Victimization of Youth: Five Years Later*
- Now, 39% of teens have posted something online that they later regretted. *Common Sense Media, 2010*



What young people are doing online

- 64% of all teens say that they do things online that they would not want their parents to know about. *Berkman Center, Harvard University, 2008*
- A Girl Scouts' survey found that teen girls believed they could do the following without their parents' knowledge:
 - Chat in a chat room (86%)
 - Carry on a cyber romance (54%)
 - Set up a meeting with someone they met online (46%)
 - View a pornography site (42%)
- In a 2008 Harris Interactive-McAfee survey, 63% of teens said they know how to hide what they do online from their parents.
- 32% clear their browsing history.
- 16% have created private e-mail addresses or social networking profiles.
- 28% use code words on a daily basis.

What it takes to keep children safe

FACT: Advanced computer skills *are not required* to understand Internet safety! All it takes is three simple things:

1. Basic knowledge of how the Internet is used today
2. A good understanding of the Internet's dangers
3. Some old-fashioned common sense and open communication



What it takes to keep children safe

FACT: Advanced computer skills *are not required* to understand Internet safety! All it takes is three simple things:

1. **Basic knowledge of how the Internet is used today**
2. A good understanding of the Internet's dangers
3. Some old-fashioned common sense and open communication



More ways to communicate than ever

Popular services that are free of charge:

- Search engines
- E-mail
- Photo- and video-sharing websites
- Chat room and Instant messaging (“IM’ing”)
- Social networking sites
- Online games
- File-sharing networks



Photo- and video-sharing websites

- Users create online “profiles” and post photos and videos directly.
- Users can comment on each other’s photos and videos and send messages to other users directly.
- Most of these websites are moderated and have strict filters for blocking adult content, but comments are often inappropriate.
- Some websites not moderated at all

Chat rooms and instant messaging

Chat rooms and instant messaging are the dominant places where solicitation occurs (77%).

Berkman Center, Harvard University, 2008

■ Chat Rooms

- Real-time conversation
- Chat rooms: Groups of people create profiles and “chat” together.
- Many allow private conversations and video chat via webcams.
- Easy to remain anonymous

Chat rooms and instant messaging

Chat rooms and instant messaging are the dominant places where solicitation occurs (77%).

Berkman Center, Harvard University, 2008

■ **Instant Messaging (IM'ing)**

- Real-time conversation
- When IM'ing, user adds “friends” as contacts, can see when they're online, and chat privately using text, voice, and/or video.
- While more likely that the user knows the person, it's easy to create false IDs.
- Messaging or texting is also popular on mobile phones:
 - U.S. girls aged 14 -17 send and receive more than 3000 texts a month.
Teens and Mobile Phones, Pew Internet, April 2010
 - Mobile text messages can take the form of cyber-bullying, “sexting,” textual harassment, and inappropriate images/videos

Social networking sites

- Create a profile with your real name, school, location, etc.
 - 73% of teens have established online profiles in 2010, up from 55% in 2006. *Common Sense Media, 2010*
- Post status updates and see what other people are up to.
- Many young people post pictures, videos and information that are inappropriate and even harmful to themselves and/or others.
- Places for online predators to lurk

Online gaming networks

- Play multiplayer console games online with others.
 - No computer required – connect your home game console directly to the Internet.
- Prone to cyber-bullying, harassment, and hate speech.
 - According to the Berkman Center at Harvard University, nearly half of game-playing teens hear racist, sexist, and homophobic name-calling and harassment on a regular basis.

File-sharing networks

- Download (or “pirate”) music, movies, and more – sometimes illegally.
- The files are shared directly from “peer to peer” so the download is hard to track.
- However, since most content is copyrighted, both downloading and distributing are illegal.
- Many files contain viruses and pornography, even though they were listed as a song or movie.



Opportunity requires responsibility

- The Internet is an amazing tool giving us unprecedented access to knowledge and communications.
- However, would you let children drive before you gave them lessons?
- On the Internet, those who haven't learned how to be safe are taking needless risks.
- **Challenge:** Narrow the parent/ adult-child “digital divide” and teach children how to use online technologies safely and responsibly.



Parent and student perspectives differ

What parents say

- 49% say their child was 13 or older before they started surfing unsupervised.
- Just 16% think their child has shared information they would not normally share in public.
- 2% say their child has posted naked or semi-naked images of themselves.



What students say

Only 14% of teens say they waited until they were this old. 37% say they started before age 10.

28% of children actually have.

13% of children actually have.

Common Sense Media, 2010

What it takes to keep children safe

FACT: Advanced computer skills *are not required* to understand Internet safety! All it takes is three simple things:

1. Basic knowledge of how the Internet is used today
2. **A good understanding of the Internet's dangers**
3. Some old-fashioned common sense and open communication



Real dangers of the Internet

- Instant exposure to inappropriate material
- Sexual solicitation and Internet-initiated offline encounters
- Online harassment and cyber-bullying



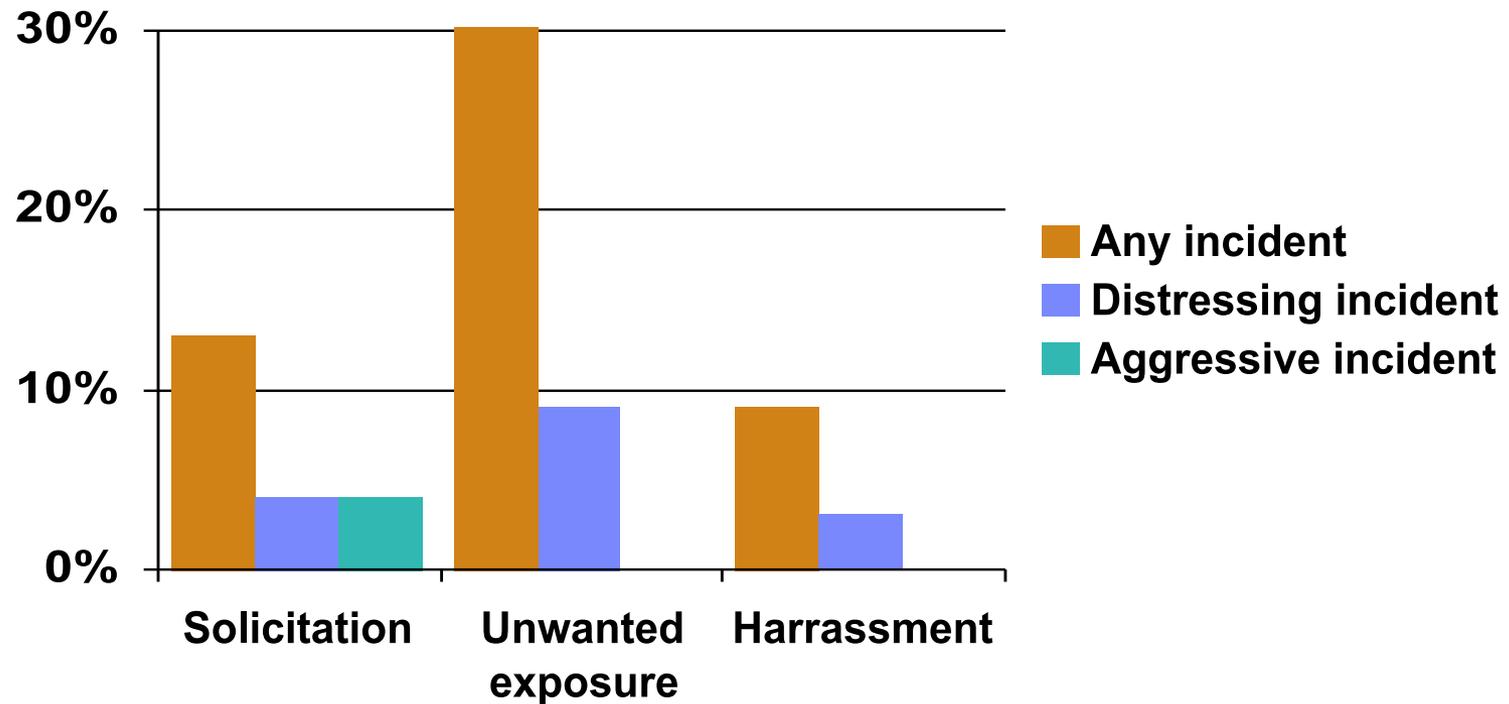
Which children are really at risk?

Every child with Internet access is at risk!



Online victimization

Percent of Internet users 10-17 years



Online Victimization: Five Years Later, Crimes Against Children Research Institute, 2006

Inappropriate material: online pornography

- Pornography can easily be viewed online – by children of any age.
- Adolescents are a large consumer group of Internet pornography.



Inappropriate material: hate sites

- The number of “hate sites” advocating hate or depicting violence rose from 8,667 at the end of 2003 to 11,500 in 2010.
SurfControl, 2004
Simon Wiesenthal Center, 2010
- Internet hate sites are showing up at a faster rate than pornography.



Instant exposure to inappropriate material

- Games and music
 - Many child-oriented sites allow gambling advertisements, and more than 33% of gambling websites have “deficiencies” that allow minors to play.
UK Gambling Commission, 2009
 - When trying to download music illegally, many files are actually pornography.
- Search engines
 - Search words or terms can produce unexpected results, such as pictures and videos, which if unfiltered, can be inappropriate for children.
 - Pornographic sites with commonly misspelled names, including Disney characters.
- E-mail
 - 92% of the world’s e-mail is spam, 2% of which is pornographic, causing many children to receive pornographic spam on a daily basis.
Symantec, 2010

Online predators

True story: 13-year-old Carrie*

- Excellent academics – “straight-A” student
- Very popular
- Captain of her cheerleader team
- Appeared to be a happy, bright, well-adjusted young girl

FACT: 66 percent of online sexual solicitation targets girls.



** Name changed to protect privacy.*

Online predators

True story: Joshua*

- High school student with a close-knit family
- Extremely knowledgeable about computers
- Frequent chat room and Internet forum visitor

FACT: Boys are as likely as girls to be targeted for violence (threats or efforts to humiliate) on the Internet.

** Name changed to protect privacy.*



Online predators: establishing a connection

FACT: Any information that children post online is essentially public, even if they change their privacy settings.

- Suppose a predator searches a social networking site for singles ages 15-21, who are near his town and looking for a relationship.
- A teenager's profile catches his attention, and some basic information is public.
 - The predator notices the teenager shares a few of his favorite movies and bands.
- Suddenly, there's a connection.

Online predators: establishing a connection

FACT: Any information that children post online is essentially public, even if they change their privacy settings.

- Knowing her hometown, he locates her school with the help of a search engine.
 - Now he can find profiles of every student that goes to the school.
- One of the pictures looks like it was taken in the same house as the original girl's picture.
 - This girl must be her good friend.



Online predators: establishing a connection

FACT: Any information that children post online is essentially public, even if they change their privacy settings.

- The predator is right; he sees dozens of posts by the teenage girl on this other girl's "wall."
- Even better, all of the friend's photos are visible to people in the community, so he can look for any photos that include the teenage girl.

Online predators: establishing a connection

- The predator watches all new photos and wall postings for weeks on end.
 - The more he sees of her life, the more he feels like he knows her.
 - He even gets to learn where she will be and when.
- Last Friday she went to the bowling alley with a large group of people.
 - He joins the virtual “group” to see every detail.
- Finally, he makes a move by sending her a friend request.
 - She sees he’s part of the bowling group, so figures he must be safe.
- Now he has her cell phone number, and all of her restricted photos.
 - Just a few weeks ago, he didn’t even know her name!

“Grooming”

- The process used by an adult to gain the trust of a young person for predatory purposes.
- A comprehensive study in 2006 demonstrated that:
 - 40% of all solicitations begin with an instant message.
 - 37% of solicitations took place in a chat room.
 - 70% of victims were girls, and 30% were boys.
 - 81% of the victims were aged 14 or older.

Source: Online Victimization: Five Years Later, 2006

The grooming process

- **1st stage: Appears familiar**
 - Predator disguises true identity and motive for the relationship; pretends to have common interests.
 - Predator's goal is to be non-threatening, friendly, comforting and familiar.
- **2nd stage: Develops trust**
 - Predator exploits natural parent/child friction; always supports child's point of view regarding family conflicts.



The grooming process

■ 3rd stage: Establishes secrecy

- Predator acquires the victim's personal Internet addresses and phone number; victim places the predator on their private e-mail list so that they can "chat" any time.
- Youth victim is convinced that parents won't understand the "special" relationship.

■ 4th stage: Erodes barriers

- The predator lures the child into adult conversations; the child's curiosity is exploited by the predator to erode personal barriers.
- The child-victim begins believing they are ready for adult experiences.



The grooming process

■ 5th stage: Direct intimidation

- The predator uses the child's psychological distance from the parents to intimidate.
- Victims can feel powerless to ask an adult or authority for safety and support.

■ Final stage: Face-to-face meeting

- **FACT:** An survey identified almost 800 cases involving adults traveling to or luring youth they first "met" on the Internet.
- **FACT:** Juveniles themselves made 44% of the solicitations.
- **FACT:** Females made 16% of the solicitations.

Source: Online Victimization: Five Years Later, 2006



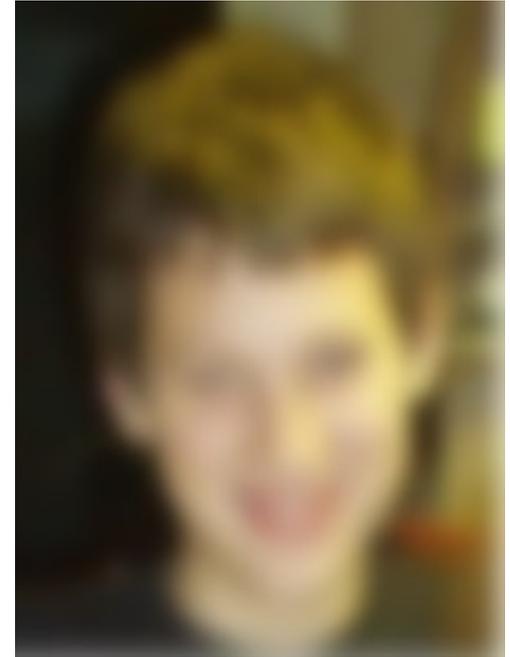
Cyber-bullying

- Up to 46% of young people have been bullied online.
Berkman Center, Harvard University, 2008
- Earlier studies show that most perpetrators of harassment are other youth. Even back in 2005 among American students grades 4-8:
 - 42% had been bullied online – 1 in 4, more than once.
 - 35% had been threatened online – nearly 1 in 5, more than once.
 - 21% had received mean or threatening e-mail or other messages.
 - 58% admitted someone has said mean or hurtful things to them online – more than 4 of 10 said more than once.
 - 53% admitted having said something mean or hurtful to another person online – more than 1 in 3 having done so more than once.
 - 58% had not told their parents or an adult about something mean or hurtful that happened to them online.

Cyber-bullying & online manipulation

True story: Chris*

- 13-year-old boy from a close-knit family
- Rules were established
 - No searching/visiting porn websites
 - No posting personal information
 - No chatting with strangers
- Monitored by parents to verify compliance
- Blindsided by cyber-bullying and an unhealthy online relationship



** Name changed to protect privacy.*

Cyber-bullying: How and where

Anywhere students are online

- Instant Messaging exchanges
- Chat rooms
- Screen-name profiles
- Websites (created by children)
- Website guest books
- Cell-phone text messaging
- Blogs / online diaries
- Identity theft

What it takes to keep children safe

FACT: Advanced computer skills *are not required* to understand Internet safety! All it takes is three simple things:

1. Basic knowledge of how the Internet is used today
2. A good understanding of the Internet's dangers
3. **Some old-fashioned common sense and open communication**



Common sense actions children must avoid

- Posting or sending personal information or pictures.
- Engaging in online sexual behavior.
- Saying rude or nasty things online to harass or embarrass others.



Tips to keep children safe online

- Be an active part of children's online experience.
- Make certain they personally know everyone on their "buddy" lists... and you do too – ***No strangers allowed!***
- Get firsthand knowledge: Register yourself for the websites that your child is a member of.
- Keep the computer where everyone sees the screen – ***No hidden screens!***
- Keep personal information private – ***No personal info or picture posting!***
- Report strangers who solicit meetings with any child.
- Teach children how to recognize, avoid and report predators and cyber-bullies.

Open communication with children

FACT: Only 44 percent of youth who received a sexual solicitation told a parent or responsible adult.

Crimes Against Children Research Center – Online Victimization: Five Years Later, 2006

- Show that your values offline match your values online.
- Promise your children that you won't get angry if something happens.
- Avoid focusing too much on rare or hypothetical dangers.
- Encourage their other interests.



Open communication with children

Take time to ask questions about their online world:

- Which programs are you using for IM and Chat?
- What is your screen name?
- What is in your profile?
- Who is on your buddy list?
- Have you ever shared your password with a friend?
- Have you ever posted your picture on the Internet?
- Have you ever cyber-bullied or have been cyber-bullied?

Final word: Internet safety resources

- i-SAFE America Foundation
www.isafe.org
- Local law enforcement
- Frontline's Growing up online documentary at:
<http://tinyurl.com/2y29qb>
- Center for Technology, Innovation, and Community Engagement (CTICE), Columbia University





Celebration *of* Service

As part of our centennial celebration, IBM shared a range of volunteering resources that IBMers have used in communities around the world.

on demand community

IBM's community service initiative supports volunteering by more than 150,000 employees and retirees, who collectively record more than 1 million hours of service every year worldwide.

© IBM Corporation 2011

IBM, the IBM logo, ibm.com and On Demand Community are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. Other product, company or service names may be trademarks or service marks of others.