



## 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*



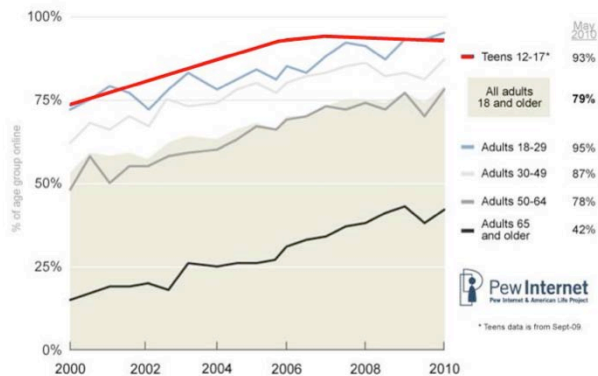
*Celebration of Service*

Empowering young people to be safe on the Internet

Hello to you all. My name is \_\_\_\_\_, and I want to talk to you today about empowering children to be safe on the Internet. Before I start, I want to underscore the fact that I am here today to raise awareness on this issue and point to other expert resources. While I care deeply about this issue, I am not an expert and do not serve as the sole source of information on this complex topic.

IBM is providing this solution for your information and use. It is not a complete list of everything adults and children should know about Internet Safety; each adult will need to decide what other kinds of resources they need to make children's Internet use a safe and enjoyable experience.

## Change in Internet usage by age, 2000-2010



*Celebration of Service*

Empowering young people to be safe on the Internet

If we take a look at how Internet usage for different age groups has changed over the last ten years, we see some startling information. A 2010 study by the Pew Internet & American Life Project shows that even though the biggest increase in Internet usage has come from older adults, the people that are using the Internet the most are teenagers ages 12 to 17!

I'm going to share several statistics with you during this presentation. While some of the statistics are from a few years ago—our oldest stat is from 2003—they are illustrative of the current risks that youth face when using the Internet.

And also consider that a slightly expanded notion of the Internet to include mobile devices. Since the mobile Internet user grows faster these years, I also suggest parents and teachers pay special attention for children's Internet safety through mobile phone access as well.

## 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%

*Celebration of Service*

Empowering young people to be safe on the Internet

This isn't the only surprising piece of information, though. It turns out that the activities that children and teenagers do online are, on average, very different from the activities that adults do online. Adults are much more likely to use the Internet for finding information quickly, such as buying things online or checking e-mail. Teenagers, on the other hand, are much more likely to use the Internet for leisure – networking, socializing, gaming, and otherwise passing the time.

Unfortunately, it's those very activities that are also the riskiest in terms of internet safety, as you can probably imagine. Not only are children and teenagers on the Internet a lot more than adults, but their activities online are a lot more dangerous.

## 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*



*Celebration of Service*

Empowering young people to be safe on the Internet

Those activities can have harrowing consequences, which is why Internet safety is more important than you think.

- 39% of teens have posted something online that they later regretted. Common Sense Media, 2010
- 79% of unwanted exposure to pornography by youth occurs in the home. Online Victimization of Youth: Five Years later, 2006
- 1 in 7 children who use the Internet have been sexually solicited. Internet Filter Review, 2005

## 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.

*Celebration of Service*

Empowering young people to be safe on the Internet

**FACT:** Youth are sophisticated users of technology – often more clever and experienced than adults.

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

The first thing to realize is that the current generation of youth is the technology generation. Remember, they can figure out how to get unrestricted Internet access by working around filters you might set or by hiding their browsing history. In fact, a Girls Scouts survey found that teen girls believed they could do the following without their parents' knowledge:

- Chat in a chat room (86%)
- Read their parents' e-mail (57%)
- Carry on a cyber romance (54%)
- Set up a meeting with someone they met online (46%)
- View a pornography site (42%)

The important thing here is to set some ground rules that can give them some common sense. That way, they can get the most out of what the Internet has to offer and maintain their social lives while making sure that they are safe.

In addition, teenagers are getting more and more adept at hiding risky online sexual behaviors from parents:

- 63% of teens said they know how to hide what they do online from their parents
- 32% clear their browsing history, making it impossible for parents to see which websites they have visited
- 16% have created private e-mail addresses or social networking profiles, separate from their "real" e-mail address that is known by parents and other adults

In fact, to communicate even faster in chat rooms and IM-ing, a new spelling system has been devised and is constantly evolving. For example, writing the three letters "POS" (or "Parents over Shoulder) indicates to their chat buddy to not write anything that might generate suspicion by a parent. 28% of teenagers admit to doing this 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



Celebration of Service

Empowering young people to be safe on the Internet

Now, just a minute ago I said that I am by no means an expert on the topic of internet safety. The good news, though, is that you don't need to be an engineer in order to understand Internet safety. Many adults falsely assume that keeping children safe on the internet requires some sort of technical degree in computer engineering, but in reality all that is required is the same degree of attentiveness that keeps our children safe in offline world, plus a little bit of know-how to deal with this ever-changing medium. All of what we need is included in this presentation:

- First, we need to get a basic knowledge of how children are using the Internet today. There are tons of Internet buzzwords out there, and they change year by year, so we'll get a quick rundown of all the activities that really matter.
- Second, we need a good understanding of the Internet's dangers.
- Third, it takes some old-fashioned common sense to make sure that children are avoiding risky behaviors online.
- Lastly, it is important to establish and maintain open communication with children, so that you become the person to turn to for all Internet-related concerns.

In short, all it takes to keep children safe on the Internet is the same degree of attentiveness that keeps our children safe in the offline world!

## 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



*Celebration of Service*

Empowering young people to be safe on the Internet

Our first major step is to take a crash course on how the Internet is being used by children today. That way, we can understand the types of situations and places where the dangers that we hear about actually take place.



## 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



*Celebration of Service*

Empowering young people to be safe on the Internet

It might not come as a surprise that most of what children do online is completely free of charge. Because each of these services is ad-supported, the only thing that children need to do to use them is register using their name and other information. Here are some of their most popular activities online:

- Search engines
- E-mail
- Photo- and video-sharing websites
- Chat rooms
- Instant messaging ("IM-ing")
- Social networking sites
- Online games

If you already know what some of these are, bear with us real quick as we take a whirlwind tour and do a quick highlight of each of them.

However, we're not going to review search engines and e-mail in order to spend more time on the services that are really attracting young people today.

## 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

Photo-sharing websites and video-sharing websites allow users to create profiles and share photos that they took or videos that they recorded with the world. You can search for photos and videos that you like and leave public comments about them afterwards. Most of the photos or videos revolve around common interests, and users can even send private messages to others who have posted photos or videos that they like. Most of these websites are moderated and have strict filters for blocking adult content, but comments are often inappropriate, and some websites are 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

*Celebration of Service*

Empowering young people to be safe on the Internet

Chat rooms are places where groups of people can type messages and “chat” with each other in real time. Each user signs into the chat room using what’s called a “screen name” or a “display name” – basically, a nickname that they can make up. The main board shows instant messages that everyone in the chat room are typing, but users can have private chats with each other as well. These are called “PMS,” private messages, and they often let you use your microphone and webcam for audio and video instead on just typing text.

77% of solicitations take place in chat rooms and instant messaging systems, according to a Harvard University recent study.

## 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

*Celebration of Service*

Empowering young people to be safe on the Internet

Instant messages, again, are any messages you type to someone that are shown in real time, as if you were chatting. Chat rooms let you "IM" with lots of people really easily, but you can also download chat programs on your computer so you can chat privately with people you added as "friends" anytime.

## 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

Social networking sites are perhaps the newest craze. They let teenagers create profiles using their real name and information, and are used as tools to stay in touch and socialize with friends. Users can post photos and “tag” other people that appear in them, and they can also chat with friends that are also currently online. The biggest feature, though, is the ability to post “status updates” that alerts other people what you are up to and view a digest of other people’s status updates.

Some children may share too much private data, such as their home address or what school they go to. Just as it is simple for a young child to fake their age online, it is easy for a potential predator to fake a profile claiming to have the same interests as, and be the same age as, your child.

## 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.

Next, there are online gaming networks. There are tons and tons of free, ad-supported games online that children can play using the computer, but many of the largest and most popular games nowadays are on home consoles. Players can talk to each other as they play using headsets, and can “friend” other people to see when they’re online and which game they’re playing.

Since kids are naturally attracted to games and because most of the games that are online are so competitive, though, these networks are prone to cyber-bullying and harassment. Think about it: a dozen teenagers and young adults are online battling in a first-person shooter. 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.



*Celebration of Service*

Empowering young people to be safe on the Internet

Finally, there are file-sharing networks, which allow users to share and download any type of content (usually music, movies, and software) directly for free. They are perhaps the best example of how children can find themselves in serious trouble since downloading the files seems innocent enough. Illegal downloads are being pursued more aggressively than ever before, but even if there wasn't a serious legal problem, the downloaded files often contain viruses and pornography even though they were listed as a song or a 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.



*Celebration of Service*

Empowering young people to be safe on the Internet

So, there are more ways than ever before for people to communicate online, and what's wrong with that? It's only a computer. After all, they see and hear some pretty raw stuff on cable TV, listening on the radio, or watching the Super Bowl.

And, how dangerous could it be? It's not like they're driving your car from here to New York City without first practicing with you around the neighborhood, right?



## 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*

*Celebration of Service*

Empowering young people to be safe on the Internet

Given those facts, we need to start looking at this from our kids' perspectives. News flash: Kids don't always listen to us!

- 49% say their child was 13 or older before they started surfing unsupervised, but only 14% of teens say they waited until there were this old, and 37% say they started before age 10!
- Just 16% think their child has shared information they would not normally share in public, but 28% of children actually have.
- Just 2% say their child has posted naked or semi-naked images of themselves, but 13% of children actually have.

## 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



Celebration of Service

Empowering young people to be safe on the Internet

By getting this basic knowledge of the kinds of ways that children are using the Internet today, you've already just taken the first step to narrow the "digital divide" between children and adults and to keep children safe.

The next step is to understand some of the dangers of using those tools to communicate with others over the World Wide Web, so now we're going to take a look at some of the real things that can happen when children aren't careful online.

## Real dangers of the Internet

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



*Celebration of Service*

Empowering young people to be safe on the Internet

The services that we described and the anonymity of the Internet has opened up an entirely new avenue for three major dangers:

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

Each one of these dangers is a big enough topic to deserve its own separate presentation, but we will show how these situations can arise from using those services we discussed, and we will show a few of the heartbreaking stories that have occurred as a result.

Which children are really at risk?

**Every child with Internet access is at risk!**



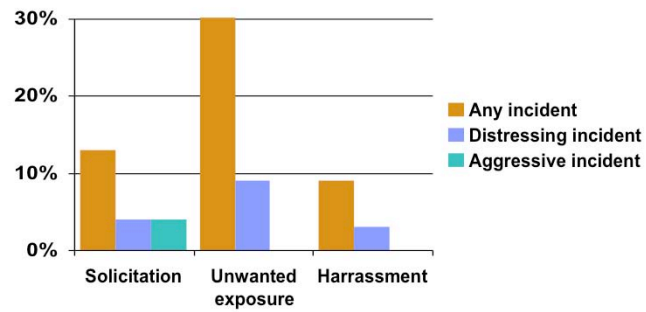
*Celebration of Service*

Empowering young people to be safe on the Internet

But first: which children are really at risk? The sad reality is that all children who have Internet access are at risk. An uninformed, naïve child is a child at high risk.

## Online victimization

Percent of Internet users 10-17 years



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

*Celebration of Service*

Empowering young people to be safe on the Internet

The most recent statistics from 2006 show that every child is at risk. In that year, a significant percent of children had been subject to solicitation, unwanted exposure and harassment.

## Inappropriate material: online pornography

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



*Celebration of Service*

Empowering young people to be safe on the Internet

In 2003, statistics showed that 90% of 8-16-year-olds had viewed pornography online. More recent statistics are not available for this presentation.

At that time, 12-17-year-olds were the largest consumer group of Internet pornography – not surprising given the early exposure to pornography that they face. The initial unwanted exposure to pornography that occurs when children are young leads to an entirely different problem: children will eventually start to go looking for inappropriate material online and will try to learn to become increasingly resourceful. The adult industry themselves state that their traffic is 20-30% children.

2003 statistics obtained from [www.familysafemedia.com](http://www.familysafemedia.com), Google, WordTracker, PBS, MSNBC, NRC, and Alexa Research.

## 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.



*Celebration of Service*

Empowering young people to be safe on the Internet

That resourcefulness becomes even more of a problem when we talk about other types of inappropriate material. The number of sites advocating hate or depicting violence rose from 8,667 at the end of 2003 to 11,500 in 2010. Sites spouting racial, homophobic, and religious hatred are showing up at a faster rate than pornography.

For example, there are white supremacist sites which might appear quite respectable although perhaps distasteful. They promote gaining governmental power and promoting white culture, through articles that contain twisted historical facts.

Children often come upon such sites in an innocent way. A prime way to target kids for the purpose of spreading propaganda is through online and downloadable games.

Not only can these websites be damaging to the children who are fooled into entering one, but the messages that they contain could unassumingly be taken to heart.

## 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*

*Celebration of Service*

Empowering young people to be safe on the Internet

The first danger was the risk of instant exposure to inappropriate material, so let’s talk about a few ways that that could happen. We need to remember that no one can escape exposure to unwanted solicitation on the Internet.

Companies target kids and teens through pop-up advertisements, which generally appear in a small window over the main display area. They also use spam, which is mass-mailing e-mail, and spim, which is mass Instant Messages. These advertisements often contain inappropriate material, including adult material and hate propaganda.

Kids approach being online differently than adults. While adults almost automatically “X out” those annoying pop-ups and e-mail, kids are more likely to open them up and look -- a situation not lost on the advertisers.

Many children-oriented websites allow gambling advertisements that appear to be games, with blinking lights and sound effects that lure youth. Plus, a survey released by the United Kingdom’s Gambling Commission in 2009 stated that more than 33% of gambling websites have “deficiencies” that allow minors to play.

In addition, a large number of files are available on file-sharing programs that have names of popular songs or bands, but are actually pornography.

Search engines – Even an innocent key word search in any search engine can yield an inappropriate solicitation. Many companies that have inappropriate Web material purchase domain names that will intentionally deceive children. Most are misspellings of popular children’s characters, activities, or interests. This is called “typo squatting.” For example, there have been sites with misspelled names of Pokemon and Disney characters. Often, simply typing in an innocuous word or phrase on a search site will produce links to inappropriate sites. For instance, the word ‘princess’ might direct you to an escort agency.

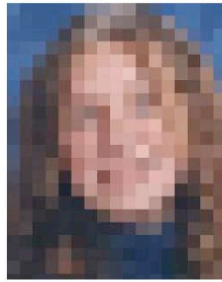
Checking e-mail – You would think that reading e-mail would be safe, but 92% of the world’s e-mail is actually spam like the messages shown here, and 2% of that spam is pornographic, causing many children to receive pornographic spam on a daily basis.



## 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.*

*Celebration of Service*

Empowering young people to be safe on the Internet

It doesn't stop at inappropriate material or unwanted solicitation. Any child can be at risk for online predators looking to initiate offline encounters, which is the next danger we will talk about.

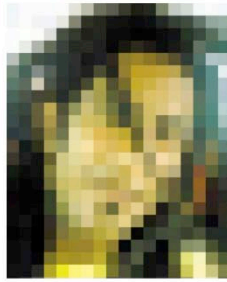
This is a true story; we've changed the name and other identifying characteristics to protect the privacy of the individual. Carrie was a straight-A student. She was captain of the cheerleading squad and very popular amongst her classmates. She was the last kid you would expect this tragedy to happen to.

Carrie was also a frequent user of chat rooms. She met someone online and began building a relationship. Once their friendship grew, they began to use Instant Messaging, e-mail and the telephone. Eventually, they decided to meet one night at a local shopping center. Carrie thought it would be okay to meet her online friend in a public location. The man she met turned out to be a 24-year-old predator. That night he raped and killed her.

## 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.*

Celebration of Service

Empowering young people to be safe on the Internet

None of us should jump to the conclusion that young girls are the only victims of Internet-related crimes.

This is a true story; we've changed the name and other identifying characteristics to protect the privacy of the individual. Josh was a bright and outgoing high school student who was really into computers. One day he met a young woman in a chat room about computers. They discovered that they really liked talking with each other so they exchanged their personal e-mail addresses and started sending e-mail directly to each other. Not long after that they began talking to each other on the telephone.

Eventually, they decided that it would be great to meet – to go out on a date. He was really excited because she was older and was interested in him. So, one weekend night, they met at a designated spot. They had a great time together and decided to meet again later that week.

For their second date, the woman drove Josh to a location where four of her friends were waiting. They shot and killed him. It turned out that this woman and her friends belonged to an Anti-Semitic hate group, and she had been online searching for a Jewish target. There was no way that Josh could have known that, even after their phone conversations or if he had used a web cam.

## 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.

*Celebration of Service*

Empowering young people to be safe on the Internet

Let's shift from our kid's perspective to that of the online predator. The thing to remember most is the fact that the same free online services that children use to check e-mail, keep in touch with friends, and share photos and videos with are used by the entire world. Any information that a child posts online is essentially public, even if privacy settings are changed. Here is one example:

Almost all social networking sites have a comprehensive search function, so suppose a stranger decides one day to browse for singles ages 15-21 who are listed in towns near his that have indicated they are "looking for a relationship."

A few results come up, and one of the profile pictures piques his eye. After clicking the picture, he sees that the teenager kept most of her information private, so he can't see her cell phone number or any more pictures, but he can see some of her basic interests.

He notices that they actually have a few things in common, and sees that she likes a few things that he has always wanted to try. Suddenly, in his mind, they have a connection. Now he is going to try to get to know her even more.

## 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.



*Celebration of Service*

Empowering young people to be safe on the Internet

Her hometown was in the search result, so he knows where she is from, but a quick run at a search engine shows him that there is only one school in that town. It's not too large of a school, so he does another quick search to see everyone on the social networking site from that school. There she is again, but here are all of her classmates, and on the fourth page of search results he sees another girl's picture that looks remarkably similar.

It is definitely not the same girl, but the picture had to have been taken in the same house somewhere, and this girl is standing next to someone who got cropped out of the picture. This girl must be her best 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.

Luckily for him, the stranger was right – he sees dozens of posts that the girl made on this new “friend’s” virtual “wall”. Even more luckily, the friend keeps comments and photos visible to people near her town, so he can see can look through the photos to see if the teenager is in them. It turns out that she appears in a lot of those photos.

## 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!

A few weeks go by and he is watching any new photos and updates with great interest. The more he sees of her life the more he feels like he knows her. She went to the bowling alley with a large group of people last Friday, and she’ll be going to the movie theater to see the matinee tomorrow. He joins the virtual “group” that was planning the bowling alley trip in an attempt to see even more details.

Each of these times, he knows exactly where she’ll be and when, but he’s cautious to make a move. Finally, he decides to do it: he sends her a friend request.

She sees he is part of the virtual group that was coordinating the trip to the bowling alley, so she figures he must be safe, and in keeping with the friendly nature of social networking, decides to confirm him as a friend.

Now he has her cell phone number, and all of the photos that are only visible to friends. And just a few weeks ago, he did not 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*

*Celebration of Service*

Empowering young people to be safe on the Internet

Stories like those show how easy it is to expose personal information, even if you took several appropriate safeguards. The sad truth is that the online predator may not end right there, but could rather engage in a six-stage “grooming” process, regardless of how the initial point of contact was made.

The grooming process is a complicated one, but the large majority of online solicitations take place using instant messaging or chat rooms. In fact:

- 40% of all solicitations begin with an instant message.
- 37% of solicitations took place in a chat room.
- 70% of the victims were girls and 30% were boys.
- 81% of the victims are teenagers aged 14 or older.

## 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.



*Celebration of Service*

Empowering young people to be safe on the Internet

(Note to presenter: this slide and the next conclude the section on online predators by saying that there is a general pattern or process to what predators do. In the interest of time, you should not linger on these slides—focus on the bold words as they are self-explanatory. However, there are optional detailed notes below if you want to provide more information and have the time.)

As we've seen in the true story of Joshua and how predators establish a connection, there's a pattern or process that they go through, which was well documented in the 2006 study. Mostly by way of review and to make it a little clearer to you what those stages are: the predator goes through about six stages...the first three being 1) making themselves seem appear non-threatening and familiar to a young person, 2) creating a bond of trust between themselves and the child—often at the parent's expense, and 3) sealing that bond that establishing secrecy between the two.

More detail (optional)

### First stage

In the first stage, predators cultivate a relationship with the child, giving the attention that he or she may not feel that he or she is getting at home. They will chat about sports, music and other common interests, even about your child's friends and enemies. Remember, the predator was once a child, too.

They will listen to your child, sympathize with complaints about family, friends or trouble at school, even encourage your child to share any fears that your child may have and respond in ways that reinforce feelings of alienation. Grooming is a very purposeful, methodic, and patient process, cloaked in kindness and empathy. Predator uses information gathered from profile and chat room conversations.

### Second stage

In the second stage, predators develop trust with the child.

Predators exploit parent/child conflicts and use them to their advantage by encouraging the feeling that the parent is wrong. To gain trust, the predator takes the child's side and disparages the parent to foster the illusion that the predator alone is the only one on the planet that really understands your child. Of course, this is exactly what many kids want to hear. This can all be done over time in a public chat room with no one the wiser.

Predator fosters the illusion that they are the only person who understands the child.



## 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.



*Celebration of Service*

Empowering young people to be safe on the Internet

### Third stage

In the third stage, the predator established secrecy.

As the relationship evolves, the predator will encourage the child to keep their "friendship" secret by stating that other people - especially parents - won't understand how the child can be such good friends with someone they met on the Internet. This is an important turning point in the relationship where the parent is purposely isolated from the relationship between predator and victim. If a child keeps secret Internet friends, it is a red flag for the parent that a predator may be at work systematically grooming the child without the child's knowledge.

Secret instant messaging and e-mail accounts now allow a predator to communicate stronger messages

### Fourth stage

The fourth stage of the grooming process has the predator getting the child to talk about adult topics—sex—removing that barrier. Direct intimidation can come next, and the child may now feel as if they cannot turn to another adult for help. And the last stage is what the predator hoped to achieve from the beginning—meeting face to face.

### More detail (optional)

In the fourth stage, the predator erodes any existing barriers.

The predator often takes advantage of the victim's natural curiosity. It is important to the predator that the child's natural and defensive barriers are weakened so that ultimately the predator can meet the child in person.

To do this, the predator gradually breaks down the child's inhibitions by introducing sexual content into their conversations and by sending pictures. By playing on their curiosity, over time the child becomes less uncomfortable with inappropriate statements and photos to the point that the predator may try to make the child think sex between adults and children is normal.

Obscene photos are sent to desensitize the child's protective inhibitions.

## 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

*Celebration of Service*

Empowering young people to be safe on the Internet

### Fifth stage

In the fifth stage, the predator employs direct intimidation. Sometimes, but not always, the predator will make threats if the child stops communicating or refuses to meet them in person. They may threaten to tell the child's parents about their relationship, including their private conversations and the images that they have shared, or even threaten to harm the child's family.

By this point the child may feel powerless against their online "friend." They may feel they have no one to turn to out of fear of the predator's threats and their parents' anger about this situation.

The predator can resort to outright threats of violence or humiliation.

### Final stage

In the sixth and final stage, the predator arranges a face-to-face meeting. The victim doesn't know this, but whatever their methods, the Internet predator's ultimate goal is to get your child to meet face-to-face.

## 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.

*Celebration of Service*

Empowering young people to be safe on the Internet

The final danger that I wanted to highlight is cyber-bullying. As we all know from reading the news, bullies aren't only on the playground.

As the name implies, cyber-bullying is the use of technology resources like e-mail, instant messaging, and website information to deliberately harass and harm others. The Internet is the latest weapon in a bully's arsenal. Through the Internet, bullies can terrorize relentlessly and humiliate their victims in front of literally millions. Cyber-bullies can send cruel messages, gossip or photos about a particular child, copying the child's whole school or peer group.

In 2006, 58% of harassment perpetrators were other youth. Online Victimization: Five Years Later, 2006

According to a survey of 1,500 students between grades 4-8 conducted by i-SAFE:

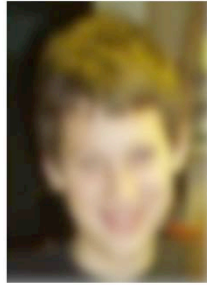
- 42% of kids have been bullied while online. 1 in 4 have had it happen more than once.
- 35% of kids have been threatened online. Nearly 1 in 5 have had it happen more than once.
- 21% of kids have received mean or threatening e-mail or other messages.
- 58% of kids admit someone has said mean or hurtful things to them online. More than 4 out of 10 say it has happened more than once.
- 53% of kids admit having said something mean or hurtful to another person online. More than 1 in 3 have done it more than once.
- 58% have not told their parents or an adult about something mean or hurtful that happened to them online.

This is a true story; we've changed identifying characteristics to protect the privacy of the individual. This incident, which happened in Japan, demonstrates that Internet safety is indeed a global concern. In 2004, a pre-teen student slashed the throat of her schoolmate while at school. The victim of the attack had used website postings and harassing e-mail to cyber bully the girl who ended up killing her.

## 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.*

*Celebration of Service*

Empowering young people to be safe on the Internet

This is a true story. Again, we've changed the name and other identifying characteristics to protect the privacy of the individual.

Chris was an eighth-grader who was bullied by students first at school and then on the Internet. Instant messaging was used as a tool to continue the verbal bullying that he was a victim of at his middle school. Certain classmates hid behind the anonymity of a screen name and carried out some very hurtful acts. One female classmate pretended to like Chris on-line through IM exchanges and then forwarded these private conversations to others at the school to embarrass and humiliate him.

Chris became depressed and suicidal. During his last days alive, he told several of the students, including the female classmate, that it was people like them that made him want to kill himself. He took his hurt and anger online and commiserated with another boy who was also not in a healthy state of mind. This other boy encouraged Chris's suicidal ideation. Chris died of suicide at age 13.

His parents wished they had paid closer attention to his use of IM and who was on their son's buddy list. They strongly advise parents to ask themselves if they know every person on their child's buddy list personally. And if they don't, they should ask their child to bring their IM buddy to their home to meet them in person. The parents feel that if you care about who your child is friends with in the physical world, you should be equally vigilant about who they are friends with in the cyberspace world.

## 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

*Celebration of Service*

Empowering young people to be safe on the Internet

Unfortunately, the ability to be anonymous and the far reaching impact of the Internet has emboldened many young people to bully and harass each other online in ways parents would never have even imagined. If your child's screen name is well known by classmates, they can easily become the target of very hurtful instant messages by children they may not even know. One only has to visit an online teen chat room for a few minutes and observe the same behavior being carried out in a much more public environment. Many children also use their IM/chat screen name profile window, the one normally used to describe yourself, to post hurtful messages and private IM exchanges with the intent to embarrass, humiliate or intimidate another child.

Websites are also another tool of choice to bully and harass others. Young people have discovered free web hosting sites that enable them to create a website with the intent to bully another child. Embarrassing pictures, private IM exchanges, hateful/ threatening messages are just a few examples you'll find on these websites. Some young people also will think it's funny to post a mean comment at a legitimate website's guestbook

Your child might have started an online diary and exposed themselves to ridicule by sharing to many personal details or may be the subject of ridicule in another child's on-line diary.

It's common for young people to share their IM account passwords with friends. It's also not uncommon for friendships to sometimes deteriorate or not be so trusting, and the result is that your child's passwords gets shared with others. A cyber bully with your child's password can sign on and pretend to be your child and behave inappropriately with others with the intent to embarrass and humiliate your child. Many young people have also figured out that they can create a screen name very similar to your child's and effectively fool others into thinking they are chatting with your child.

## 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**



*Celebration of Service*

Empowering young people to be safe on the Internet

Now that we have a good grasp of how children are communicating online and have gotten a sense of the dangerous situations that can arise, let's take a look at some of the ways to keep children safe. The good news is that most of what we can do to help boils down to nothing more than making sure that children are using basic common sense when they're online, and that adults use common sense to monitor their online behavior.

## 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.



*Celebration of Service*

Empowering young people to be safe on the Internet

Given these facts, there are a few things that children should always avoid doing as a no-brainer:

- They should avoid posting or sending personal information or pictures, which online predators and cyber-bullies use to identify them
- They should also avoid engaging in online sexual behaviors such as going to X-rated websites on purpose, using screen names with sexual connotations, sending sexual pictures online, or talking to people they only know online about sex
- Lastly, they should refrain from 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.

*Celebration of Service*

Empowering young people to be safe on the Internet

Here are several simple, common sense tips. Perhaps the most important is the first: have fun being part of children's online experience. Let them teach you about the Internet. It's good that our children are the experts! Don't let the technology distance you from children; use it to bring you together.

At the same time, be vigilant! Children, despite our best advice, may still go into chat rooms they should not or may share information on the Web that they should not. It's important that we, as adults, have firsthand knowledge of the Internet experiences our children are having. Try registering yourself for the websites that your child is a member of so that you can learn what they are all about and see your child's profile. What they view as "innocent" or "safe" behavior may not be.



## 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.



*Celebration of Service*

Empowering young people to be safe on the Internet

The following tips were provided by the Crimes Against Children Research Center and Cyber Angels:

First, make it a point to plan ahead and let kids know about the things they may encounter online. You don't have to scare them, but teach them that your values offline match your values online. You can start by printing a copy of the Internet Usage Agreement that is located on [www.cyberangels.org](http://www.cyberangels.org), going over that agreement with your children, and posting it on a wall near the computer. Remember, if they can't hang out at the park at 2:00 a.m., they shouldn't be surfing then either!

Then, be sure to promise your children that you won't get angry if they come to you with a problem about an online situation. Stay calm and remember that your child trusted you to help when they came to you - don't let them down!

In addition, avoid focusing too much on rare or hypothetical dangers. Keep your focus centered on helping your children understand common risks so that they know you are grounded in their reality.

Finally, do your best to encourage their interests outside of the Internet. Children shouldn't spend excessive amount of time online - it's just not healthy for them.

## 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?

*Celebration of Service*

Empowering young people to be safe on the Internet

We care about where children hang out after school, how they dress and portray themselves to others, who their friends are and what activities they are up to in the physical world. The new challenge we have as adults today is the need to apply these same concerns to the Cyber world.

Become aware of where children are hanging out online. Have they chosen a very age-inappropriate screen name? Perhaps to be provocative? Or with an older age posted so that they can pretend they are older than they really are?

Parents should know everyone on their children's buddy list. If not, perhaps you should ask your child to invite them over for dinner so you can get to know them.

Stress the importance of keeping passwords private. Explain the risks to children. The same goes for posting personal information and pictures on websites. And be clear that bullying is unacceptable in both the real and Cyber world. Make sure children know that it is important not to engage or retaliate online, and if they are a victim of cyber bullying, they should report it to you ASAP.

## Final word: Internet safety resources

- i-SAFE America Foundation  
[www.isafe.org](http://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*

Empowering young people to be safe on the Internet

As adults, it is our responsibility to know how to recognize and avoid dangerous, destructive, inappropriate or unlawful online behavior. But it's also important to recognize that we don't know all there is to know about this important subject. There is a lot more to learn about keeping our children safe online. Remember, while I hope that I shared some important information with you today, my goal is to raise awareness. I am not an expert and do not serve as the sole source of information on this complex topic.

The good news is that there are expert resources available to you. Expert resources include:

I-SAFE America Foundation, a non-profit foundation, designated by the United States Congress, to educate and empower youth of the nation to safely and responsibly take control of their Internet experiences. In fact, I-SAFE created this presentation for IBM's On Demand Community.

Most local law enforcement agencies have a task force dedicated to Internet crime, which can provide you with specific information on Internet safety issues in your community.

Finally, there is an excellent book called *Keep Your Kids Safe on the Internet* by Simon Johnson. It includes a forward written by Teri Schroeder, founder and chief executive office of i-SAFE. You can get this book on [amazon.com](http://amazon.com), as well as many bookstores.

Thank you for attending.



## 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.

Empowering young people to be safe on the Internet