

BLOG BEWARE



■ The Problem ■

Recent incidents involving Internet crimes against children have been prominent in the media. In some incidents, the crimes have involved suspects and victims who met each other on social networking or blogging sites such as MySpace, Friendster, Xanga, and Facebook.

Blogs and social networking sites where people can meet, communicate, and interact have recently exploded in popularity. The number of visitors to MySpace went from 4.9 million in 2005¹ to currently over 67 million.² Like most new technological developments, this brings both positive and negative implications, especially for parents and their children.

The majority of the activity on these sites is legal and can be positive. Young people who are curious connect with friends and seek like-minded individuals. However, many children and teens are not aware they are putting themselves in danger by giving out too much personal information and communicating with people they've only met online.

The unprecedented amount of personal information available on blogs and social networking sites makes them a perfect place for people who would harm children to identify their victims and gain their trust. This trust can be used to lure children and teens into a false sense of security, making them vulnerable to "grooming" and enticement to meet in person, which could have very serious consequences.

Other dangers to children include exposure to inappropriate content, cyberbullying, or identity theft.

Children and teens are often not aware that their words — which may have been intended for a small audience — sometimes find their way to a larger one, especially if they are controversial. Some students who have posted threatening words against their school or classmates have attracted the attention of law enforcement, while

those who have posted inappropriate comments about school personnel have also been disciplined. Some universities and employers have even used online postings when considering potential candidates.

Even before the rise of blogs and social networking sites, children faced many dangers while online. Our 2000 study reported that one in five children had received a sexual solicitation online and one in 33 received an aggressive solicitation. This problem is compounded because most children did not inform their parents of the incidents. Less than 1 in 4 told a parent about the sexual solicitation they received.

To help stop this dangerous trend, NetSmartz is releasing "Blog Beware" to raise the awareness about the risks associated with these sites and give parents, children, and teachers the tools they need to keep children and teens safer online. This resource contains safety tips for parents and children and includes a quiz that they can take together. It is also supported by the extensive material available on NetSmartz.org for kids, teens, parents, educators, and law enforcement.

The NetSmartz® Workshop is an interactive, educational safety resource from the National Center for Missing & Exploited Children® (NCMEC) and Boys & Girls Clubs of America (BGCA) for children aged 5 to 17, parents, guardians, educators, and law enforcement that uses age-appropriate, 3-D activities to teach children how to stay safer on the Internet.

NetSmartz has developed a comprehensive educational Internet safety program that has been proven successful in more than 3,000 Boys & Girls Clubs across the country reaching over 3.3 million young people. NetSmartz officially partners with 15 states to implement its important Internet safety message in the community and help prevent the online victimization of children.

¹Janet Kornblum. "Teens hang out at MySpace." *USA Today*. January 8, 2006, http://www.usatoday.com/tech/news/2006-01-08-myspace-teens_x.htm?csp=34.

²April 3, 2006, <http://www.myspace.com>.



■ Data ■

Online Victimization: A Report on the Nation's Youth

You can access the entire report at www.NetSmartz.org under "Statistics."

This report is based on interviews with a nationally representative sample of 1,501 youth ages 10 to 17 who use the Internet regularly³ and found that

- Approximately one in five received a sexual solicitation or approach over the Internet in the last year.
- One in thirty-three received an aggressive sexual solicitation—a solicitor who asked to meet them somewhere; called them on the telephone; sent them regular mail, money, or gifts.
- One in four had an unwanted exposure to pictures of naked people or people having sex in the last year.
- One in seventeen was threatened or harassed.
- Approximately one quarter of young people who reported these incidents were distressed by them.
- Less than 10 percent of sexual solicitations and only 3 percent of unwanted exposure episodes were reported to authorities such as a law-enforcement agency, an Internet Service Provider, or a hotline.
- About one quarter of the youth who encountered a sexual solicitation or approach told a parent. Almost 40 percent of those reporting an unwanted exposure to sexual material told a parent.
- Only 17 percent of youth and approximately 10 percent of parents could name a specific authority, such as the Federal Bureau of Investigation, CyberTipline®, or an Internet Service Provider, to which they could make a report, although more said they had "heard of" such places.
- In households with home Internet access, one third of parents said they had filtering or blocking software on their computer at the time they were interviewed.⁴



³David Finkelhor, Kimberly J. Mitchell, and Janis Wolak. *Online Victimization: A Report on the Nation's Youth*. Alexandria, Virginia: National Center for Missing & Exploited Children, 2000, page ix.

⁴Ibid.



■ The Solution ■

Tips to Keep Your Children and Teens Safer When Using Social Networking Sites

1. Discuss the dangers and future repercussions with your child.
2. Enter into a safe-computing contract with your child about his or her use of these sites and computer use in general.
3. Enable computer Internet filtering features if they are available from your Internet service.
4. Install monitoring software or keystroke capture devices on your family computer that will help monitor your child's Internet activity.*
5. Know each of your child's passwords, screennames, and all account information.
6. Put the computer in a family area of the household and do not permit private usage.
7. Monitor what your child's friends are posting regarding your child's identity. Often children and their friends have accounts linked to one another, so it's not just your child's profile and information you need to worry about.
8. Know what other access your child has to computers and devices like cell phones and PDAs.
9. Report all inappropriate non-criminal behavior to the site through their reporting procedures.
10. Report criminal behavior to the appropriate law-enforcement agency including the NCMEC CyberTipline at www.cybertipline.com or the Internet Fraud Complaint Center at <http://www.ic3.gov>.
11. Contact your legislators and request stronger laws against Internet crime.
12. Visit the NetSmartz Workshop at www.NetSmartz.org for more information.
13. Remember that every day is Halloween on the Internet. People on the Internet are not always who they appear to be.

*For information about monitoring software, visit www.getnetwise.org.

Tips for Kids and Teens to Stay Safer When Using Blogs and Social Networking Sites

1. Never post your personal information, such as cell phone number, address, or the name of your school.
2. Be aware that information you give out in blogs could also put you at risk of victimization. People looking to harm you could use the information you post to gain your trust. They can also deceive you by pretending they know you.
3. Never give out your password to anyone other than your parent or guardian.
4. Only add people as friends to your site if you know them in real life.
5. Never meet in person with anyone you first "met" on a social networking site. Some people may not be who they say they are.
6. Think before posting your photos. Personal photos should not have revealing information, such as school names or locations. Look at the backgrounds of the pictures to make sure you are not giving out any identifying information without realizing it. The name of a mall, the license plate of your car, signs, or the name of your sports team on your jersey or clothing all contain information that can give your location away.
7. Never respond to harassing or rude comments posted on your profile. Delete any unwanted messages or friends who continuously leave inappropriate comments. Report these comments to the networking site if they violate that site's terms of service.
8. Check the privacy settings of the social networking sites that you use:
 - a. Set it so that people can only be added as your friend if you approve it.
 - b. Set it so that people can only view your profile if you have approved them as a friend.
9. Remember that posting information about your friends could put them at risk. Protect your friends by not posting any names, ages, phone numbers, school names, or locations. Refrain from making or posting plans and activities on your site.
10. Consider going through your blog and profile and removing information that could put you at risk. Remember, anyone has access to your blog and profile, not just people you know.



■ Activities: Blog Beware Quiz ■

Here are a few of the questions from the NetSmartz “Blog Beware” quiz. See if you know the answers or sit down with your child or teen to test each other.

For answers and additional activities and Internet safety material, please visit www.NetSmartz.org.

Which is the safer screenname to have for your social networking site?

- a. Katie_ny13
- b. cute14girl
- c. YankEEfan7444
- d. Grade10hottie

Which item is more risky to post on your profile or blog?

- a. Your religious affiliation
- b. Your favorite food
- c. Your ethnic background
- d. Favorite movie
- e. Your hometown

Do you know the impact that your social networking site can have on your future?

- a. Yes, I know that college recruiters and future employers can search out my social networking site to get information about me.
- b. Yes, I know that once I submit something online it can never be taken back, because people can download my information onto their computers.
- c. No, I didn't know that college recruiters and future employers can search out my blogs or profiles and use them.
- d. No, I didn't know that once I submit something online it can never be taken back because people can download my information onto their own computers.

Which is the safer entry for your blog or personal profile?

- a. Full name, name of school, hobbies
- b. Nickname and state
- c. First name only, school mascot, photo of yourself

If you were to post a picture on your social networking site, which is the better choice?

- a. A picture of just yourself
- b. A picture of yourself with friends or family
- c. A picture of your sports team
- d. A picture of your car
- e. A picture of your local hang out
- f. A picture of your favorite celebrity, sports team, artist, or singer, author

Of the choices below, what would be an appropriate entry for a blog?

- a. “I am feeling depressed and sad; no one likes me.”
- b. “I scored 16 points at my basketball game last night! GO TIGERS! ON TO STATE!”
- c. “I had a great weekend filled with fun, I went to the movies with my best friend and then we went for ice cream.”
- d. “Today at school Connor Bodally made fun of me. Just because his dad owns the Drive-Ins in Beach Town, he thinks he is the coolest kid around. I hate him.”
- e. “I walked to work after school like usual. I really hate that we have to wear these stupid purple uniforms (see pic)...I mean we're just serving hamburgers right?”