Internet Safety: A Guide to the Information Superhighway

Mrs. Patrice Davis
Intervention Supervisor
Baldwin County Public School System
The Need for Internet Safety

- The Internet has opened up a world of information for anyone with a computer and a connection.
- But just as you wouldn’t send your children near a busy road without some safety rules, you shouldn’t send them on the information superhighway (the Internet) without rules of the road.
- Too many dangers from pedophiles to con artists can reach children (and adults) through the Internet.
What are the Dangers of the Internet?

1. Cyberbullying

- This includes sending hateful messages or even death threats to children, spreading lies online, making nasty comments on their social networking profiles, or creating a website to bash their looks or reputation.
What are the Dangers of the Internet?

2. Sexual Predators

- These are individuals who attempt to sexually exploit children through the use of on-line services and the Internet.
- Some of these individuals gradually seduce their targets through the use of attention, affection, kindness, and even gifts.
- Some of these individuals listen to and empathize with the problems of children. They are aware of the latest music, hobbies, and interests of children.
- While some sexual predators have targeted children in chat rooms, they also scour social networking sites such as MySpace and Facebook because these sites have centralized so much information, i.e., a child’s picture, personal interests, and blogs.
What are the Dangers of the Internet?

3. Pornography

- One of the worst dangers of the Internet, for many parents, is the idea that pornography could pop up and surprise their children.
- But parents may not realize that some children are going online to seek out web porn, too.
- Although you can view the Internet browser history to see which websites your child is viewing, you may also want to install Internet filtering software to block porn sites in the first place.
What are the Dangers of the Internet?

4. Damaged Reputations

- Camera phones, digital cameras, and web cams are everywhere these days; consequently, children can be victims of their own inexperience with new technology.
- Many children post pictures, videos, or notes online that they later regret.
- Encourage children to think before they click “send” because once they do, their picture is going to be in cyberspace forever.
Information Overload?

12 Things You Can Do To Protect Your Child Online
Internet Safety Tips for Parents

1. **Install the children’s computer(s) in a common family area** and have the screen facing the center of the room. It is far easier to monitor length and content of activity.

2. **Develop and agree upon a list of family computer use rules.** Include how long children may use the computer, which sites they may visit, where and with whom they may chat, what information they can give over the Internet, etc. Once you have made a list, both parents and children should sign it. Then post it by the computer as a reminder to all.
3. **Balance your children’s computer time with activities in the real world**, especially physical activities. Time on the computer competes with time spent with friends, family, exercise, school work, etc. Children need these activities as well.

4. **Distinguish between a “friend” and a “cyber pal.”** Friends are people you have met, and you can verify the truth of who they are. Cyber pals are people you have only met on the Internet and cannot verify. It doesn’t mean they are false or bad, only that you can’t “prove” they are who they say they are.
5. **Periodically discuss what information your children may share over the Internet.** Do not give out any personal information over the Internet—even to cyber pals and friends. With all of the search capabilities on the Internet, it is easy for a predator to find where you live and deduce family schedules.

6. **Teach your children to understand and respect intellectual property rights.** Copying electronically stored material may not seem as bad to children as taking a physical item, but it is still stealing. Gone are the days when you could bootleg music, images, and software with impunity.
7. Similarly, be aware of the quantity of your child’s possessions—particularly music, software, and games. Is it in keeping with your child’s income? Music and software that were not purchased can lead to stiff fines regardless of the child’s age.

8. Keep an up-to-date list of approved online friends with whom your child may correspond. This list should contain each person’s e-mail address, real name, street address, and phone number. Post a copy of the list by the computer and keep one yourself.
9. **Establish a rule about when your child may meet a cyber pal in person.** For example, you may decide that your child may meet a cyber pal *only* with explicit parent permission and a parent accompanying him or her.

10. **Routinely check your child’s computer activity.** Look at history files and bookmarks for use of sites that you are unfamiliar with and check them out. If they are inappropriate, delete them. Look for gaps in the history files or for bookmark, history, and/or cache files that are empty when you did not delete them. This includes documents, cookies, and trash.
11. **Watch for signs of secrecy, addiction, and unauthorized e-mail accounts.** Secrecy might be the child turning off the screen or computer when you come in the room, or logging off the Internet when you get home. Addiction might show itself as not having interest in anything but the computer, having more Internet pals than real friends, or having poor hygiene.

12. **Consider using blocking, filtering, or monitoring controls on your computer.** However, remember that every system has its limitations and needs to be checked periodically. Establish the rule that the system be changed only by you—the parent.
Before Clicking Send, Think on These Things...

10 Online Safety Tips for Teens
Internet Safety Tips for Teens

1. Do not give out personal information such as your address, telephone number, parents’ work address/telephone number, or the name and location of your school without your parents’ permission.

2. Tell your parents right away if you come across any information that makes you feel uncomfortable.

3. Never agree to get together with someone you “meet” online without first checking with your parents. If your parents agree to the meeting, make sure that it is in a public place and bring your mother or father along.
Internet Safety Tips for Teens

4. Never send a person your picture or anything else without first checking with your parents.

5. Do not respond to any messages that are mean or in any way make you feel uncomfortable. It is not your fault if you get a message like that. If you do, tell your parents right away so that they can contact the service provider.

6. Do not give out your Internet password to anyone (even your best friends) other than your parents.
Internet Safety Tips for Teens

7. Talk with your parents so that you can set up rules for going online. You and your parents should decide upon the time of day that you can be online, the length of time you can be online, and appropriate areas for you to visit online. Do not access any other areas or break these rules without their permission.

8. Check with your parents before downloading or installing software or doing anything that could possibly hurt your computer or jeopardize your family’s privacy.
Internet Safety Tips for Teens

9. Be a good online citizen and do not do anything that hurts other people or is against the law.

10. Help your parents understand how to have fun and how to learn things online. Teach them things about the Internet, computers, and other technology.
Internet Communication Methods

- E-mail
- Instant Messaging
- Chat rooms
- Blogs
- Forums/Newsgroups
- Web Cam
- Social Networking
Chat Rooms

- Chat rooms let you engage in a live conversation with people around the block or around the world.
- Everyone in the “chat room” can see everything you type.
- Even if the room is “teens only,” you have no way of knowing if everyone really is a teenager, so you still have to be on guard.
Instant Messaging (IM)

- Instant messaging is a way to stay in touch with friends without having to wait for them to respond to an e-mail.
- You type a message and the moment you click “send” that message appears on another person’s screen wherever they happen to be.
- You can exchange instant messages on computers and cell phones or between any other Internet connected devices.
E-mail

- E-mail is typically a one-to-one communications system.
- Just like regular mail, you write to someone and they can write back.
Forums/Newsgroups

- A forum is an online discussion group.
- Forums are sometimes referred to as a bulletin board, or a discussion area, or a newsgroup.
- Forums have proven themselves as valuable business resources—often creating communities of customers helping customers.
Blogs

- A blog is short for Web Log.
- A blog is a website of your own where you enter information ordered by date.
- A blog is an online diary or online journal that is shared with others online.
- A blog is generally maintained by an individual with regular entries of commentary, description of events, or other material such as graphics or video.
- Entries are commonly displayed in reverse-chronological order.
Web Cam

- A web cam is a digital video camera, usually attached directly to a computer.
10 Most Popular Social Networking Sites

- Facebook
- MySpace
- Twitter
- LinkedIn.com
- Classmates.com
- Ning.com
- Bebo.com
- H15.com
- Tagged.com
- Myyearbook.com
Safe and Responsible Social Networking

- Social networking sites such as MySpace and Facebook are useful Internet tools to keep in touch with family and friends and can be utilized to meet new people with similar interests.
- These sites have become very popular among teens as they seek to explore/define who they are and connect with others like themselves.
- Unfortunately, however, teens include too much personal information, discuss inappropriate behaviors that could get them into trouble, or otherwise place themselves at risk by what they share on their online profiles.
MySpace

- MySpace is a social networking website offering an interactive network of photos, blogs, user profiles, groups, and an internal e-mail system.
- The minimum age requirement to use this site is 14.
- As of March 5, 2010, MySpace was ranked as the second most popular social networking site with over 130 million users.
Facebook

- Facebook is a social networking site that anyone over the age of 13 (with a valid e-mail address) can join.
- Users can add friends and send them messages, and they can also update their personal profiles to notify friends about themselves.
- Additionally, users can join networks organized by workplace, school, or college.
- Facebook currently has over 400 million active users worldwide.
Facebook Features

- Wall—a space on each user’s profile page that allows friends to post messages for the user to see while displaying the time and date the message was written.
- Poke—intended to be a “nudge” to attract the attention of another user.
- Photos—users can upload albums of photos, tag friends, and comment on photos.
- Status—allows users to post messages for all their friends to read; in turn, friends can respond with their own comments and can also press the “like” button to show that they enjoyed reading it.
Facebook Features

- Gifts—allows users to send virtual gifts to their friends that appear on the recipient’s page; Facebook users are given one free gift upon registering their account; additional gifts cost $1.00 each
- Videos—users can add their videos by uploading a video, adding a video through Facebook Mobile, or using a webcam recording feature
- Events—a way for members to let friends know about upcoming events in their community and to organize social gatherings
Facebook Features

- Notes—a blogging feature that allows tags and embeddable images; a recent use of notes includes the Internet meme: “25 Random Things About Me,” which involves writing 25 things about the user that their friends don’t already know about them and using the tag function to ask 25 friends to do so also.

- Marketplace—allows users to post free classified ads within the following categories: For Sale, Housing, Jobs, and Other; ads can be posted in either available or wanted format.
Social Networking Tips for Keeping Yourself Safe Online

- Assume that everyone has access to your profile (parents, teachers, future employers, and law enforcement) even if you have your profile restricted to “friends only.” Don’t discuss things you wouldn’t want them to know about. Don’t use language you wouldn’t use in front of your parents. And make sure you set your profile to “private” so that you can control who has easy access to your information.
Social Networking Tips for Keeping Yourself Safe Online

- **Use discretion when putting pictures (or any content for that matter) on your profile.** Your friends might think that picture of you acting silly at the party last night is hilarious, but how will your parents or a potential employer react? Also remember that when your friend (or a stranger) takes your picture, it may end up on their profile for all to see.
Social Networking Tips for Keeping Yourself Safe Online

- Assume people will use the information on your profile to cause you harm. Don’t put anything online you wouldn’t want your worst enemy to know. Also, don’t add people as “friends” unless you know them in real life. Even if you think you know them, be skeptical. Teens often think it is cool to accumulate and have thousands of “friends.” Just remember, however, that these people have open access to all of your posted content and information.
Social Networking Tips for Keeping Yourself Safe Online

- Assume there are predators out there trying to find YOU based on the information you provide on your profile. Think like a predator. What information on your profile identifies who you are, where you hang out, and where you live? Never post this kind of information anywhere online. Your friends know how to find you.
Social Networking Tips for Keeping Yourself Safe Online

- You may be held responsible for inappropriate content on your profile that is in violation of the Terms of Service or Acceptable Use Policies of the Internet Service Provider or web site(s) you use.
Online Safety Quiz

1. I’m online and I meet someone my age in a chat room. Is it OK to give him or her my address or telephone number so we can get together? Yes or No

2. I have a digital picture of myself and someone I met online wants to see it. Is it OK to send it to that person? Yes or No

3. I’m visiting a site from a company or organization that I’ve heard of. They want my name and telephone number so I can enter a contest. Is it OK to enter? Yes or No
4. I’m in the middle of a chat session and someone says something really mean. Should I
   a. Say something mean back?
   b. Ask them to apologize?
   c. Don’t respond—tell an adult if it bothers me.

5. My parents and I have established rules as to what I can do on the Internet when I’m home, but I’m at a friend’s house. Should I go by my parents’ rules or do whatever my friend does?
   a. Go by your parents’ rules.
   b. Do whatever your friend does.
Online Safety Quiz

6. I’m online and I get a message from my Internet service provider asking for my password. They say they need it to fix my account. Should I give it to them? Yes or No

7. I met someone in a chat room who wants to get together. They live nearby. Can I arrange a meeting? Yes or No

8. If someone sends me an inappropriate message/material, I should
   a. Never reply to these messages and tell my parents so that they can notify our online service provider.
   b. Keep it a secret.
   c. Reply to the message and ask the sender to stop sending me messages.
Online Safety Quiz

9. If someone I meet online asks me to keep a secret from my parents, I should
   a. Keep the secret because they are my “cyber friend.”
   b. Tell all of my friends because it’s hard for me to keep a secret.
   c. Tell my parents because no one should ever ask me to keep secrets from my parents.

10. If someone is on my e-mail “buddy list,” “friend list,” or “contact list” and I only know that person online, he or she is
   a. My friend and someone I can trust.
   b. The person he or she claims to be.
   c. Someone I should be cautious about because I don’t know him or her well.
Online Safety Quiz

11. As I travel through cyberspace, I should never
a. Take a break and have a snack.
b. Use the Internet to help me with my homework.
c. Agree to meet someone in person who I have met online.

12. The “CyberTipline” is
a. A cool, new video game.
b. My online source to report child-sexual exploitations.
c. A web site where I can find information about UFO’s.
What is the CyberTipline?
www.cybertipline.com or 1-800-843-5678

- The Congressionally-mandated CyberTipline is a means for reporting crimes against children including:
  - Possession, manufacture, and/or distribution of child pornography
  - Online enticement of children for sexual acts
  - Child prostitution
  - Sex tourism involving children
  - Extrafamilial child sexual molestation
  - Unsolicited obscene material sent to a child
  - Misleading domain names, words, or digital images on the Internet

- Reports may be made 24-hours a day, 7 days a week online at www.cybertipline.com or by calling 1-800-843-5678.
The Internet is essential to our children’s education, future careers, and lives…

However, while teens, parents, and schools embrace technology for all of its benefits for our children, there needs to be awareness about its inherent risks, as well. By practicing a few simple safety measures, Internet dangers can usually be avoided.
Remember: Be smart about what you post on the Web and what you say to others while online. The Web is a lot more public and permanent than it seems.