Internet Safety For Our Children

Bergen County Prosecutor's Office
John L. Molinelli

DANGERS & RISKS:

HARRASSMENT & BULLYING

A child sent messages and communications that are demeaning, harassing and bullying in nature. Teenagers can communicate negative, hurtful messages via the Internet as a means to "bully" other young people.

SEXUALLY EXPLICIT MATERIALS & INAPPROPRIATE PREDATOR CONTACT

A child contacted through instant messages, chat rooms, and via e-mail by sexual predators who are seeking to engage and meet your child for the purpose of sex. Children are frequently exposed to pornography of all types while online.

VIRUSES & HACKERS

Materials and files downloaded by your child that contain a virus that could damage your computer. Hackers can gain remote access to your computer and get your private information.

FINANCIAL REPERCUSSIONS

Financial information is frequently given over the Internet, which could be used to assume your identity.

INTERNET COMMUNICATION:

Instant Messaging:

Instant messaging is comparable to a one-on-one phone conversation except with words on a screen instead of voices over a phone. Instant messaging requires a software application and some of the most popular ones are America OnLine, America OnLine Instant Messenger (AIM), and Microsoft Network (MSN). While it is a great way for kids to communicate with friends and family, predators use this technology to contact potential victims. Parents must therefore enforce strict rules that **prohibit children from instant messaging anyone they do not know**. This should be done through rules set by the parents as well as controls set on the particular software application. Just as you teach your children not to talk to strangers in the real world, so too should you **teach your children that they should not to talk with strangers in cyberspace.** Many of today's Instant Message programs also allow for voice conversations with the use of a simple computer microphone. **It is not uncommon for children to speak with adults unbeknownst to their parents.**

Chat rooms:

If Instant Messaging is like a phone call, then Chatting is like a conference call with many participants. Many companies, including America Online, Yahoo, and Microsoft, offer chat rooms. Chat rooms are designed for all types of people and topics. For adults it is a great way to meet people and discuss things with others that share a similar interest. For children, however, it is largely used to socialize. It is risky for children to chat with people they do not know and therefore **parents should regulate a child's access to chat rooms.** Sometimes chat rooms are setup for specific groups, like school and town recreation organizations. Thus it would be acceptable for a child to **be allowed to participate, enter and talk in a chat room when he or she knows all of the participants.**

Blogs /Social Networking: (My Space, Facebook, etc.)

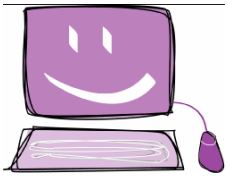
Blogs, short for Web Logs, are popular Internet spots for children. Sites such as myspace.com are spots where kids can have a personal web page. Parents must regulate and control the information that their children post on these sites. **Children should never post personal information or pictures on Blogs - or any other web site or profile for that matter.** Children should never represent themselves older than they actually are. All such sites should be set to private / invite only!

CAMERAS AND PICTURES

It is common for many kids to have their picture in their computer to send to people they communicate with. Children should never send their picture to anyone they do not know. Generally speaking, it is not wise to allow a child to have their picture in the computer – anyone they're communicating with online should already know what they look like. The same rules apply to the utilization of web cameras. These must be strictly regulated (if not disallowed) by parents. **Under no circumstances should a child have a computer with an Internet connection and a web camera in their bedroom.**

PEER TO PEER SOFTWARE:

Many kids use peer-to-peer software to download free music files. This software comes in many flavors: Limewire, Kazza, BearShare, eMule, just to name a few. There are several problems with allowing children to use peer-to-peer networks. First, any music downloaded freely from these sites is done so in violation of copyright laws. (This differs from legitimate paid sites such as iTunes). Second, when downloading from other peer-to-peer clients, children are often exposed to pornography, even child pornography. Finally, the very nature of the way of peer-to-peer technology functions puts your computer system at extreme risk from malicious software. It is the opinion of the Bergen County Prosecutor's Office that **unless a legitimate use of peer to peer technology can be shown, children should not be allowed to utilize the technology.**



HOW TO REDUCE RISKS:

Keep the Computer Family Public: The Internet connected computer should never be located in a child's bedroom or similarly secluded room.

Check-up On a Child's On-Line Activity: Parents should be aware of what their children are doing online. Frequent and surprise looks over a child's shoulder, checking the computer following a child's activity, and the implementation of software babysitters are a few of the ways to check up.

Implement Computer Parental Controls: Parents can filter, block, control, and/or record what a child views over the Internet. Service providers offer parental controls and software programs can be purchased to protect your children from access to inappropriate, sexually explicit, and violent materials or sites advocating contraband.

WHAT TO DISCUSS WITH CHILDREN:

1. Never talk to anyone online who you do not personally know. This rule applies to all forms of Internet communication: Instant Messaging, Chatting, On-Line Gaming Sites, and E-Mail.
2. Never enter a chat room where you don't know all of the participants. Chat rooms are popular locations for child predators to lurk about.
3. Never send your picture to anyone whom you do not know.
4. Never use a web camera or voice chat with anyone whom you do not know.
5. Control your personal information on line. This applies to your profile, blogs, personal web pages, or any other location where you could post information.
    a. Avoid posting your last name.
    b. Never post your address.
    c. Never post your phone number.
    d. Never post your picture on line.

6. Communicate on the Internet Responsibly:
    a. Do NOT engage in harassing behavior on-line. No name calling or posting nasty remarks about others. Bullying and Harassment are crimes in the State of NJ.
    b. Do NOT post personal information about other people – this could constitute a crime.
    c. Do NOT engage in threatening behavior online. Threats are taken very seriously and could result in arrest and the loss of your computer.
7. Surf the Web Responsibly:
    a. Do not visit sites that deal with pornography or other inappropriate topics.
    b. Utilize search engines (such as Google) responsibly. Innocent and legitimate searches can lead to accidental exposure to inappropriate sites. Be sure to read the text below your search engine results before clicking on the link and entering the site.