Child Safety on the Information Highway

***IMPORTANT NOTE**: This is the classic and first widely distributed Internet safety article, written first in 1993 and revised several times up until 2003. While much of the information is timeless, some is now out-of-date, especially for parents of teenagers who are using interactive "web 2.0" services like MySpace, Facebook and other social networking sites. Please realize that any advice varies by the age of the child, the values of the family and changes in technology. For up-to-date advice for teens, visit our sister sites ConnectSafely.org and SafeTeens.com.*

Larry Magid, March 2008

'Cyberspace,' the 'Web,' the 'Net,' the 'Information Highway'"

Whatever it's called, the majority of people in developed nations are now going online to exchange electronic mail (E-mail) and instant messages; participate in chat groups; post and read messages in social networking sites and blogs, "surf" the world wide web; and many other online activities. Children are no exception in fact they are more likely to be online than adults.

Personal computers are no longer the only method used for accessing the Internet. Children can go online from personal computers at home, a friend's house, in school, a library, club, or cafe. Many game consoles can be connected to the Internet and used for chatting and other online interaction. It is also possible to access the Internet on mobile devices such as cellular telephones and other handheld devices. In other words children don't have to be in the company of responsible adults to use the Internet.

Even though companies that provide Internet access strive to provide their subscribers with an enjoyable, safe, and rewarding online experience, it's not possible for these companies to monitor everyone who uses their service anymore than a local government can control the behavior of the people within its borders. Once you're connected to the Internet you're able to exchange information with people who use other providers unless you're using a service that offers restricted access such as blocking mail from outside the service or from people who aren't pre-approved by a child's parent.

There are no censors on the Internet. Anyone in the world — companies, governments, organizations, and individuals — can publish material on the Internet. A service provider links you to these sites, but it can't control what is on them. It's up to individuals to make sure that they behave in a way that's safe and appropriate.

Benefits of the Information Highway

"As an educational…tool users can learn about virtually any topic…"

There is a vast array of services available online. Reference information such as airline fares, encyclopedias, movie reviews, news, sports, stock quotes, and weather are readily available. Users can conduct transactions such as banking, making travel reservations, shopping, and trading stocks online. You can find information about your local schools, government, vital health matters, or read an out-of-town newspaper or watch TV and listen to radio from thousands of online "stations" around the globe. Hundreds of millions of people communicate through E-mail with family, friends, and colleagues around the world. Others use chat areas to make new friends who share common interests. You can even use the Internet to watch videos and listen to audio programs produced by major media companies, businesses, organizations, and individuals. In fact, there is a growing trend towards "user supplied" video that can vary in quality, content and suitability for a general audience. As an educational and entertainment tool users can learn about virtually any topic, visit a museum, take a college course, or play an endless number of computer games with other users or against the computer itself.

Most people who go online have mainly positive experiences. But, like any endeavor — attending school, cooking, riding a bicycle, or traveling, — there are some risks and annoyances. The online world, like the rest of society, is made up of a wide array of people. Most are decent and respectful, but some may be rude, obnoxious, insulting, or even mean and exploitative. Children get a lot of benefit from being online, but they can also be targets of crime, exploitation, and harassment in this as in any other environment. Trusting, curious, and anxious to explore this new world and the relationships it brings, children need parental supervision and common-sense advice on how to be sure that their experiences in "cyberspace" are happy, healthy, and productive.

Putting the Issue in Perspective

There have been some highly publicized cases of exploitation involving the Internet, but that doesn't mean that every child will experience major problems. The vast majority of people who use the Internet do not get into serious trouble.

Many people, including children, have been confronted with material that is disturbing or inappropriate. There are steps parents can take to try to shield their children from such material, but it's almost impossible to completely avoid all inappropriate material. Sadly there are some cases where children have been victimized by serious crime as a result of going online. Parents can greatly minimize the chances that their children will be victimized by teaching their children to follow our basic safety rules. **The fact that crimes are being committed online, however, is not a reason to avoid using the Internet.** To tell children to stop using the Internet would be like telling them to forgo attending school because students are sometimes victimized or bullied there. A better strategy would be to instruct children about both the benefits and dangers of "cyberspace" and for them to learn how to be "street smart" in order to better safeguard themselves in any potentially dangerous situation.

What Are the Risks?

There are a few risks for children who use the Internet or other online services. Teenagers are particularly at risk because they often go online unsupervised and are more likely than younger children to participate in online discussions regarding companionship, relationships, or sexual activity. If you have a teen in your family or you are a teenager, check out **Teen Safety on the Information Highway** or order a free copy by calling 1-800-843-5678.

Some risks are

- ***Exposure to Inappropriate Material***

A child may be exposed to inappropriate material that is sexual, hateful, or violent in nature, or encourages activities that are dangerous or illegal. Children could seek out such material but may also come across it on the web via chat areas, social networking sites, E-mail, or even instant messaging if they're not looking for it.

- ***Physical Molestation***

A child might provide information or arrange an encounter that could risk his or her safety or the safety of other family members. In some cases child molesters have used chat areas, E-mail, and instant messages to gain a child's confidence and then arrange a face-to-face meeting.

- ***Harassment and Bullying***

A child might encounter messages via chat, E-mail, on their social networking site or their cellular telephones that are belligerent, demeaning, or harassing. "Bullies," typically other young people, often use the Internet to bother their victims.

- ***Viruses and Hackers***

A child could download a file containing a virus that could damage the computer or increase the risk of a "hacker" gaining remote access to the computer; jeopardizing the family's privacy; and, perhaps, jeopardizing the family's safety.

- ***Legal and Financial***

A child could do something that has negative legal or financial consequences such as giving out a parent's credit-card number or doing something that could get them in trouble with the law or school officials. Legal issues aside, children should be taught good "netiquette" which means to avoid being inconsiderate, mean, or rude.

How Parents Can Reduce the Risks

While children need a certain amount of privacy, they also need parental involvement and supervision in their daily lives. The same general parenting skills that apply to the "real world" also apply while online. If you have cause for concern about your children's online activities, talk to them. Also seek out the advice and counsel of teachers, librarians, and other parents. Having open communication with your children, using computer resources, and getting online yourself will help you obtain the full benefits of these systems and alert you to any potential problem that may occur with their use. If your child tells you about an upsetting message, person, or web site encountered while online, don't blame your child but help him or her avoid problems in the future. Remember — how you respond will determine whether they confide in you the next time they encounter a problem and how they learn to deal with problems on their own.

Beyond these basics, there are some specific things that you should know about the Internet. For instance did you know that there are chat areas, newsgroups, and web sites that have material that is hateful, is violent, or contains other types of material that parents might consider to be inappropriate for their children? It's possible for children to stumble across this type of material when doing a search using one of the web sites that is specifically designed to help people find information on the Internet.

Most of these sites, called “search engines,” do not, by default, filter out material that might be inappropriate for children, but some offer a child safe option and some are designed specifically for use by children.

Also the Internet contains newsgroups, web sites, and other areas designed specifically for adults who wish to post, read, or view sexually explicit material including pictures, stories, and videos. Some of this material is posted on web sites where there is an attempt to verify the user’s age and/or a requirement for users to enter a credit-card number on the presumption that children do not have access to credit-card numbers. Other areas on the Internet make no such effort to control access. Nevertheless, consider monitoring your credit-card bills for such charges. In addition to “adult” pornography, there are also areas on the Internet that contain illegal child pornography. If you or your children come across this type of material, immediately report it to the National Center for Missing & Exploited Children’s (NCMEC) CyberTipline® at www.cybertipline.com.

Some internet service providers allow parents to limit their children’s access to certain services and features such as adult-oriented “chatrooms,” bulletin boards, and web sites. There may be an area just for children where it is less likely for them to stumble onto inappropriate material or get into an unsupervised “chatroom.” At the very least, keep track of any files your children download to the computer, consider sharing an E-mail account with your children to oversee their mail, and consider joining them when they are in private chat areas.

In addition there are ways to filter or control what your children can see and do online. One type of filter, called a “spam” filter limits unsolicited E-mail including mail promoting sexually explicit material. Some service providers include filters as part of their service but, if not, there is software you can purchase that will attempt to limit the type of mail that gets through.

There are also ways to filter what a child can see on the world wide web. Check with your service provider to see if they offer age-appropriate parental controls. If not consider using a software program that blocks chat areas, newsgroups, and web sites that are known to be inappropriate for children. Most of these programs can be configured by the parent to filter out sites that contain nudity, sexual content, hateful or violent material or that advocate the use of alcohol, drugs, or tobacco. Some can also be configured to prevent children from revealing information about themselves such as their name, address, or telephone number. You can find a directory of these filtering programs at kids.getnetwise.org/tools/. Also, the latest versions of both Microsoft Windows (Vista) and Apple’s OS X have parental control tools that can limit what you child can do online.

Another option is to use a rating system that relies on web-site operators to indicate the nature of their material. Internet browsers can be configured to only allow children to visit sites that are rated at the level that the parents specify. The advantage to this method is that only appropriately rated sites can be viewed. The disadvantage is that many appropriate web sites have not submitted themselves for a rating and will therefore be blocked.

While technological-child-protection tools are worth exploring, they’re not a panacea. To begin with, no program is perfect. There is always the possibility that something inappropriate could “slip through” or something that is appropriate will be blocked. Finally, filtering programs do not necessarily protect children from all dangerous activities. And even though they might block children can **see** online, they might not block what they can **say**. For example, even with a filter it might be possible for a child to post inappropriate material or personal information on a social networking site or blog or disclose it in a chat room or instant message. Also some filters do not work with peer-to-peer networks that allow people to exchange files such as music, pictures, text, and videos. These peer to- peer networks are sometimes used to distribute pornography, including child pornography. Filters are not a substitute for parental involvement. Regardless of whether you choose to use a filtering program or an Internet rating system, the best way to assure that your children are having positive online experiences is to stay in touch with what they are doing. One way to do this is to spend time with your children while they're online. Have them show you what they

If a meeting is arranged, make the first one in a public place. And be sure to accompany your child. do, and ask them to teach you how to use the Internet or online service. You might be surprised by how much you can learn from your children.

Guidelines for Parents

Set reasonable rules and guidelines for computer use by your children

By taking responsibility for your children's online computer use, parents can greatly minimize any potential risks of being online. Make it a family rule to

- Never give out identifying information — home address, school name, or telephone number — in a public message such as chat or newsgroups, and be sure you're dealing with someone both you and your children know and trust before giving out this information via E-mail. Think carefully before revealing any personal information such as age, financial information, or marital status. Do not post photographs of your children in newsgroups or on web sites that are available to the public. Consider using a pseudonym, avoid listing your child's name and E-mail address in any public directories and profiles, and find out about your ISP's privacy policies and exercise your options for how your personal information may be used.
- Get to know the Internet and any services your child uses. If you don't know how to log on, get your child to show you. Have your child show you what he or she does online, and become familiar with all the activities that are available online. Find out if your child has a free web-based E-mail account, such as those offered by Hotmail and Yahoo!® , and learn their user names and passwords.
- Never allow a child to arrange a face-to-face meeting with someone they "meet" on the Internet without parental permission. If a meeting is arranged, make the first one in a public place, and be sure to accompany your child.
- Never respond to messages that are suggestive, obscene, belligerent, threatening, or make you feel uncomfortable. Encourage your children to tell you if they encounter such messages. If you or your child receives a message that is harassing, of a sexual nature, or threatening, forward a copy of the message to your ISP, and ask for their assistance. Instruct your child not to click on any links that are contained in E-mail from persons they don't know. Such links could lead to sexually explicit or otherwise inappropriate web sites or could be a computer virus. If someone sends you or your children messages or images that are filthy, indecent, lewd, or obscene with the intent to abuse, annoy, harass, or threaten you, or if you become aware of the transmission, use, or viewing of child pornography while online immediately report this to the NCMEC's

CyberTipline at 1-800-843-5678 or www.cybertipline.com. Set reasonable rules and guidelines for computer use by your children.

- Remember that people online may not be who they seem. Because you can't see or even hear the person it would be easy for someone to misrepresent him- or herself. Thus someone indicating that "she" is a "12-year-old girl" could in reality be a 40-year-old man.
- Remember that everything you read online may not be true. Any offer that's "too good to be true" probably is. Be careful about any offers that involve you going to a meeting, having someone visit your house, or sending money or credit-card information.
- Set reasonable rules and guidelines for computer use by your children. (See "My Rules for Online Safety" on the back cover.) Discuss these rules and post them near the computer as a reminder. Remember to monitor your children's compliance with these rules, especially when it comes to the amount of time your children spend on the computer. A child's excessive use of online services or the Internet, especially late at night, may be a clue that there is a potential problem. Remember that personal computers and online services should not be used as electronic babysitters.
- Check out blocking, filtering, and ratings applications. Be sure to make this a family activity. Consider keeping the computer in a family room rather than the child's bedroom. Get to know their "online friends" just as you get to know all of their other friends. If your child has a cellular telephone, talk with him or her about using it safely. The same rules that apply to computer use, also apply to cellular telephones.

About this Document

This document was written by Larry Magid, a syndicated columnist and technology commentator, who is coauthor of MySpace Unraveled (Peachpit Press) and host of www.safekids.com, a web site devoted to keeping children safer in "cyberspace." He is also the author of Teen Safety on the Information Highway, a free brochure that is also published by the National Center for Missing & Exploited Children.

The National Center for Missing & Exploited Children (NCMEC) is the national clearinghouse and resource center funded under Cooperative Agreement #98-MC-CX-K002 from the Office of Juvenile Justice and Delinquency Prevention, Office of Justice Programs, U.S. Department of Justice. Points of view or opinions in this work are those of the author and do not necessarily represent the official position or policies of the U.S. Department of Justice or Bureau of Immigration and Customs Enforcement, U.S. Department of Homeland Security.

Additional edits 2007 by Larry Magid (not vetted by National Center for Missing and Exploited Children).

For more information on child safety, please contact the Charles B. Wang International Children's Building 699 Prince Street Alexandria, Virginia 22314-3175 1-800-THE-LOST® (1-800-843-5678) www.missingkids.com ®

Trackback URI | Comments RSS

Safety Myths and Web 2.0

Kids today live in an interactive “Web 2.0″ world where they socialize, post photographs and videos and share common experiences with friends, friends of friends and, in some cases, strangers. Millions of kids are doing it every day and the overwhelming majority of them seem to be doing just fine. But that doesn’t mean that the social Web is a danger-free zone. There are things teens, parents, teachers and other caregivers need to think about to ensure that online socializing remains “smart socializing.”

Let’s start by dispelling one popular myth. Your kids don’t have all the answers when it comes to the use of technology. They may know more about how to operate a computer or a cell phone or put a page up on a social networking site, but just because some adults are a bit technologically challenged doesn’t mean that they have no place supervising kids’ use of technology. Adults have one thing that teens don’t have - life experience - which for most translates into wisdom. Adults know, for example, that things aren’t always what they appear to be. They know that while most people in this world are decent and caring, there are a few who will take advantage of others and you can find these people on the Internet just as you would in “the real world” (though, for teens there is no distinction between the Internet and “the real world.” The Internet is a big part of their world).

But there are other myths that we must also dispel. One is that Internet predators typically deceive their victims by lying about their age or their gender. While that is possible, it’s usually not the case. Research has shown that most adults who attempt to engage in a physical relationship with a minor do not grossly exaggerate their age. In most cases, the young person is aware that that person is an adult prior to the meeting.

To be sure, there are predators who would harm children. That’s one reason that it’s important for kids to be cautious when communicating with people they don’t know in person, especially if the conversation starts to be about sex or physical details. Fortunately most teens are pretty careful which is why there is a fairly small number of cases of teens who are physically harmed by these criminals. Still, one case is too many and if you hear about a case of someone using the Internet to groom or lure a minor into a sexual situation or if you find sexual images of children (child pornography), call local authorities and report it at CyberTipLine.com.

If you don’t get together with someone you meet online, they can’t physically harm you so your safest bet is to avoid meeting such people in the real world. If a teen does get together with someone it should be in a very public place and they should bring along a parent, a group of friends or maybe the football team and cheerleading squad. You never want to meet someone in person in a way that could make you vulnerable.

Another thing we know about threats to teens and children is that they don’t always come from adults and they’re often from someone they know. Kids can and sometimes do harm other kids. Threats often come from peers kids know from school or other real world situations. Whether it’s unwanted sexual advances, harassment or what’s now called “cyber bullying,” peer to peer threats are real and can be harmful.

If a teen or child is being bothered or harassed by anyone the best advice is to not respond to that person and tell someone. That should include a parent, guardian or teacher but, for teens, it can also include trusted friends. Sometimes kids can handle the situation on their own or in groups but at other times it requires adult intervention and, in serious cases, maybe even the police. Not all harm is physical. Cyber bullying can be emotionally devastating.

For adults - whether parents, teachers, administrators or authorities, it's important to listen and provide support to a child or teen who is scared, worried or bothered by such contact but not to overreact or "punish the victim" by taking away Internet privileges or forcing them to avoid using social networking sites or other services. The fear of an adult overreacting is one of the reasons many teens give for not coming forward if they have a problem.

Parents also need to know that taking away a teen's online privileges could backfire by prompting him or her to go into stealth mode by finding hidden ways to get online. If you take away a child's online profile for a service, he or she can easily create another one or - worse - find a service that doesn't even try to enforce basic safety rules. And if you ban teens from using a computer or attempt to filter what they can access, the young person can find another way to get online including friends' computers or a cell phone. Modern phones have web browsers and some even have special software for getting onto social networks.

Which all leads to the fact that - regardless of what technology parents try to employ, the best filter is the one that runs in the young person's brain - not on a computer.

Cell phones can also be used to bully and harass a young person. Text messages can sometimes be hurtful. And some phones have global positioning systems and software that allow teens to broadcast their location. Kids need to know how to use the privacy features these services offer to be sure they aren't easily locatable by people they don't trust.

Finally, Internet safety is a two-way street. Kids should be good online citizens and not harm, threaten or bully others for two reasons. First because it's wrong and second because it can get them in trouble with authorities, parents and even other kids.

New Approach to Online Safety Education

More than a dozen years ago I wrote a booklet for the National Center for Missing and Exploited Children called Child Safety on the Information Highway. Millions of copies are in print and countless people have seen it online. The first item in the child safety rules was "I will not give out personal information such as my address, telephone number, parents' work address/telephone number, or the name and location of my school without my parents' permission." But new research suggests that my Rule No.1 may have been an overstatement.

I still don't think anyone should give out their home address or phone number in a public forum, but it's also important to face the reality of how today's youth are using social networks and consider new data that suggest that as far as sexual solicitation is concerned, there are greater risks than disclosing personal information.

David Finkelhor, director of the Crimes against Children Research Center
at the University of New Hampshire, said that a recent study conducted by his center "suggests the need for a somewhat different approach to Internet safety education." The study, said Finkelhor, "finds that giving out personal information online (one of the key prevention strategies emphasized in safety education) does not really increase a youth's risk for sexual solicitation." The emphasis, instead, should be about "making a lot of online acquaintances and talking with them about sex." The study appeared in the February issue of the Archives of Pediatric and Adolescent Medicine.

The data is consistent with other recent findings that have caused the National Center for Missing and Exploited Children to no longer focus on "stranger danger" but rather the types of interactions that children are having with other people, including both strangers and acquaintances.

The often quoted study found that one in seven young people who use the Internet "reported an unwanted interpersonal victimization in one year's time" yet 55 percent of the youth reported having posted personal information. Of those, 80 percent gave out their age or year of birth, 61 percent gave out their real last name, telephone number, school name or home address and 33 percent posted a picture. In other words, giving out personal information is common practice, despite what I and other Internet safety advocates have been saying for years.

The authors also looked at other forms of potentially risky or inappropriate behavior and found that one in three had someone in their buddy list they didn't know in person. They also found that 9 percent had harassed or embarrassed others online and 28 percent had made rude or nasty comments to someone on the Internet. They found that 5 percent of the sample said they had engaged in "talking about sex with someone they met online." Specifically, 2.2 percent of the sample had one such encounter, 2 percent had two and only 1 percent had talked about sex online with a stranger 3 or more times.

When the researchers estimated the association between these risky behaviors with Internet victimization, they discovered that that talking about sex with someone known only online three or more times was associated with a 3-fold increase in the likelihood of being a victim. On the other hand, neither posting nor sending personal information was significantly related to being a victim.

What’s more, there is also a connection between a youth’s rude behavior and his or her chances of becoming a victim. “Youth who engage in online aggressive behavior by making rude or nasty comments or frequently embarrassing others are more than twice as likely to report online interpersonal victimization,” the study reports.

The authors also found that, “as the number of different types of behaviors online increased, so too did the odds of online interpersonal victimization.” Young people who engaged in four types of risky behavior “were 11 times more likely than those reporting none of the online behaviors to also report online interpersonal victimization.”It’s no surprise to me that kids who engage in sexual conversations with strangers they meet online are at a greater risk of becoming victims.While there is no activity that can ever justify victimizing another person, it is also true that there are certain activities that put us at greater risk, and talking about sex with a stranger is clearly one of them. I’m also not terribly surprised to find that engaging in rude or harassing behavior is also associated with becoming a victim. Showing a disregard for others is often associated with disregarding one’s own safety and well being.In a funny kind of way, I’m relieved to learn that giving out personal information may not be as dangerous as we once thought. For better or worse, we’re at a stage where millions of young people are publishing at least some information about themselves on social networking services. When I perused public profiles of teens on MySpace and other services about a year ago, I noticed lots of kids had posted photos and most disclosed the name of their school and many had other personal information, sometimes even last names. But both MySpace and the kids who use it are getting smarter.Last August MySpace introduced new privacy policies that make possible for anyone to maintain a private profile and, according to a 2006 study conducted by Dr. Justin at the University of Wisconsin-Eau Claire and Dr. Sameer Hinduja at Florida Atlantic University, kids are more privacy conscious than adults may realize.The researchers found that 91 percent of teen profiles they looked at didn’t include full names and 40 percent of teens had private profiles. This tracks with a 2006 survey from the Pew Internet & American Life Project that reports “66 percent of teens who have created a profile say that their profile is not visible to all internet users. They limit access to their profiles.”But there is still plenty of personal information out there. Patchin and Hinduja found that 57 percent of profiles had at least one photo and 9 percent had the teen’s full name. 81 percent revealed city they live in while 28 percent named the school they attend. Bottom line: kids are posting some personal information but most are being selective about it.

Both these studies suggest that we need to take another look at risk factors before we preach to our kids or start passing laws that restrict use of these services. The Wisconsin and Pew studies suggest that most kids are getting the message but that a significant minority is still revealing too much information. The New Hampshire study concludes that revealing personal information is less risky than other types of behavior.While pouring through research data can be murky, the take away for parents is relatively clear. Talk with your kids about their online behavior and focus on the big picture. Rather than make them paranoid of strangers, make them aware that how they interact with people can have an impact on how they are treated and whether they will likely be victimized. Keeping your personal information personal is still a very good idea, but knowing where to draw the boundaries in online conversations can go a long way towards keeping kids safe.