Teen Safety on the Information Highway
by Larry Magid

Revised 2004

a publication of the National Center for Missing and Exploited Children

General Information

Whatever your age, the Internet is a great place to hang out. It's not only fun, but it lets you keep in touch with friends and family and provides an enormous amount of information. There are lots of great educational sites as well as places to keep up with your favorite hobbies, music, sports, and much more. If you're a teen, we probably don't need to sell you on the benefits of the Internet. Many of you know far more than your parents or even teachers about the wonders of cyberspace. If you're a parent, talk to your children about "the Net" and — if you need to learn more — see if they can help you. Either way, it's important for teens and parents to share knowledge. You have something to learn from each other — if not about the Internet, then about life in general, how to make good decisions, and how to look at information critically.

Cyberspace is like a big city. There are libraries, universities, museums, places to have fun, and plenty of opportunities to meet wonderful people from all walks of life. But, like any community, there are also some people and areas that you ought to avoid and others that you should approach only with caution.

By knowing the dangers and how to avoid them, you can take advantage of all the positive aspects of the Internet while avoiding most of its pitfalls.

If you're a teen, or a parent of a teenager, you might feel that you don't need the same restrictions and controls as younger kids. You may be right, but just because you're older doesn't mean that you're out of danger. Teenagers are actually more likely to get into trouble online than younger children. Teens are more likely to explore out-of-the-way nooks and crannies of cyberspace; they're more likely to reach out to people outside of their immediate peer groups; and, sadly, they're more often preyed upon as victims by child molesters and other exploiters.

How do I get into Cyberspace?

There are lots of front doors to cyberspace, including Internet service providers and online services, which can provide you with an account that gives you access to everything on the public Internet. This includes chatrooms, discussion groups called newsgroups, Email, file libraries, instant messaging, web sites, and lots of other services including those that give you the ability to listen to music and view videos.

Most people think of computers as the only way to get online, but it's possible to reach into cyberspace from other devices including cellular telephones, personal digital assistants, and even video-game consoles. Some video-game systems, for example, are Internet enabled so you can compete against — and chat with — players around the world.

Most cellular telephones can also be used to exchange instant messages, send E-mail, and surf the web. Exchanging short messages, called "texting," is growing in popularity in the United States. Many cellular telephones also have color screens and builtin digital cameras making it possible to exchange photographs. As cellular telephone companies "roll out" faster and more advanced features, the cellular telephone is becoming a viable alternative for getting on the Internet. Unlike a personal computer (PC), it can be used anywhere.

While companies that provide Internet service can, in certain situations, exercise some control over the type of content and "customer conduct" in its own areas, the services have no control or jurisdiction over what takes place on the Internet as a whole. And even within their own areas, these services can't possibly monitor everything that happens. So, even if you're going online using one of these services, you're not completely protected from the larger dangers.

Before going into the dangers, let's put this into context. Millions of teenagers go online every day, and most are safe. The way to stay safe is to understand the dangers and follow some simple rules to help you stay out of trouble. By following these rules you minimize the risks, but you can never completely eliminate all risks in life.

General Risks

Situations and Behaviors that Make You Feel Uncomfortable

Not everything that can go wrong in cyberspace necessarily puts you in physical danger. There are chatrooms, newsgroups, web sites, and other places online containing material that could make you feel uncomfortable. It could be material that's sexual and/ or violent in nature. It could be material espousing hateful attitudes or discussing activities that you find repulsive or unpleasant. It really doesn't matter what it is. What does matter is that you have the right – and the tools – to instantly remove yourself from any area where you feel you shouldn't be.

Teens have been bullied, harassed, or "hit on" by others while in chatrooms, instant messaging sessions, or on their cellular telephones. Sometimes the people responsible for this inappropriate behavior are fellow teens or young adults, but that doesn't make it OK. At other times, it can be older adults posing as teenagers. Either way, no one should have to put up with rudeness or unwanted sexual banter.

Putting Yourself in Physical Danger

The most serious risk you can face involves the possibility of someone hurting or exploiting you because of information that you post or someone else posts about you online or because of something you do or somewhere you go as a result of what you encounter online. The number of teens who are molested, abducted, or leave home as a result of contacts made on the Internet are relatively low, but when it happens the results can be tragic.

Giving Up Privacy Or Putting Yourself or Your Our Family In Financial Risk

The Internet, like so many other places in this world, is home to people who would try to take money from you or your family or just pester you with unwelcome advertising and marketing material. Be especially wary of any "get rich quick" schemes that promise to help earn you lots of money in your

spare time or offers that will help you lose weight quickly or enhance your appearance. If something sounds "too good to be true," it probably is.

Harassment and Bullying

Not everyone in cyberspace minds his or her manners. When you're online, especially in bulletin boards or chatrooms, there is a chance that you'll get messages that are demeaning, harassing, or just plain mean. Don't take it personally. A message that is demeaning says a lot more about the sender than it does about the person who gets it. Ironically, even people who are nice in the "real" world can forget their manners when they go online. The best thing to do if you encounter messages or people in chatrooms who are acting that way is to ignore them. Some messages, however, may constitute harassment, which is a crime under federal law. If someone sends you messages or images that are filthy, indecent, lewd, or obscene with the intent to abuse, annoy, harass, or threaten you, report it to your Internet service provider and the National Center for Missing & Exploited Children's CyberTipline® at www.cybertipline.com or by calling 1-800-843-5678. You should also report it to school authorities if the incident takes place at school or involves other students from your school.

Hurting Others and Getting into Trouble

Avoid anything that might hurt people and risk getting you into trouble. You need to respect other people's privacy and avoid taking any actions that annoy, harass, or hurt other people. You are responsible for your behavior online.

Risks by Area

The Web

Web sites give you the opportunity to read newspapers, tour museums, check out libraries, visit distant lands, play games, look at pictures, shop, or do research to help you with your homework. You can pursue your hobbies, plan vacations, and do much more. There are millions of web sites on just about every topic imaginable.

Did You Know? Some web sites are wonderful, others are kind of dumb, and some contain so-called "adult" images and other material that teens should avoid. Still others are demeaning, racist, sexist, and violent or contain false information. Some of these sites contain material that can be disturbing, even for adults. If you wander into any of these areas, it's best to immediately leave by clicking on the Home icon, going to another site, or shutting down your browser.

Caution: In addition to displaying information, web sites sometimes ask you for information about yourself. The site may ask for your name, your mailing address, your E-mail address, and other information before letting you in. It may entice you to provide information in exchange for sending you a promotional item or entering you in a contest. Never enter any information about yourself without first checking with your parents.

When you enter information on a web site or any place on the Internet, you're giving up a bit of your privacy. At best, your name could wind up in some database, probably to be used to sell you something now or later. At worst, it could be used to harm or exploit you. Just because a web site seems to be operated by a reputable organization or individual doesn't mean that it necessarily is what it seems to be. Anyone – including creeps and criminals – can set up their own web site. So be extremely cautious

before telling the “web master” anything about yourself. This is especially true with sites that contain adult material.

Also be careful about downloading anything from a web site. Some web sites ask your permission to download a program or “plug-in.” In some cases these programs can be used to display unwanted advertising on your computer but they can do far more including invading your privacy by tracking what you’re doing online. They can also plant viruses or increase your risk of a “hacker attack.” Don’t download anything unless you’re certain it is from a trustworthy source.

Some teenagers have their own web sites or post material to web sites maintained by their school or an organization. That’s terrific, but if you do post something on the web, be sure to never include your home address, telephone number, or photograph. If you do want people to be able to contact you through the web, just give an E-mail address.

Chatrooms

Chatrooms let you engage in a live conversation with people around the block or around the world. It’s like being on a party line, only you type instead of talk. Everyone in the “chatroom” can see everything you type. The types of chatrooms vary depending on the service you’re using. Some chatrooms are just open conversations. Everyone has a pretty much equal role. Some rooms are moderated where there is a “speaker” who is leading the discussion and participants. Some rooms have chaperons or monitors who are responsible for maintaining order, but even in some of these rooms what you type is immediately displayed. The monitor can kick someone out of the room who is acting in an inappropriate manner, but he or she may be able to act only after the fact. The monitor can’t, however, prevent you from going off to a private chat area with a person who might do you harm or typing information that could put you in danger.

Did You Know? Chat is probably the most dangerous area on the Internet. As with other areas of the Internet, you don’t know who is there, so never say anything in a chatroom that you wouldn’t say in public.

Beyond that it’s not uncommon for people to make “friends” in chatrooms. You enter a room; start a conversation with someone; and, before you know it, you’ve established a relationship of sorts. That relationship could turn out OK, but there are some not-so-happy stories. Chatrooms are sometimes used by people to exploit others. To put it bluntly, chatrooms – especially those used by teenagers – are sometimes also used by child molesters to find victims. Adults or even older teens seeking to exploit younger people don’t necessarily tell the truth about who they are. Even teens your own age could pose a threat or harass or bully you. You have the right to remain in control of your own experiences, and don’t accept abuse from anyone.

You might meet someone in a room who appears to be sympathetic and understanding and offers you wonderful advice and counsel. If the relationship remains strictly online, that could be OK as long as you’re careful not to give out any personal information.

Caution It can be tempting to get together with someone you meet in a chatroom, but remember – people are not always who they seem to be. The basic rules for online safety apply to all areas of the Internet, but they are especially important in chat areas. Never give out personal information, and never arrange a face-toface meeting with someone you meet in a chatroom without first checking with your parents and taking the precautions list ed in “Never Get Together With Someone You ‘Meet’ Online”

Chatrooms are sometimes organized around topics, so avoid any topic area that makes you feel uncomfortable. But just because a chatroom is designed around a particular topic doesn't mean that other topics aren't discussed. 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.

Be especially careful of chatrooms that get into subjects that might be associated with sex or cults or groups that practice potentially dangerous rituals. It might seem interesting or even fun to discuss actions that you might never consider engaging in, but some people who fantasize about things also like to carry them out.

Be suspicious of anyone who tries to turn you against your parents, teachers, or friends. They may have a hidden agenda.

On some services and web sites you can enter into a private chat area. Once there you can arrange to meet friends. In some cases those rooms are truly private. But in other cases they may be listed in a directory of rooms. If so, there is nothing to stop others from entering those rooms.

One trick to avoid harassment, especially for women and girls, is to choose a gender-neutral name – like your initials or a word – to use in a chatroom. It's fine to be cute or funny with the name you choose, but be sure it doesn't identify you and doesn't have any meaning or implication that might encourage others to bother you.

Instant Messaging

Instant messaging (IM) has become extremely popular among teenagers. It's 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 cellular telephones or between computers and cellular telephones or any other Internet connected devices.

As great as it is, IM can be a dangerous way to interact with people. As with chatrooms, you need to be extremely careful about whom you are "IMing" with and what you are saying. Never give out any personal information in an instant message unless you are 100 percent sure of who is connected. Also be aware that some instant message services make it possible to exchange messages with several people at once — just like a chatroom.

Some instant messaging software can also be used for video chat where you send your picture — in real time — along with your words. Be very careful about your privacy if you have any type of camera attached to your computer, and be aware that it might be possible for others to send you unwelcome images.

Some services encourage you to post a "profile" with information such as your age, sex, hobbies, and interests. While such profiles can help you meet likeminded people, they can also make you the subject of harassment or worse, even if you don't post your name and address or other information that could lead to a physical contact. To be safe and avoid hassles it's better not to have a public profile.

Caution: Be sure you know who you are "IMing" with, and be aware that anything you type could be forwarded to other people. There is no way to "take back" something once you enter it. Be especially careful about using video or digital cameras during an IM session. You don't have to respond to any

messages that are rude, annoying, or make you feel uncomfortable.

Email

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

Did You Know? Increasingly, people and companies are using Email to send out messages to thousands of people at a time, encouraging them to buy something, do something, or visit a web site. The process, known as "spamming," can be intrusive and annoying. Because E-mail is essentially free, "spammers" can send out thousands or even millions of messages at little or no cost. Some use spamming to try to entice people to visit sexually explicit web sites. Each E-mail message that you send and receive contains a return address. What many people don't realize is that the return address can be fake. So, just because you get a message from "grandma@cottage.com" doesn't mean it's really from grandma. It could really be from "wolf@bigfangs.com."

E-mail also contains other information called a "header" that provides more information about who sent the message and where it came from. Understanding the header information can be difficult, but if you ever receive an E-mail message that is belligerent, threatening, or contains material that makes you feel uncomfortable, you should report it to your Internet service provider and ask them to investigate where it came from. If the material appears to be illegal in nature, you should report it to the CyberTipline at www.cybertipline.com or call 1-800-843- 5678. Illegal material includes threats to your life or safety, threats to others, pornographic images of children, and evidence of other crimes. NCMEC will refer this report to the appropriate law-enforcement agency.

Caution Be careful how you respond to E-mail from people you don't know. Remember, the sender might not be who he or she seems to be. Never send a photograph of yourself or any personal information to someone you don't know. Also, E-mail can easily be copied and forwarded to others. So if you do send personal information to friends, be sure that they are willing to respect your privacy.

In general it's best not to respond to spam mail or mail from someone you don't know. By responding you are verifying a valid E-mail address to the sender, and that information can be used to encourage a person who may send inappropriate E-mails or get you on even more lists. If you receive a message containing material that is sexually explicit, violent, or advocates something that is illegal or simply makes you feel uncomfortable, show it to your parents and report that message to your Internet service provider. You can usually find that address on the service's main web page (www.servicename.com). When in doubt, report the message to postmaster@servicename.com (substitute the name of your service for "servicename").

Peer-To-Peer

Peer-to-Peer (P2P) systems make it possible for people to exchange files without necessarily having to go through a web site or other centralized system. Napster, the most famous of these services, was used by millions to exchange music files until it was shut down by a court after the music industry sued Napster over alleged copyright violations. Napster has re-emerged as a legal music downloading service, operating with the consent of the recording industry.

There are plenty of other P2P systems including some that allow you to exchange other types of files including video, photographs, text documents, and software. Aside from the legal and ethical issues

regarding the unauthorized sharing of copyrighted material, there are some very serious safety issues regarding these services.

To begin with, some of the files you can download — including photographs and videos — might contain disturbing and inappropriate material. There are also cases where these services have been used by child molesters to exchange illegal images of children. It's also possible that these services could invade your privacy and slow down your Internet access. The whole concept behind P2P file-sharing systems is that users who download files are encouraged to upload them as well. Many of these services, by default, will turn your PC into a server that shares your files. That can place you in legal jeopardy, and it could also make it possible for others to gain access to information on your computer including personal photographs, videos, sound files, and other documents. What's more it can also cause problems for other computers if you're on a business, home, or school network.

Another problem with file-sharing services is that the software used to access them can sometimes come with some unwelcome extra "features" such as "spy ware" programs that can invade your privacy and display unwelcome advertising.

If you do use a file-sharing service, be very careful about what "permissions" you give it when you set it up. Avoid sharing your own files and decline any offers to install extra software. Even then, there is no guarantee that you might not experience problems as a result of having the software on your computer.

Newsgroups, Forums, and Bulletin Boards

Newsgroups, sometimes called bulletin boards or forums, are places where you can read and post messages or download or upload files. Unlike chatrooms, newsgroups are not live or "real time." If you post a message it remains on the newsgroup for people to look at later. Newsgroups can also be used to post files including computer programs, illustrations, pictures, and stories.

Did You Know? There are newsgroups on almost every possible subject, and they are often used as ways to get questions answered and share information about hobbies, musical groups, or any other subject of interest. Unfortunately, newsgroups, like other areas of cyberspace, have risks.

Caution The biggest risk is that you might post something that reveals information about yourself. Even if you are responding to a particular individual's posting, what you type, in most cases, is available for anyone to see. So, once again, remember the basic rules and never reveal identifying information about yourself. In many cases the mere act of posting something makes your E-mail address public. Even if you don't say anything revealing, your address will be available for people to send you E-mail that could be bothersome, and newsgroups are a favorite place for people who send out junk mail ("spam") to gather addresses.

There are newsgroups that contain sexually explicit illustrations, photographs, and stories. In some cases this material may be illegal especially if it contains images of people who are younger than the age of 18 or certain other material that has been defined as "obscene." Some of this material can be disturbing and should be avoided. It is dangerous to post anything in these types of groups because anything you type reveals your E-mail address that could then reveal your identity or at least subject you to unwanted E-mail. Remember, anytime you post to a newsgroup you are broadcasting your E-mail address, even if you don't include your actual name.

Educate Your Parents

Your parents spent more than a decade educating you and teaching you about things they know. Now it's your turn. Regardless of whether your parents are Internet novices or technology gurus, there are probably things you know about the Internet that they don't. This is a great opportunity for you to show them what you do online and, perhaps, help them get more out of the Internet themselves. Hey, it could be the start of a whole new relationship.

Basic Rules of Online Safety for Teens

The most important thing to remember is that when you're online in any kind of a public forum, you're out in public and anyone can read whatever you post. You should never post anything on the Internet that you wouldn't want known to the public at large. You should also remember that people you meet in cyberspace might not be who they seem to be. If you're in any type of public forum, avoid giving out your full name, your mailing address, your telephone number, the name of your school, or any other information that could help someone determine your actual identity. The same applies to your family and friends. Never reveal anything about other people that could possibly get them into trouble. The biggest danger to your safety is if you get together with someone you "meet" online. Remember, you never know for certain if people you meet online are who they say they are. If you do feel it's appropriate

Keep Your Identity Private

If you're in any type of public forum, avoid giving out your full name, your mailing address, your telephone number, the name of your school, or any other information that could help someone determine your actual identity. The same applies to your family and friends. Never reveal anything about other people that could possibly get them into trouble.

Never Get Together with Someone You "Meet" Online

The biggest danger to your safety is if you get together with someone you "meet" online. Remember, you never know for certain if people you meet online are who they say they are. If you do feel it's appropriate to meet with someone, discuss it with your parents and never go to the meeting by yourself. Arrange to meet in a public place like a coffee shop or mall that you, not just the other person, are familiar and comfortable with, and never go alone. The safest procedure is to have your parents talk with the parents of the other person and for both of you to bring your parents along on the first meeting.

Never Respond To E-Mail, Chat Comments, Instant Messages Or Other Messages That Are Hostile, Belligerent, Inappropriate Or In Any Way Make You Feel Uncomfortable

It isn't your fault if you get a message that is mean or in any way makes you feel uncomfortable. If you get such a message, don't respond. Instead, show it to your parents or a trusted adult to see if there is anything you can do to make it stop. Sending a response just encourages the person.

Talk with your Parents About Their Expectations and Ground Rules for Going Online

It's important that you and your parents are on the same "channel" when it comes to your online activities. This includes when you can go online, how long you can stay online, and what activities you can do online. Communicating with your parents doesn't mean that you have to give up your privacy. It

just means that you come to an agreement based on mutual trust and understanding. While you're at it, perhaps you can help your parents better understand the Internet, what it can be used for, and how it is helpful for teens.

Guidelines for Parents

Talk with your Teens About What They Can and Cannot Do Online

Be reasonable and set reasonable expectations. Try to understand their needs, interests, and curiosity. Remember what it was like when you were their age.

Be Open with Your Teens and Encourage Them to Come to You if They Encounter a Problem Online

If they tell you about someone or something they encountered, your first response should not be to blame them or take away their Internet privileges. Work with them to help avoid problems in the future, and remember – you respond will determine whether they confide you the next time they encounter a problem and they learn to deal with problems on their own.

Learn Everything You Can About the Internet

Ask your teens to show you what's cool. Have them show you great places for teens and fill you in on areas that you might benefit from as well. Make "surfing the net" a family experience. Use it to plan a vacation, pick out a movie, or check out other family activities. Make this one area where you get to be the student and your child gets to be the teacher.

Check Out Blocking, Filtering and Ratings Applications

As you may know, there are now services that rate web sites for content as well as filtering programs and browsers that empower parents to block the types of sites they consider to be inappropriate. These programs work in different ways. Some block sites known to contain objectionable material. Some prevent users from entering certain types of information such as their name and address. Other programs keep your children away from chatrooms or restrict their ability to send or read E-mail. Generally these programs can be configured by the parent to only block the types of sites that the parent considers to be objectionable.

Whether or not it is appropriate to use one of these programs is a personal decision. If you do use such a program, you'll probably need to explain to your teen why you feel it is necessary. You should also be careful to choose a program with criteria that reflects your family's values. Be sure to configure it so that it doesn't block sites that you want your teen to be able to visit.

It is important to realize that filtering programs cannot protect your child from all dangers in cyberspace. To begin with, no program can possibly block out every inappropriate site. What's more, it's possible, in some cases, for the programs to block sites that are appropriate. If you use a filtering program, you should re-evaluate it periodically to make sure it's working for your family.

Regardless of whether you use a filtering program, you should still be sure that your teen follows all of the basic rules listed in this brochure. Filtering programs are not a substitute for good judgment or critical thinking. With or without filters, children and their parents need to be "net savvy" and communicate with each other.

About this brochure

This brochure was written by Larry Magid, a syndicated columnist, media commentator, and host of www.safekids.com and www.safeteens.com. He is also the author of The Little PC Book (Peach Pit Press, 1993-2000).

Teen Safety on the Information Highway was jointly produced by the National Center for Missing & Exploited Children and The MASTER Teacher®.

The National Center for Missing & Exploited Children was established in 1984 as a private, nonprofit organization and serves as a clearinghouse of information about missing and exploited children per federal statutes 42 USC § 5771 and 42 USC § 5780. A 24-hour, toll-free Hotline and CyberTipline is available for those who have information about missing and exploited children at 1-800-THE-LOST® (1-800-843-5678) and www.cybertipline.com. Founded in 1969,

The MASTER Teacher provides staff development publications, videos, software, and other motivational resources to help teachers and administrators work with students to better fulfill the work and mission of schools. The MASTER Teacher, PO Box 1207, Manhattan, Kansas 66505-1207, can be contacted at 1-800-669-9633 or visit their web site at www.masterteacher.com.

This brochure is funded by the Bureau of Immigration and Customs Enforcement, U.S. Department of Homeland Security. 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 brochure are those of NCMEC and do not necessarily represent the official position or policies of the U.S. Department of Homeland Security or U.S. Department of Justice.