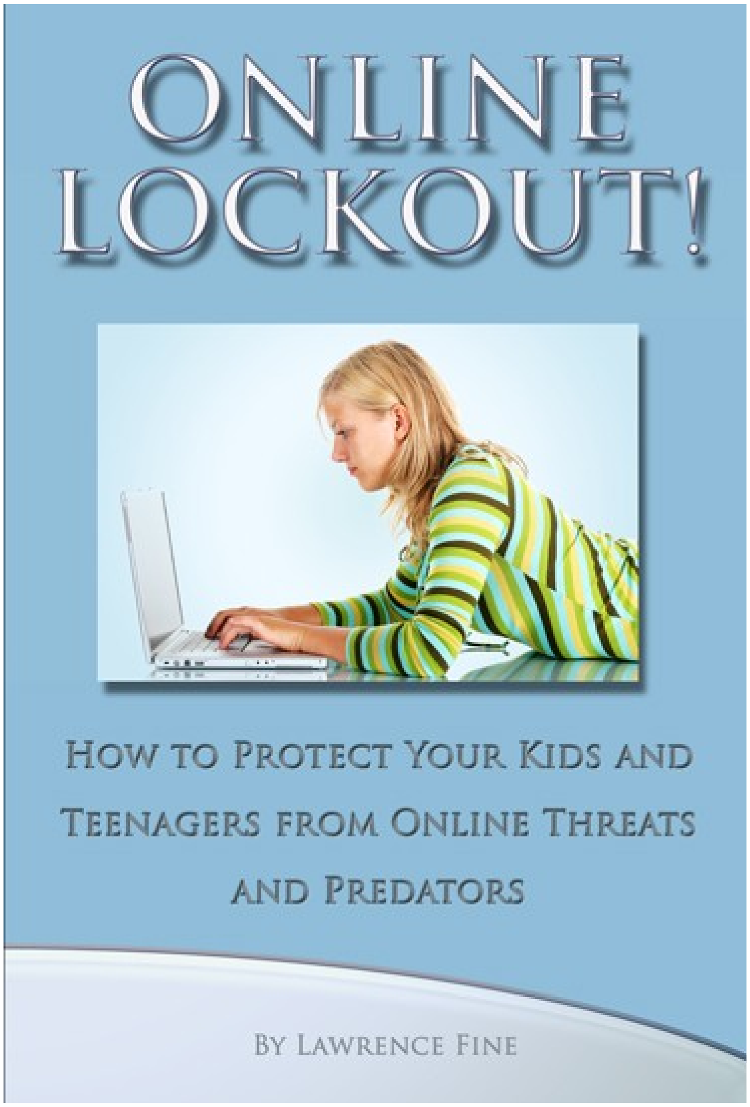
ONLINE LOCKOUT!
How to Protect Your Kids and Teenagers from Online Threats and Predators
By Lawrence Fine

Online Lockout

How to Protect Your Kids and Teenagers from Online Threats and Predators

By Lawrence Fine
www.lawrencefine.com

Obligatory legal notice

While all attempts have been made to verify information provided in this publication, the Author assumes any responsibility for errors, omissions, or contrary interpretation of the subject matter herein. Any perceived slights of specific persons, peoples, or organizations are unintentional.

This publication is an information product, and is not intended for use as a source of legal, accounting, or tax advice. Information contained herein may be subject to varying national, state, and/or local laws or regulations.

The purchaser or reader of this publication assumes responsibility for the use of these materials and information, including adherence to all applicable laws and regulations, federal, state, and local, governing professional licensing, business practices, advertising, and all other aspects of doing business in the United States or any other jurisdiction in the world. No guarantees are made. Author reserves the right to make changes. If you can’t accept these terms, kindly return product. The Author assume no responsibility or liability whatsoever on the behalf of any purchaser or reader of these materials.

Dedication

This book is dedicated to everyone who has ever been misled, misrepresented, or flat-out lied to on the Internet. It's also dedicated to all the kids and teenagers out there who don't understand the dangers and risks involved in what seems like such a safe thing as the Internet.

Acknowledgements

This book was written with the help of a great many people who contributed their energies to the project.

I would like to start with a special acknowledgment for the encouragement and support given by Nina Fuentes for her help with the research of the book and for my friends who kept me excited about the project.

Rather then trying to single out everyone who has been of help, knowing that somehow or other I will miss at least one person, I would like to simply say thanks to everyone who has been involved, whether as sounding boards, or just as supporters.

About the Author

A web design expert and active member in his community, Lawrence Fine is a concerned advocate for the safety of children. Through his experience of coaching soccer for over 20 years, he has seen how vulnerable kids and teenagers can be to the many dangers in this world.

The Internet is a relatively new medium of entertainment that has become very popular in recent years. Along with this popularity, it has also become a minefield for threats from online predators and hackers. Fearing for the kids' safety in the community where he coaches and for his own personal information, Lawrence decided it was time he did something about this growing problem.

He started researching the topic of Internet safety and decided to put together an informative pamphlet. During the process, he found out there was more information that people needed to know about than he originally planned. This prompted him to expand the pamphlet into the thorough and easy-to-use guide you read today.

You will be truly amazed at how making a few simple changes while using and interacting on the Internet will help to make you and your family safer. The information in this guide will also help you to make better choices to keep your personal information more secure.

Lawrence resides near Charleston, West Virginia, where he spends his non-writing time working, coaching soccer, traveling, and spending time with friends.

Table of Contents

Introduction

As the world becomes more and more technologically advanced, parents begin to face unique and new challenges in keeping their kids safe. One of the most complex challenges facing parents today is the Internet and the dangers that potentially lurk there.

While there is no doubt that the Internet can provide a wealth of resources and information our children can use to expand their horizons, there are distinct dangers present that seek to steal the very innocence in our children that we hold dear. Unlike other dangers in the world that we can easily pinpoint and from which we can shield our children, online dangers are often much less precise and far more difficult to monitor with traditional methods.

In many cases, one of the most difficult aspects of protecting our children from online dangers lies in the very fact that parents may not know the nature of the dangers facing their children. As technology continues to evolve and advance, so do potential online dangers.

Today's savvy parents must take the initiative to understand the lures and threats presented by the Internet in order to protect their children.

Throughout the rest of this guide, we will discuss a variety of factors related to keeping kids safe online; we will come to understand both how and why our kids go online, what they do while they're surfing; and we will learn the steps we can take to protect them while they're in cyberspace.

Why Taking Steps to Protect Youth Online Is Important

We all know that the Internet can be dangerous. This is certainly not news to most parents. We've all heard of the dangers presented in cyberspace by sexual predators who seek to lure unsuspecting children online for dangerous purposes. Across the nation, entire law enforcement units as well as groups of dedicated parents and others are working to lure predators out into the open using their own techniques against them, all in an effort to protect our children from would-be assailants.

Many parents might be surprised to learn, however, that the danger of online predators is not the only danger lurking in wait for our kids to encounter. Certainly, it is one of the most frightening, but it is by far not the only potential harm that could befall our kids simply by logging online.

Besides the imperative point that our children can become the victim of serious crime by surfing the Net, as parents and concerned adults, we must also understand the impact that spending large amounts of time online can have on our children.

Statistics indicate that children and teens are now spending more time than ever online. Some of them are actually spending hours online in a variety of activities, from surfing the net to chatting with their friends through text messaging. We must ask ourselves what cost this is presenting.

This much time dedicated to online activities is certainly providing a negative impact on family relationships and activities. A distraction from school work? That is certainly a possibility.

In addition, it is important to note that children and teens who spend inordinately large amounts of unmonitored time online may also become exploited by a variety of advertising techniques used online specifically for the purpose of luring children and teens into certain thought and behavior patterns.

Finally, we must consider the fact that beyond encountering strangers online, children and teens face the possibility of encountering content that their parents and guardians may deem to be inappropriate or which may prove to be a bad influence, initiating behavior and thoughts that may be dangerous and/or self-destructive.

When monitored appropriately, the Internet can be a wonderful teaching tool for children and teens. There is a wealth of information available online that our youth can use to expand their horizons that is simply not available anywhere else.

In a sense, the Internet is akin to the world's largest library. Like any library, however, there must be a responsible librarian present to ensure that our youth do not accidentally or intentionally "check-out" material and content that could be dangerous to them.

It is our job as parents—and concerned adults—to act as responsible librarians to protect the future of our youth by guarding them against material and content we deem to be inappropriate as well as would-be predators. Our first duty in that role is to take the initiative to understand how today's evolving technology allows our kids to go online and what they're doing once they arrive there.

Communication Tools Kids Use to Interact Online

One of the most important factors in understanding how we go about keeping our kids safe online is in understanding the tools our kids are using and specifically how they are using them. Many parents may believe that the biggest thing they have to worry about in regards to keeping their kids safe online is what and who they encounter while logging online using the family's home computer.

There is certainly no doubt that this is a major issue and one which deserves attention; however, studies indicate that this is not the only communication area in which our children may be threatened.

First, it's important to realize that while a large majority of kids are going online using the family desktop computer, this is not the case in all situations. A surprising percentage of those kids who do have the capability of logging on at home also use a variety of other locations in order to surf the web. Some parents might even be surprised to learn that while they thought their kids were safe because the family did not have an internet accessible computer at home, the truth of the matter is that kids are going online in a variety of locations.

Research indicates that while 87% of teens do use the Internet most often at home, an astounding 87% are logging on at school; followed closely by 74% who are logging on at a friend's house. While you may be doing your part to keep your child safe online at home, who is to say that the parents of your child's friend are doing the same?

Furthermore, more than half of teens are using the Internet at places like the library and a community center. [1]

If the fact that such a large majority of kids claim that their primary location for using the Internet is someplace other than home startles you, it's with good

[1] Source: Pew Internet & American Life Project Teens and Parents Survey, Nov.-Dec. 2004. Margin of error is ±4%.

reason. Of all the prospective locations that a teen could log onto the Internet, the library is growing faster than any other location.[2]

Beyond the fact that kids are going online in locations where their online activities may not be subjected to parental approval and screening is the irrefutable fact that computers are not the only device we have to worry about.

Sitting down to the old desktop and logging on with a slow dial-up connection is now passé. Today's kids are sophisticated and the technology they are using to communicate with one another is even more sophisticated.

- Cell phones
- Instant messaging (IM)
- PDA

With most kids indicating that a large majority of their pals are online, it may be even more disturbing to learn that 45% of all teens are communicating on cell phones, usually with text messaging. Many parents may find themselves concerned about what their kids are chatting about over email, but in reality email may not be the area that should concern us.

A large number of teens indicate that they actually view email as rather old-fashioned and only use in situations in which they need to communicate with "old" people. Some studies indicate that that popularity of text messaging is growing so rapidly that it could even be eclipsing email.

When given a choice, most teens choose IM over email. Estimates indicate that some 13 million teens are using instant messaging as a major form of communication.

While kids once talked for hours on the phone, they are now using instant messaging as the primary tool for communicating with their friends. Instant

[2] Pew Research Center for the People and the Press survey on media consumption, May 2004.

Just a few of the devices and communication tools that kids are using to go online and communicate include:

messaging allows groups of friends to get together and chat, regardless of whether they are from the same area or not.

The discussions that take place on instant messaging sessions range from subjects as light as planning events to as serious as relating unpleasant news or even ending romantic relationships.

It is obvious that instant messaging has become an important part of the teenage generation. In comparison to less than 50% of adults who use instant messaging, nearly 75% of all teens use instant messaging, and almost all of those do so on a regular basis.

Perhaps even more staggering than the numbers of kids who are communicating through instant messaging are the percentages related to the amount of time kids are spending utilizing this form of communication.

Nearly half of all kids who use instant messaging state that they spend between thirty minutes and an hour each time they IM. With a large majority of kids admitting they instant message several times per week, it is easy to calculate how much time kids are spending on their IM sessions.

A Snapshot of What Teens Are Doing Online

When looking at how we approach keeping our kids safe online, we need to take a look at the activities our kids are engaging in online. Research indicates that approximately 87% of kids between the ages of 12 and 17 use the Internet. Across the nation, this is the equivalent of more than 20 million young people who are logging onto cyberspace. On any given day, there are about 11 million of those kids actively surfing the web, compared to only about seven million who were logging in 2000.

This is in direct comparison to the number of adults who use the Internet, which has only increased by 10% since 2000. These statistics indicate that Internet usage is growing increasingly prevalent among teens and is doing so at a rapid rate.

So, what is it that is drawing these millions of kids to log on each day? Research for homework? For some, yes. Further research, however, indicates that the mix of online teen interests is varied. Consider these statistics:

- 81% of teen Internet users admit that they log onto the Internet to play online games.
- 76% of teen Internet users claim they log on for news content.
- 43% of teen Internet users are logging on to make purchases.
- 31% of teen Internet users access the Internet to obtain health information.[3]

The statistic above provide some insight into some of the most common activities share by the largest majority of teens, but it is in no way a complete and exhaustive picture of the types of activities teens engage in when logged on or why they do it.

[3] Data from: Pew Internet & American Life Project

May teens log online in order to research the latest trends in music and fashion. This is particularly common among girls in the 12 to 14 age group. Children in families with less Internet experience and/or with incomes of less than $50,000 per year are far more likely to use the Internet as a research tool for this purpose.[4]

Teens also like to log on in order to obtain music. Some sites, such as Napster, have made it quite easy for teens to log on and download music as a way to satisfy their seemingly bottomless appetite for the latest tunes.

The Internet has also made it increasingly easy for teens to stay on top of activities related to sports teams, clubs, and groups to which they may happen to belong. Everything from the high school football team to the local Girl Scout troop now seems to have its own website where information regarding practices, meets, and other activities can be posted.

Other teens have found that the Internet is the perfect place to buy, sell, and trade. Auction and trading sites, in particular, are quite popular among boys in the 15 to 17 age range.

The Internet's reputation as a huge reference library hasn't been lost on teens, either. Many older teen girls tend to turn to the Internet when looking for health, dieting, and fitness related information.

In many cases, these topics coincide with subjects they feel they are unable to discuss with adults, especially their parents. At a time in which most teens are looking for ways to express their own unique identify, the Internet provides a way for them to do just that by creating their own web page or blog or even to simply post their opinion regarding a variety of issues on existing websites and blogs.

For the most part, it appears that teens prefer to use the Internet as a way to browse for fun and connect with their friends. When quizzed regarding their Internet usage and relationships with friends, a large percentage of teens feel that instant messaging has improved the quality of their relationships with friends.

[4] From the Pew Internet Project May-June 2000 Survey

Teens frequently use instant messaging to stay in contact with friends who have moved or whom they have met at camp. They indicate that this allows them to maintain friendships that might have otherwise withered away.

Teens are also using these communication tools as a way to handle conversations that are difficult. They may begin and end relationships using instant messaging because it is easier to manage than face-to-face confrontations.

Other teens indicate that Internet usage allows them to discover their true self at a time in which they are struggling to separate themselves from the identities of their parents and siblings. The anonymity of the electronic communication allows teens to reveal aspects of their personalities they might otherwise find difficult to share.

In many cases, the Internet also provides a way for teens to experiment with multiple identities. A majority of teens interviewed admit to having multiple email addresses and/or screen names.

The addresses and screen names they use typically differ according to the different aspects of their lives. In some cases, teens actually use screen names that they keep secret from their friends in order to keep their friends from finding out when they're online.

While some teens admit to having used "secret" screen names for the purpose of playing tricks on others—even their friends—many claim they simply use various aliases as a way of controlling their Internet usage.

One teen reported that it was not uncommon for her to use email to play tricks on her friends.

Sometimes, she said, she would do it just to freak them out.

Other times, her favorite trick is to pretend to be someone that she knows her friends like. "It's fun," she says, "to act like maybe I'm someone who likes my friend. Just to see what she would say."

Although most of the time her tricks do not cause any problems, there have been a few times, she admits, when her friends have found out and become really angry.

This type of experimentation also provides a way for teens and youth to discover their self-identity. As they evolve toward adulthood, this gives teens a safe way to experiment with how they present themselves to the world.

Who Is Most Vulnerable Online

Some parents may be tempted to believe that their children and teens are not at risk for dangers presented online for a variety of reasons. Perhaps they have even developed this belief because they do not own a home computer or because they restrict access to their home computer.

In recent years, studies into this very subject have provided some interesting insight into who among our youth are most vulnerable when it comes to online dangers.

One such study compared the differences between how youths in single-parent households and youth in two-parent households approached online usage. The study concluded that there is a definitive difference.

According to the research gathered in the study, children and youth living in single parent households are more likely to use the Internet for entertainment purposes rather than educational purposes. These youth go online to visit chat rooms, play games, and look up products they are interested in buying. Comparatively, youth living in two-parent households typically use their Internet time to view news online or complete online purchases. [5]

Age can also play in important role in regards to the level of risk a youth may be exposed to online as well. Statistics indicate that older teens appear to be more vulnerable online than younger teens.

Part of this risk is due to the fact that older teens appear to log on more often and spend more time once they are there as well as the fact that the activities of older youth tend to be different than those of younger youth.

Studies found that younger youth, those between the ages of 12 and 14, typically go online more often than older youth for the purposes of playing or downloading online games. Older youth, from ages 15 to 17, spend their online time involved

[5] From the U.S. Census Bureau current population report from March 1998. Available on the Census Bureau web page at http://www.census.gov/population/www/socdemo/ms-la.html

in sending and receiving email, instant messaging, visiting chat rooms and locating information they feel is difficult to discuss with adults. [6]

Parental Concerns

When it comes to Internet usage by kids, there are a number of areas that should and do worry most parents. Surprisingly, one of the biggest worries for many parents is the level of attachment that most youth seem to have developed regarding Internet technology.

When interviewed, a large percentage of youth admit that they would not only miss their time in cyberspace, but would "just die" if they were no longer allowed to surf the Internet. There is also the concern regarding the possibility of interaction between youth and strangers.

While some would dismiss the threat of potential targeting by predators that teens might encounter online to be an idea that has been hyped by the media, the statistics simply do not lie.

In a study conducted to determine the level of risk Internet activities potentially pose to teens, it was discovered that 60% of all teens have received an email or instant message from a stranger and 63% have actually responded and exchanged emails or instant messages with people unknown to them. [7]

Some of these encounters occur in chat rooms, where teens may have lied about their age in order to access the site. In other cases, the contact occurs as a result of the youth having been targeted by the stranger.

When teens go online and set-up profiles on places such as AOL or Yahoo, they frequently list personal information as well as info regarding their interests and hobbies. All it takes for a stranger to find them is entering a string of search criteria, and if that criteria matches the info your youth has entered on the profile, the User ID can be accessed in a matter of seconds, and an IM or email will be on its way to your teen from someone completely unknown to him or her.

A 15-year old girl claims that at least 40% of the people she talks to are people whom she has met online, usually through her profile on sites like Yahoo. "I set

[6] Source: Pew Internet & American Life Project Teens and Parents Survey, Nov.- Dec. 2000. Margin of error is ±4%.

[7] Source: Pew Internet & American Life Project Teens and Parents Survey, Nov.-Dec. 2000.

up a profile for hobbies that I enjoy, and that's how I met a lot of my online friends. They enter different search criteria, and if I match what they've entered, they are able to get my user ID. I usually have a lot in common with the people I meet like this."

When asked if she would tell her parents about the friends she's met online, the teen laughs and replies, "No way! My parents are, like, really overprotective and they would probably tell me I couldn't use the Internet anymore."

As frightening as this idea may be to most parents, a large majority of teens interviewed admit they do not let their parents know when they are contacted online by a stranger. Even those youth who do not routinely respond to emails and IMs sent by strangers believe that discussing with their parents any stranger's contact would lead to a restriction of their Internet usage.

Furthermore, beyond the threat of possible restriction of their online time, most youth simply do not think of this as a big deal. For the most part, they see no danger in meeting new people online and think that parents tend to overreact.

"I don't really worry about the people I meet online," says a 16-year old boy. "I mean, I know that there are people out there that use bugs or whatever to spy on you, but, I like, don't ever really think that it's going to happen to me. I haven't ever had a problem."

The truth of the matter, however, is that while our youth tend to dismiss contact by strangers online as simply a cool way to make new friends, it is frighteningly easy for would-be predators to contact our children using the method described above, converse online with them for a period of time, and gain enough personal information to actually locate them.

Below is an excerpt from an e-mail story that recently made the rounds in an effort to alert both parents and kids alike to the specific dangers that can be encountered when teens give out too much information online to people they do not know. To the best of anyone's knowledge, the author of the story is anonymous, and it is unknown as to whether the story is actually true or not. Regardless of the truth of the actual story, the moral lying behind it is nonetheless important and relevant.

Shannon could hear the footsteps behind her as she walked toward home. The thought of being followed made her heart beat faster. "You're being silly," she told herself, "no one is following you."

To be safe she began to walk faster, but the footsteps kept up with her pace. She was afraid to look back, and she was glad she was almost home. Shannon said a quick prayer, "God, please get me home safe."

She saw the porch light burning and ran the rest of the way to her house. Once inside she leaned against the door for a moment, relieved to be in the safety of her home. She glanced out the window to see if anyone was there. The sidewalk was empty.

After tossing her books on the sofa she decided to grab a snack and get online. There she could talk to strangers without being afraid. After all, none knew who she really was and couldn't hurt her.

She logged on under her screen name ByAngel213. Checking her Buddy List she saw GoTo123 was on.

She sent him an instant message:

ByAngel213: Hi I'm glad you are on! I thought someone was following me home today. It was really weird!

GoTo123: LOL You watch too much TV. Why would someone be following you? Don't you live in a safe neighborhood?

ByAngel213: Of course I do LOL I guess it was my imagination cause didn't see anybody when I looked out.

GoTo123: Unless you gave your name out on line. You haven't done that have you?

ByAngel213: Of course not. I'm not stupid you know.

GoTo123: Did you have a softball game after school today?

ByAngel213: Yes and we won!

GoTo123: That's great! Who did you play?

ByAngel213: We played the Hornets LOL. Their uniforms are so gross! They look like bees LOL

GoTo123: What is your team called?

ByAngel213: We are the Canton Cats. We have tiger paws on our uniforms. They are really cute.

GoTo123: Do you pitch or what?

ByAngel213: No, I play second base. I got to go. My homework has to be done before my parents get home. I don’t want them mad at me. Bye!

GoTo123: Catch you later. Bye

GoTo123 decided it was time to teach Angel a lesson. One she would never forget. He went to the member menu and began to search for her profile. When it came up he highlighted it and printed it out. He took out a pen and began to write down what he knew about Angel so far:

Her name: Shannon

Birthday: Jan. 3, 1985 Age: 13

State she resides in: North Carolina

Hobbies: softball, chorus, skating and going to the mall

Besides this information he knew she lived in Canton. She had just told him, he knew she stayed by herself until 6:30 every afternoon until her parents came home from work. He knew she played softball on Thursday afternoons on the school team and the team was named the Canton Cats. Her favorite number "7 "was printed on her jersey.

He knew she was in the seventh grade at the Canton Junior High School. She had told him all this in the conversations they had online. He had enough information to find her now. "She’ll be so surprised," he thought. "She doesn’t even know what she has done."

Shannon didn’t tell her parents about the incident on the way home from the ball park that day. She didn’t want them to make a scene and stop her from walking home from the softball games.

Parents were always overreacting, and hers were the worst. It made her wish she were not an only child. Maybe if she had brothers and sisters her parents wouldn’t be so overprotective.

By Thursday Shannon had forgotten about the footsteps following her. Her game was in full swing when suddenly she felt someone staring at her. It was then that the memory came back.

She glanced up from her second base position to see a man watching her closely. He was leaning against the fence behind first base and he smiled when she looked at him. He didn't look scary and she quickly dismissed the fear she had felt.

After the game he sat on a bleacher while she talked to the coach. She noticed his smile once again as she walked past him. He nodded and she smiled back. He noticed her name on back of the shirt. He knew he had found her.

Quietly he walked a safe distance behind her. He didn't want to frighten her and have to explain what he was doing to anyone. It was only a few blocks to Shannon's home and once he saw where she lived he quickly returned to the park to get his car.

Now he had to wait. He decided to get a bite to eat until the time came to go to Shannon's house. He drove to a fast food restaurant and sat there until time to make his move.

Shannon was in her room later that evening when she heard voices in the living room. "Shannon, come here," her father called. He sounded upset and she couldn't imagine why. She went into the room to see the man from the Ballpark sitting on the sofa.

"Sit down," her father began. "This man is a policeman and he has just told us a most interesting story about you." Shannon moved cautiously to a chair across from the man. How could he tell her parents anything? She had never seen him before today!

"Do you know who I am, Shannon?" the man asked. "No" Shannon answered. "I am your on-line friend, 'GoTo123'."

Shannon was stunned. "That's impossible! "GoTo" is a kid my age! He's 14 and he lives in Michigan!"

The man smiled. "I know I told you all that, but it wasn't true. You see, Shannon, there are people online who pretend to be kids. I was one of them. But while *others do it to find kids and hurt them, I belong to a group of parents who do it to protect kids from predators."*

"I came here to find you to teach you how dangerous it is to give out too much information to people online. You told me enough about yourself to make it easy for me to find you. Your name, the school you went to, the name of your ball team and the position you played. The number and name on your jersey just made finding you a breeze."

Shannon was stunned. "You mean you don't live in Michigan?"

He laughed. "No, I live in Raleigh. It made you feel safe to think I was so far away, didn't it?" She nodded. "I had a friend whose daughter was like you. Only she wasn't as lucky. The guy found her and murdered her while she was home alone. Kids are taught not to tell anyone when they are alone. Yet they do it all the time online."

"The wrong people trick you into giving out information a little here and there online. Before you know it, you have told them enough for them to find you without even realizing you have done it. I hope you've learned a lesson from this and won't do it again."

"I won't," Shannon promised solemnly.

"Will you tell others about this so they will be safe too?"

"It's a promise!"

That night Shannon and her dad and Mom all knelt down together and prayed. They thanked God for protecting Shannon from what could have been a tragic situation.

While the thought of someone with less than honorable intentions going to such lengths to locate your child may make your toes curl, statistics reveal that only 25% of parents worry a lot about their children being contacted by strangers online.

Considering that the majority of teens and youth online readily admit they have been contacted by strangers and have even responded back, it rather puts the entire situation in a new perspective. [8]

Beyond the idea of our children becoming potential crime victims lurks the additional threat that the Internet could possibly prove to be too much of an irresistible lure in which our own children engage in criminal activity. While none of us ever wants to believe that our child could be capable of such activity, it appears the Internet may be just too much of a temptation for some kids to resist. Of youth interviewed, most admit they have used the Internet to send a prank email. That isn’t to say, of course, that all of those emails led to dire results, but it certainly isn’t a commendation for unfettered restriction of teen Internet usage. 26% of youth admit they have used instant messaging in order to pretend to be someone else. In some cases, kids are using such tricks for what they deem to be just pure fun.

They might IM someone, even a friend, just to mess with him. In other cases, teens are using such deception to obtain information from friends they may think are being less than honest with them.

A 17-year old girl admitted that when she was a few years younger she used the Internet one evening for fun when her parents were away. “I was just messing around, you know, and decided it would be fun to play a trick on someone. So, I pretended to be someone who had been kidnapped. I emailed the police and told them a story they actually believed.

I didn’t think it would go that far, but the police actually came to investigate and knocked down the door of the fake address I had given them. Later, they tracked me down using my IP address, and my parents had to pay for the damage done

[8] Source: Pew Internet & American Life Project Teens and Parents Survey, Nov. - Dec. 2000.

to the house at the address I had given them. I didn't mean for it to happen; I was just having a little fun, but as it turned out I was the only one who thought it was funny."

Another growing concern regarding Internet safety and kids is the fact that it is becoming much easier for kids to engage in various types of addictions online. One of the most common, many parents would be surprised to learn, is gambling.

According to the National Research Council, most adolescents are gambling online, and they're doing it often. Sports betting and card games are the two most common types of gambling used by kids when they go online.

And we're not talking penny ante stuff, either.

These sites can rack up big bucks quickly, and they do it when they are able to lure in kids who have access to a credit card. The horror stories of parents who have discovered too late that their youth was involved in such activities are just that –horrific.

Large sums of money lost. Credit ratings ruined; preventing parents from purchasing homes, cars, and in some situations from getting jobs. Perhaps even more frightening than all that, however, is the fact that by the time it is discovered, the youth has become a gambling junkie.

But wait a minute, you might be thinking. It's illegal for kids to gamble. How can sites get away with this? Quite simple.

A large number of the sites frequently visited by kids operate out of the jurisdiction of the US. Their sole purpose is to make money, and they will do it anyway they can, regardless of whether they're luring in your fifteen year old daughter or your fifty-five year old neighbor.

Gambling sites aren't the only type of content that parents need to worry about when it comes to the type of inappropriate material their kids might encounter while online, either. Just a few of the types of sites your kids could run into include:

- Sites that advocate the use of illegal drugs, tobacco, and alcohol

- “Adult” porn and erotica sites
- Sites that promote racism, anti-Semitism, and hatred toward other groups

There are literally thousands of these types of sites floating around in cyberspace and it doesn’t take much for your kids to stumble onto one. Would it surprise you to know that your kids might even be invited to visit a site that promotes nonconsensual acts of violence or depicts images and stories that even you as an adult might find uncomfortable?

Our kids are no more immune to receiving pornographic Spam than we are. The difference, however, is that while we may become annoyed and simply hit the delete button, our kids have not yet developed the decision making skills to avoid such temptations.

The thought of taking a quick “peek" quickly introduces them to a dark and sordid world that can project all kinds of thoughts and images into their still developing young minds that, as parents, we might prefer to lurk elsewhere.

There is also the growing concern that the amount of time kids are spending online today could be changing how youth interact with their families and even their friends.

One of the most frequent problems involves simple scheduling, particularly in families with more than one teen at home. The sheer logistics of trying to arrange a schedule in which all are able to spend the amount of time online they feel they should be allotted to have is enough to drive some parents mad.

The time this devotion to online surfing takes away from family activities is also a concern for some families. Two-thirds of teens who regularly go online admit that their time online takes away from time they would otherwise spend with their families.

The only exception to this rule seems to be in situations in which both parents and children routinely go online. In these cases, both teens and parents indicate they feel they spend more time together through their mutual Internet usage.

Some of the most common activities parents and teens may share online include planning weekend activities, shopping for gifts for other family members and researching health information together.

Parents who rarely or infrequently go online, however, are far more likely to report a sharp decline in family activities as a result of their kids' Internet usage as well as a higher fear regarding the usage of the Internet by their kids.

The statistics regarding decrease in family activities associated with parents who are not wired appears to directly correlate with the fears of parents who do not use the Internet.

For the most part, when asked about their experience regarding online activities, parents and youth both admit that youth know far more about the Internet than parents.

How Parents Can Protect Their Kids' Online Access

With the number of dangers that kids could potentially encounter online, it is obvious that steps must be taken in order to protect our kids from the nefarious content and individuals they might otherwise 'bump' into while surfing the Internet.

It can be quite tempting to think that we can protect our kids from these dangers simply by restricting or monitoring their access to the Internet. There is only one problem with this assumption.

It doesn't take into account the fact that unless we spend 24 hours a day, 7 days a week with our kids, we cannot possibly prevent or monitor their Internet usage all the time. There are simply too many possibilities outside our control in which they can go online: the library, their friends' homes, and even school.

When we're not there to look over their shoulder and see exactly where online they're visiting and what they're doing while they are on there, our kids are truly on their own. Therefore, it is imperative that the approach we take toward protecting our kids from online dangers be multi-pronged.

We must take steps to not only protect them from dangers when we're with them but also teach them how to protect themselves when we're not around. Most teens report that they simply do not think they are in any danger when online. Their young minds fail to comprehend the much larger picture that we as adults see. It is our job to help them understand the dangers that could be posed while teaching them Internet self-defense.

In terms of what we can do to protect our kids from online dangers when we're in relatively close proximity, there are a number of tools and techniques that can be used.

One technique is to restrict the amount of time your kids can actually spend online. Certainly, this method won't guarantee that your kids won't visit objectionable sites during the amount of time in which they are online, but it certainly decreases the window of opportunity.

The biggest advantage of this technique is that it helps to prevent your teens from becoming so caught up in online activities that they lose sight of other important activities in their lives. Given the concern among some parents that their youth are spending more time instant messaging their friends, playing online games, and other activities that could potentially become quite addictive, this is a good tool to use in order to combat this problem.

In order for this technique to be effective, however, parents must take steps to ensure that it is consistently enforced. Determine how much time your child is allowed to spend online, and then monitor that amount of time rigorously.

Ideally, this technique works best when the computer your child uses is located inside a public area of the family home such as the family room, etc. Keep in mind that this won't keep your kid offline in other settings, such as when visiting friends, so it should not be the only tool that you utilize.

Many parents are also using content filters in order to control the sites their children are allowed to visit. This technique proves to be particularly popular in situations in which the child has private access to a computer, such as a desktop or laptop located in their bedroom.

It is also effective in situations in which one or both parents are the last to arrive home—leaving plenty of opportunity for their kids to surf without restrictions.

A few of the most well known filter programs include NetNanny, CyberPatrol, CyberSitter, and SurfWatch. These programs are known to do a relatively good job of filtering out sites that depict hatred, sex and crime; however, like any technique or tool, they are not foolproof.

Each program varies in the techniques it uses to filter out sites you might find objectionable. In some cases, the program might do an acceptable job of preventing kids from deliberately searching for sex sites, but that doesn't mean that it will screen out all sex sites.

Even if your kids are not deliberately looking online for pornographic sites, it may still be possible for sites containing pornographic content to pop up on a list of search results. In other cases, your children may be informed they have typed in an unacceptable word in the search engine; but it's quite possible that search results will be displayed anyway.

For the most part, NetNanny seems to be the best at allowing parents and guardians to configure the controls, allowing you to remove sites from the blocked list that you feel are acceptable as well as allowing you to add sites to the block list that you would prefer your child not visit. Unfortunately, NetNanny appears to be one of the sites that will display some sex sites on occasion, depending on the search criteria used; so be aware of this fact.

Some of the programs, particularly CyberPatrol, will also give you the ability to block your child's access to other programs you may have installed on your computer. If you have a financial program installed to help balance the family checkbook, for example, you can prevent your kids from tweaking with your figures by blocking access to it using this program.

If you're concerned about the amount of information your child reveals online, you should also consider a program that allows you to block specific words or phrases when online, especially in chat rooms. Certain programs will even give you the ability to stop your child from entering their full name, address, etc. This can prevent a would-be predator from actually locating your child and carrying out dangerous intentions, such as kidnapping, molestation, etc.

Various types of filtering programs run from about $27 upwards to about $50.

While there are numerous benefits to using filtering programs, there are also some disadvantages.

One of the big disadvantages to this type of technique is that the software must be maintained and updated to ensure that it continues working properly. In this way, it is rather similar to virus detection software. You are only protected as much as your software program is updated.

Other similar options you might consider include allowing your Internet Service Provider (ISP) to do the filtering for you. Many parents feel this option is advantageous because the ISP takes on the responsibility of updating and maintaining the filtering software, unlike self-installed filters, with which you must handle the updating yourself.

Of course, the disadvantage to this technique is that you are handing that responsibility over to the ISP and assuming that they are doing what they are supposed to do. A few of the ISPs that offer family friendly service you might want to consider include America Online, FamilyClick, Integrity Online, and Mayberry USA.

Each one of these offers service that runs about $22 a month. Most give the option of setting different levels of access for different family members. For example, some sites provide the availability of limiting access to youth, pre-teen, teen, etc.

Teen access might block personals, chat rooms (unmonitored), and sites that promote illegal drugs, while pre-teen sites block all of the above along with any sites that discuss topics such as sex, STDs, pregnancy, etc.

Some of the sites allow adults to turn off the filters for their own use, while others do not, so be sure to check first if you would like adult members of your household to be able to log on without restrictions.

Above and beyond filters and blocking services, the best tool that you can use to protect your child online is old-fashioned parenting, and that means getting involved and understanding what you and your kids are facing online.

If you aren't already wired to the Internet and wouldn't know an IM from a blog, then it's time to change that. For many of us the thought of sitting down to a computer and venturing into cyberspace is more than a trifle disconcerting; however, it is perhaps the best thing you can do to protect your kids.

In the event that when you last sat down to a computer, disks were large, black, and literally floppy; below are some definitions to help you become acquainted with the times:

Internet – A large, global network that is used to connect computer through telephone lines and fiber networks to databases of electronic information. Using the Internet, people from all around the world can communicate and share information.

Bulletin Board Systems (BBSs) – Computers that are networked together, connected by a central setup, and operated by a system administrator. Users are able to link their individual computers to the central BBS computer setup, allowing them to then post and read messages as well as exchange information and hold conversations. Access to a BBS is usually privileged, with access granted by the operator.

Commercial On-line Service (COS) – Typically offers limited services to the Internet as part of a package plan. Examples include CompuServe, Microsoft Network, Prodigy, America Online, etc.

Internet Service Provider (ISP) – A type of service that offers full access to the Internet for a flat monthly rate. Electronic mail service is also typically offered as part of the plan. Individuals may also maintain web sites on space provided by servers.

Public Chat Rooms – Sites that are created, maintained, listed, and monitored by public domain systems. Large numbers of customers may be in the chat rooms at the same time. A wide range of topics may be covered, including sports, entertainment, children only, etc.

Electronic Mail (E-Mail) – Refers to the transmission of messages and files between computers using a communications network. The e- mail is stored on a server until it is retrieved by the receiver.

Chat – Refers to a type of real-time text conversation between users in a chat room. There is no expectation of privacy associated with chats, which may be accessible by any of the persons logged into the chat room during the time in which the conversation occurs.

Instant Messages - Private, real-time text conversation between two users in a chat room.

Internet Relay Chat (IRC) -- real-time text conversation similar to public and/or private chat rooms on COS.

Usenet (Newsgroups) – Similar to a bulletin board where users can post messages and information. Graphic image files may also be attached. Responses can be posted.

One of the best ways to protect your kids and learn something yourself is by setting aside some time to surf together. If your kids are already surfing the net, perhaps at school for instance, have them sit down with you and show you some of their favorite sites. Plan an activity or trip together by researching info online.
It is also critically important that you take the time to talk to your kids about their online activities. One of the first rules you should teach them is never to give out any information online that someone else might be able to use in order to personally identify them.
At the top of the list should be information such as:

- Full name
- Address
- School name
- Phone number
- Parents' place of work

You should also make a point of stressing to your kids the importance of never arranging a personal meeting with anyone they have encountered online. When a child or teen has met someone online who seems to share their interests, who listen to their problems, and who truly "gets" them, it can be quite tempting to want to take that a step further and meet in person.
The only problem is that because it is so easy to falsify information online, there is no way for your child to know for sure whom they are chatting with and what kind of intentions that person might really have.
You can also help to protect your children from online dangers by understanding exactly where the most dangers are posed and how they may infiltrate your child's self-imposed feeling of security. Without a doubt, one of the biggest dangers facing children and teens online today are chat rooms.
Estimates indicate that at any given time millions of teens and youth may be corresponding in online chat rooms. The only problem is that you never know exactly who may be on the other end of the chat.

Perhaps the most frightening aspect of chat room dangers is the fact that it can be incredibly easy to submit to activity you would have never dreamed possible. The scenario usually goes something like this. Contact takes place in a chat room. Mutual interests are discovered and a rapport is developed.

The youth won't know they are actually chatting with an adult predator. They will frequently believe they are communicating with a kid their same age. If you're wondering how an adult could possibly make the pass as a teen and the kid actually go for it, keep the following in mind.

Predators devote a considerable amount of time and energy toward learning teen lingo. They are completely in sync with the phrases that sound like foreign language to the rest of us.

They are up on the latest musicians and music groups and frequently are able to converse with sufficient knowledge regarding hobbies that would be of interest to your teen.

For predators, this process is known as setting a comfort level. They may send the youth a photograph of themselves to help them feel reassured. The youth won't know, however, that the photograph is not, in fact, of the real person they have been chatting with.

It's usually a fake photograph the predator has obtained from elsewhere, possibly even a magazine, of a youth about the same age. Depending on the intent of the predator, the 'relationship' may proceed in one of two or three different ways.

If the intent of the predator is to eventually initiate a face-to-face meeting, he may work on getting the child to agree to a telephone conversation. While your child may adhere to your advice to never give out their own telephone number, predators are not stupid. In fact, they are quite creative.

A popular technique involves giving out their own telephone and encouraging the child to use it. This lures the child into a false sense of security. When they place the call, the predator is able to find out the child's number using Caller ID.

If you're thinking right now that you would know when you review the phone bill if your child were calling someone, especially long distance, think again. Predators have even been known to obtain toll-free 800 numbers which allow kids to call them so that the number won't show up on the phone bill and the parents never find out.

Or they may encourage the youth to call collect. Either way, this allows the predator to have an increased level of contact with the child and both methods will result in providing the child's own telephone number to the predator, making it increasingly easy for the predator to control the relationship further and even locate the child.

Keep in mind that this transition may not happen immediately, but predators are usually patient enough to wait months if need be. This develops an even stronger bond, and before long a personal meeting is arranged, at which time any number of potential dangers can befall the unsuspecting child or teenager.

Not all online predators work to initiate face to face meetings, but this does not mean that your child is in any less danger.

Some predators will proceed by beginning to introduce sexual content into their conversations with your child. You would think this would be an immediate clue to most kids to log off and run screaming in the opposite direction, but it's usually not.

The biggest problem is that kids are just naturally curious about sex, and they usually don't feel comfortable talking about it with their parents or other adults in their lives. So, introduce some caring individual on the other end of a chat room willing to discuss with candor subjects that have up until this point just been running through their imagination and you've got a kid who thinks he just walked into a candy store with a blank check in his hands.

Online predators work in a variety of methods because different activities appeal to different predators. For some, it's all about building up to a personal meeting so they can either coerce or force a child into sexual intercourse.

Others, however, are primarily interested in luring youth into an online relationship so they can collect pornographic images. You might think right now that your children would never allow anyone to take advantage of them in such away. You've taught them better than that. They would never, ever send a stranger sexually explicit images of themselves.

Introduce the webcam. If you're unfamiliar with the idea of a webcam, you should know that it is a small camera that can be connected to a computer in order to allow Internet users to view other people and places.

Video feed can be sent of pre-recorded shots of live feed for real time viewing. Corporations and organizations frequently use these devices for the purpose of video chats and conferencing. The units are quite inexpensive, usually under $30, and quite easy to set-up.

The problem with webcams and your kids lies in the fact that predators could quite easily convince your kids to transmit video of themselves, which they may then use in a variety of corrupt and illegal manners.

Without your children even realizing what they have done, they could be putting themselves in a position of becoming material on child porn site.

If you think that there is no cause to be concerned by the idea of your children having a webcam on their computer, consider the following true story that was published by the New York Times after a sting operation that lasted over a period of six months.

At the age of 13, a young man by the name of Justin Berry obtained a webcam for the purpose of meeting his teenage friends online. Since he didn't have a lot of friends at school, he reasoned that the webcam might enable him to meet friends his age online.

In case you're wondering how he even managed to obtain such a high tech device; it was quite simple actually. He received it for free from an internet service provider when he signed up for service. While the boy had initially obtained the webcam for the purpose of meeting friends online, the contacts he made were far from friends his own age.

As soon as the webcam was connected and the software loaded on his home computer, his profile appeared on an online directory of webcam users. Within no time at all, he was contacted by a sexual predator, although he failed to realize it at the time. More predators followed.

Although the teen failed to make the teenage friends that he had hoped, he found the contacts he did make to be just the sort friendship he was looking for. He later stated that the men he met online made him feel smart and were very affectionate with him.

At first, the predators worked their way into his life carefully. He would later reveal that his friends explained to him how he could set up a wish list on Amazon.com and ask for anything that he wanted: books, toys, music, whatever. They told him that anyone who knew his profile name would then be able to log on and send him presents from his wish list. That was just the beginning of what would eventually come.

Meanwhile, his parents had no idea that anything inappropriate was going on. They felt that the computer and webcam enabled their son to meet friends online, helped him with the shyness that had previously been a big problem for him, and even would further his education.

The teen's mother later stated that she had always been told computers were good for kids and they should be exposed to them whenever possible. From presents sent via Amazon, the teen's initiation with his webcam quickly progressed.

It didn't take long for him to become fodder for a sexual predator online. In fact, it only took a few weeks.

Within that short amount of time, he met a man online who assisted him in setting up a PayPal account and offered to pay him $50 to sit in front of his webcam without a shirt on for only three minutes. For a thirteen year old kid, this was a lot of money for practically no work at all.

Over a period of time, the requests made by the teen's online friends grew bolder. As the requests grew bolder, the offers of money grew larger.

One 'friend' offered the boy $100 to pose in his underwear in front of his webcam. If the teen would drop his underwear, even more money would be paid.

The men pursuing the teen were quite adept at their business. They made sure that each new request was never much more than the last, so that the teen was never alarmed.

The boldness of the requests grew with such subtlety that there was never any reason to doubt. These predators had worked at fine- tuning their skills so that they could entice kids with the lure of money with such talent and proficiency that the end result was chilling.

At the conclusion of the investigation, it was eventually determined that of the 1500 people who had paid the boy to perform in front of his webcam, a surprising number of them were well-educated professionals. They included business men, doctors, lawyers and even teachers.

As the teen's online self-published porn business grew, it became patently obvious that not only was he willing to do almost anything on camera for money and cool new equipment, but his fans were also willing to spend any amount of money it took to keep him in business.

Over the next few years, the teen managed to add several pieces of upgraded, high-tech equipment to his Amazon wish list, including hubs which would allow for the use of multiple cameras, upgraded memory cards to speed up the broadcast of his performances, and expensive high tech cameras. All the items he placed on his wish list were quickly purchased and rushed to his home.

You may be wondering how the teen managed to hide his growing enterprise from his parents. During the day, he hid his equipment behind his desk. At night, after his parents were in bed, out came the equipment and off came his clothing.

His business continued to grow. He was able to set up his own website for the sole purpose of self publishing his pornographic video with the assistance of one of his "fans." Throughout it all his grades remained good and his parents saw no reason to suspect that anything was amiss.

An untold number of services online made it incredibly easy for the teen to continue to grow and expand his business. He was able to take credit card payments through credit card processing services that would handle the payments without the need for tax identification numbers.

Other services allowed him to stream live video onto the Internet, free of charge, as long as company executives could receive a free peep. As if the thought of *that isn't frightening enough, other sites posted advertising from such sites and posted contests that would allow fans and viewers to vote for their favorite sites. As his business progressed, it didn't take the teen long to realize that he was one of just many teens who were basically prostituting themselves online for money and gifts. The offers on paid advertising sites to boost ratings of self-published child pornography sites were shocking to say the least.*

Teens offered to do practically anything on their webcam if viewers would vote for them and help to boost their ratings and rankings. Higher ratings and rankings meant more viewers, which translated to more money and more expensive gifts.

That's not all that was offered, either. Within a year of setting up his webcam, the teenager was encouraged to leave the safety of his home and meet a fan at a computer camp.

Thinking the camp would be educational and beneficial, the boy's parents let him go without a backward glance. They had no clue what was really transpiring. From that point, the requests to meet outside his home grew.

There was always an incentive in it for the teen, such as the opportunity to attend a special event as well as the lure of sex with teenage girls. In every instance, the teen was molested by the fans who lured him out.

As time went on, the requests for his performances continued to grow, and fans began to make personal requests for certain types of performances. The teen opened a second site, which he then charged a monthly subscription fee for along with payments for individual private shows.

In some cases, he would charge hundreds of dollars to perform for a single hour. He had no lack of customers. By this time, the boy was willingly meeting even more "fans" offline and was collecting thousands of dollars for the subsequent molestings.

Within two years, the boy's business took on an all new perspective. One of his fans agreed to rent an apartment for him so that he could perform without worrying that his parents might accidentally stumble across his business.

This allowed him to tell his parents he was simply going out to visit friends, when in reality he was only traveling a couple of blocks away to perform sexually in front of his webcam in the apartment one of his fans had leased for him.

As time went on, the teen would eventually leave home, flee to Mexico and create yet another site, where he would charge a monthly subscription fee which allowed others to watch him have sex with prostitutes. By this time he had become addicted to drugs and most of the money he made off his site went to fueling his drug habit.

By the time he was 18, he was recruiting others to perform on his site. The beginning of the end came when he was solicited for another offline meeting. As it turned out, the solicitor was a reporter for the New York Times.

With the reporter's help, the teen was able to turn over what he knew about the world of child pornography published via webcams to prosecutors and kick his drug habit. The FBI became involved, as the boy worked to identify the people who had solicited him over the years and children who were still involved in the business of online child pornography.

Shortly after his 19th birthday, the teen went into witness protection, received immunity and helped to track down one of the men who had molested him multiple times while still under the age of 18.

While this story is quite surprising, it is certainly not an isolated incident. When the story broke in the New York Times, it quickly became apparent that this teenage boy was just one of many who were part of what has become known as a Webcam Matrix, teenagers who operate their own websites for the purpose of self-publishing child pornography.

The sting investigation discovered that underage kids are running such sites completely aware of what they are doing, and yet they do it anyway. Most of these teens have coined a name for themselves as a result of their online activity.

They call themselves ‘camwhores’ because they are willing to do practically anything in front of their webcam if it means they can make money doing it.

While the previous story is certainly disquieting and disturbing, it is important to recognize that even if the adult in question is not inciting your children to transmit images of themselves, he could still be introducing your children to pornographic content.

This is one of the most common techniques used by sexual predators who prey on children. Most commonly, predators may send their young victims images that depict adults and children or youth engaged in sexually explicit activities in an attempt to show the child that this type of activity is normal.

Be aware that in order to discover whether your child may be the victim of this type of activity, you may have to be quite creative and even stoop to none other than what your child will certainly label as privacy invasion. Keep in mind that most youth won’t feel as though they have become a victim at all.

They will appreciate the fact that the friend they have been chatting with has provided them with content and images they have been curious about all along. They generally know you won’t approve, however, and will take steps to hide it from you.

Usually, you won’t find pornographic images on the hard drive of the computer, particularly if the computer is used by multiple family members. Instead, they will usually try to hide it on disks.

It is also important for parents to understand that the makeup of sexual predators can be completely different from the images that most of us harbor in the dark recesses of our minds. Most people think of sexual predators as older men, slightly unkempt with a certain “look” about them. Nothing could be further from the truth.

According to a study released by the National Center for Missing and Exploited Children, 96% of online predators seeking to solicit teens online are actually under the age of 25. Almost half of those are no more than children themselves under the age of 18 and almost 1/4 are female, not male.

The best thing you can do to protect your kids from this type of danger is to simply be aware of what your kids are doing and remain in tune with them and their activities. Make a point to notice whether your kids try to shut the door or shut off the computer monitor whenever you walk-by or enter the room.

If so, this could be a sign that they are engaging in activity online or chatting with someone they would rather you not know about. Of course, your child may simply be exercising the desire to have privacy, but you won’t know unless you take the time to investigate and most importantly keep the lines of communication open.

Starting from when they are an early age, take the time to appropriately discuss the potential dangers of online activity with your children. Ask them about their favorite sites, and if you aren’t sure about the content posted on those sites, find out.

If your child is visiting chat rooms, be aware that these can be some of the most dangerous sites online. While filtering software can be somewhat useful, they will not block all objectionable sites online.

Sites are constantly changing, and it can be difficult for even the best filtering software to keep up. Furthermore, any chat room can become dangerous when the wrong person enters with the explicit purpose of soliciting a child.

The best way to protect your children from this particular threat is to personally monitor your child’s chat room activity. Whenever possible, it’s also a good idea to keep the computer your child uses in a public area within your home.

When family members are frequently passing by, it becomes quite difficult for your children to hide any objectionable sites they might be visiting and most importantly, makes it difficult for would-be predators to contact them and continue contact.

Be prepared for the fact that your kids will feel as though you are saying you do not trust them and are trying to invade their privacy. But, even if your kids object, realize that this may be one of the most important conversations you have with your children.

Think of it in this perspective: wouldn't you rather have your child irritated over the seeming appearance of privacy invasion rather than picking up the phone to call 911 because a predator has kidnapped your child after meeting him or her in an online chat room?

Here are some signs that your child may be participating in dangerous activities online or at risk online:

- Spends large blocks of time online
- A large amount of online activity occurs at night
- Spends a lot of time in chat rooms
- Receives phone calls from people you don't know
- Makes phone calls to people you don't know
- Receives gifts and/or packages from people you don't know
- Shuts off the monitor, changes the screen or minimizes the screen when you walk into the room
- Becomes withdrawn from the family and family activities

If you notice any of the above highly suspect activities, you should immediately consider opening a conversation with your child regarding the potential dangers of online sex offenders. Be open and frank with them regarding the techniques that predators use and the dangers that can occur as a result.

Don't be afraid to monitor your children's activities. They won't like it, but this is perhaps the most important key to protecting your kids from dangers online.

Routinely review the material and content that is on your children's computer, particularly if they have their own computer that is not used by multiple family members. If you're not sure how to review the material, ask someone to help you.

Whenever possible, opt to share an e-mail account with your children rather than choosing to have separate accounts. This makes it that much easier for you to monitor their online activities and who they may be exchanging messages with online.

Keep in mind that monitoring your child's phone calls can be an important tool in the arsenal of protecting your child from potential online dangers.

It is also important to monitor your child's e-mail as well as instant messaging history. In order to be effective, random checks appear to work best. When your kids complain, and they will, initiate a frank discussion with them regarding your concerns and why you feel it's necessary to check their messages.

Keep in mind as well that while you may take every conceivable effort at home to protect your children from potential online dangers, you cannot always be there to physically protect them.

It is, of course, a good idea to find out what kinds of techniques are utilized by other locations where your child may log online, such as their school, the library or even their friends' homes to protect against online dangers; however, ultimately you must teach your children how to protect themselves.

That is why it is imperative that you discuss potential dangers with them:

- Counsel your children never to arrange an in-person meeting with someone they have met online.
- Remind them to never give out any information that could be used to personally identify and locate them.
- Explain why it is important that they never upload pictures of themselves onto the Internet or download pictures from a source they do not know well.

- Discuss the importance of not responding to any messages that may be objectionable.
- Ask them to select a screen name that provides anonymity, preferably one that does not reveal information regarding their gender or name.
- Teach them it's dangerous to share their password with anyone other than their parents. Unfortunately, password sharing has become a problem among today's youth. In fact, many teens see it as a true test of friendship.

Finally, make a point to let your children know that everything they are told online or read online is not true.

In the event that you feel your child has been targeted by an online predator, immediately notify your local law enforcement as well as the FBI and National Center for Missing and Exploited Children. Turn off the suspect computer and keep it turned off in order to preserve any evidence that may be present.

It is also important to understand how to protect your children from dangers they may encounter from an act as simple as checking their email. Unfortunately, there are far too many nefarious companies and individuals out there who will send objectionable unsolicited e-mail to anyone regardless of age.

Even if your children have never visited a site that you might find objectionable, they could be targeted by the kind of e-mail advertising. In the event that your children receive e-mail that is inappropriate and unsolicited (known as Spam) it is important that they understand they should report this to you immediately.

For your part, it is imperative that you not immediately jump to conclusions and blame your children. Chances are, they are quite innocent in the matter, and you certainly want to keep the lines of communication open.

Remind your child never to respond to such messages. Doing so only confirms to the sender that your child's e-mail address is live and working.

It is imperative that you not respond, not even to use the "opt out" option.

Instead, if at all possible, it's best to attempt to track down the company or the Internet Service Provider from which the e-mail was originated.

If this can be done, you should report the message as inappropriate. Depending on your e-mail options, you may also be able to block that specific e-mail address from further future contact. Future e-mails will automatically be directed to the Trash bin of your e-mail program.

Furthermore, be aware of the use of “cookies” and how you can use them to protect yourself and your children online. Basically, cookies are devices that are used by most sites online in order to track specific information about each user that visits the site.

This information may include email address, name and data about shopping preferences. Even if your child isn’t intentionally giving out such personal information, others could be able to obtain it when your child visits any sites that use cookies.

The good news is that these devices can be disabled. Usually this can be accomplished by selecting the Tools feature at the top of your browser, selecting Internet Options and Security; although, this may vary from one ISP to the next. If you’re not sure, be sure to contact your individual ISP for specific details on how to manage cookies for security purposes. Also, don’t forget to exercise the same parenting techniques regarding your children’s online activities that you would in any other aspect of their life. If your child makes a new friend, you usually will want to find out about that friend and be introduced to them before your child spends much time with them.

The same should be true for any friends your child makes online. Insist on being introduced to any online friends your child might happen to make. If the “friend” is a predator, he’ll usually disappear quickly enough when mom or dad enters the scene.

You should also be aware of the fact that sex predators are not the only dangerous people your child could encounter online. Individuals driven by hate and other intense feelings and emotions may also use the Internet in order to express their opinions—which may be at the expense of your child.

Usually, victims of cyberstalkers and cyberharassers are not actually targeted but more often are in the wrong place at the wrong time. The types of harm that may be inflicted by these individuals varies from activities such as hurtful comments and messages to true stalking activities.

In the latter, offensive e-mails may be sent to persons known by the victim, such as family and friends. The truly ingenious among the cyberstalker/harasser sect will even find a way to hack into the private email accounts of their victims and use these against them to lock them out or flood their inboxes with inappropriate Spam by signing their victims up for such content.

Once they are targeted by such persons, it may seem as though it is difficult to lose their trail. They may follow their victims into different chat rooms and onto various bulletin boards.

Untrue and misleading information may be posted about the victim. Just a few examples include posting sexually explicit images that have been doctored to include the face of the victim on sites known to be frequented by friends and family members of the victim.

When they are able to obtain it, these dangerous individuals may also post private and identifiable information regarding the victim online. In other cases, cyberstalkers have even been known to make death threats to others, all in the name of their victim.

If you suspect that your child has become the victim of such activities, contact your local law enforcement immediately.

Another problem that is a growing threat for teenagers on the Internet is cyberdating. Studies indicate that a surprising number of teens are using the Internet to conduct a variety of facets related to relationships and dating.

Many teens indicate that they have used email and instant messaging to ask out members of the opposite sex or even to break off relationships. Other youth are using online activities to meet potential love interests.

While cyberdating has become a popular technique for many adults with dating sites popping up like crazy all over the Internet, it must be stressed that cyberdating can be quite dangerous for adults with experienced decision-making skills. When it comes to teens, there is no safe way to cyberdate.

How to Protect Your Family's Personal Information Online

If you happen to surf online any at all, you probably know that the Internet is rife with scams and fraud. It's a con man's dream come true. Today one of the biggest concerns regarding society is the avoidance of identify theft.
Adults are not the only online users who need to be concerned about this problem; however. It is imperative that we teach our children how to avoid scams, frauds and cons.
Ideally, the best tool you can use to protect your child in this regard is to pass on the old adage to them, "If it seems too good to be true, it probably isn't true." It's also important to be aware of the various types of hoaxes and scams that make the Internet circuit. Some of the most common include:

- Disaster related scams—e-mails and even bogus websites that are used exploit and scam money from unsuspecting people who believe they are contributing to persons who have become victims of natural disasters. Following the wake of the 2005 hurricane season, Katrina related websites and e-mails flourished. Many of them were nothing more than scams.
- Nigerian e-mail scam—this one is particularly popular among con artists; although each new e-mail seems to develop a new twist. It usually comes with a story that indicates there is a large sum of money waiting for the would-be victim in an off-shore bank account, which the sender will share under certain circumstances. They typically request the deposit of a sum of money as show of "good faith."

In other cases, your kids may run into e-mails and sites that while not specifically designed to solicit money from them, are none the less nothing more than hoaxes designed to trick your child. Chain letters and urban legends are both included in this category.

By teaching your children that they simply cannot believe everything they read online, you can help to protect them from this type of fraud. If, up until this point, your biggest concern may have been whom your kids are exchanging e-mails with, it may be time to check-out just one of the ways many kids are meeting online.

Some of the most popular methods include blog and diary or profile sites as well as social-networking sites. In the past few years, social-networking sites in particular have become quite popular, both with adults and teens.

In the adult world, social-networking sites are used for a variety of purposes. Many higher level executives like to use them because it allows them to keep their fingers on the pulse of the industry across the globe.

It can be a great way to network and make connections that could eventually lead to better career opportunities. Other people like to use such sites specifically for the purpose of meeting potential love interests or simply as a way to connect with other individuals who share similar interests.

The dangers posed when kids use these types of sites are clearly obvious. Unfortunately, it can be difficult for even the sites to monitor whether underage users are logging on.

It's simply too easy for kids to lie about their age in order to access these sites. Ultimately, the best way to protect your child from any inappropriate contact or content they may come across through using this type of site is to stay in tune with your children, ask them about their use of such sites and follow-up to monitor sites they have visited in order to determine whether they are being up-front with you.

You can find out which sites your kids are visited by accessing the cached Internet history of the computer your child uses. If you're not sure how to do this, be sure to ask someone who is knowledgeable to help you.

You can also determine whether your child may be accessing a social networking site by performing a search and entering your child's e-mail address or name. If your child has posted a profile page on one of these websites, it should pull up.

It is also important that you find out whether or not your child has created a web site online. Web sites can be created quite easily online.

There are numerous ISPs that provide a variety of hosting options ranging from free to quite inexpensive. Interviews conducted with teens and youth indicate that some 57% have logged online in order to create content for the Internet.

This content can range from something as simple as creating a blog, a type of web based diary, to something more complex as creating a personal webpage. Teens post a variety of content online, including artwork, stories, videos, photos and remixes of content they have found elsewhere.

For many teens, online content creation can be a creative outlet. So, where's the danger? You might ask yourself. When used correctly and responsibly, there is no danger at all.

However, teens aren't always responsible, and they may not be aware of the danger they may be creating for themselves by simply creating and posting content online. If the site that your teen has created is in any way defamatory or objectionable, your child could actually land themselves in trouble with the law. Even considering Freedom of Speech, your child may be considered highly suspect if they create material that is comprised of hate messages. Even if you are completely unaware of your child's online activities and content creation, you may also be held responsible as your child's legal guardian for whatever activities and content they posts on their site.

There is also the possibility that your child could get into serious trouble associated with copyright laws. Far too many teens have no problem whatsoever with taking creative license and borrowing content from elsewhere and posting it on their own sites.

Unfortunately, this is known as plagiarism and the penalty can be rather stiff, including large fines. Once again, even if you are unaware of your child's activities, you will still be responsible if your child is convicted of copyright infringement.

One of the most notorious cases of this type of activity occurred in the recent past when several teens and youth were found to be guilty of downloading free music. While the cases remains largely debatable, the fact remains that in the end the kids who were found to be guilty, and their parents, were still responsible for paying large penalties and fines.

In case you're not familiar with this problem, it works something like this: the teen logs on to any one of a number of sites that allows the downloading of popular songs for free. The teen then generously shares the downloaded music with friends.

At this point, the teen has distributed copyrighted music without the permission of the artist; this naturally cuts into the profits of music groups and music producers. Needless to say, they're not too happy about it and have taken very strict steps in order to track down kids who are downloading and distributing music for free.

The problem with most teens is that they see absolutely no problem with what they're doing. In fact, most teens believe it's unrealistic to expect them not to do it.

Even when it became apparent that music industry groups were tracking down individuals found to be guilty of music downloading and sharing, most teens still indicated they saw no problem with it and were not worried about getting caught.

Regardless of which side you happen to take in this questionable situation, the facts remain the same. Downloading and distributing music for free has been deemed to be illegal and the penalties are far from pretty.

Teens as young as 13, and their parents, were ordered to pay thousands of dollars in reparations in some cases. The teens were identified when they logged on to download their music through their ISP.

So, if you begin to notice that your kids are suddenly enjoying tunes that you know you didn't purchase for them and that they did not have the funds to purchase on their own, it's time to find out exactly where and how they are coming by their music.

You may also find it helpful to understand exactly what website operators and administrators are allowed to do and not allowed to do when it comes to content, information exchange and your teens.

By law, operators of websites must post a privacy policy. Furthermore, website that are directed toward children or that are aware they are collecting information from children under the age of 13 must also post a notice of their information collection practices. This notice must include the following information:

- Types of personal information they collect from kids—for example, name, home address, email address or hobbies.
- How the site will use the information— for example, if the information will be used to market products and information to the child who supplied the information, to notify contest winners, or to make the information available through a child's participation in a chat room.
- Whether personal information is forwarded to advertisers or other third parties.
- A contact at the site.
- The need to obtain parental consent. Generally, a site must obtain parental consent before collecting, using or disclosing personal information about a child.

Be aware that consent is not required when the site is collecting an email address only for the following purposes:

- To respond to a one-time request from the child.
- To provide notice to the parent.
- To ensure the safety of the child or the site.
- To send a newsletter or other information on a regular basis as long as the site notifies a parent and gives them a chance to say no to the arrangement.

Website are also required to obtain new consent when information-practices change in a "material" way.

For example, website operators are required to notify the parents and obtain consent any time they change the type of information they collect or change the way in which they use the information. They are also required to notify the parents at any time in which they offer the information to new and different third parties.

Additional access may not be provided to the child by the operator of the website if it extends beyond the boundaries of the parents' original consent. Under this example, the website administrator would be unable to grant access to a chat room if the parents did not originally specify it in their consent.

Parents are also allowed to review personal information collected from their children. The identity of the requesting parent usually must be verified by the website operator.

Parents, furthermore, may revoke their consent and request that the operator delete information collected from their children. When revocation by the parent is initiated, the website must stop collecting, using or disclosing information from that child.

At this time, the site may end a child's participation in an activity if the information it collected was necessary for participation in the website's activity. The Children's Online Privacy Protection Act provides further information and control for parents regarding the type and amount of information that is collected from children online and how that information may be specifically used.

Commercial websites and online services that are directed toward children under the age of 13 and that collect personal information are covered under the rule. Operators of general audience sites that knowingly collect personal information from children under 13 as well as operators of general audience sites that have a separate children's area and that collect personal information from children under 13 are also covered. Under this rule, these sites and their operators are required to meet the following stipulations:

- Post a privacy policy on the homepage of the Web site and link it to the privacy policy on every page where personal information is collected.
- Provide notice about the site's information collection practices to parents and obtain verifiable parental consent before collecting personal information from children.
- Give parents a choice as to whether their child's personal information will be disclosed to third parties.
- Provide parents access to their child's personal information and the opportunity to delete the child's personal information and opt-out of future collection or use of the information.
- Note a condition for a child's participation in a game, contest, or other activity or on the child's disclosing more personal information than is necessary to participate in that activity.
- Maintain the confidentiality, security and integrity of personal information collected from children.

With this information parents can take a more proactive role in controlling the information their children are allowed to access online by:
Looking for a privacy policy on any website directed to children. Keep in mind that the policy must be available through a link on the website's homepage and at each area where personal information is collected from kids.
Websites that are targeted for general audiences and that have a children's section must post the notice on the homepages of the section for kids. Once you have located the policy, take the time to read it closely in order to learn the kinds of personal information being collected, how it will be used, and whether it will be passed on to third parties.
If you run across a website that fails to post basic protections for children's personal information, ask for details about their information collection practices.
After reading the privacy policy, make a decision regarding whether to give consent.

Keep in mind that giving consent authorizes the website to collect personal information from your child. It is permissible to give consent and still refuse to have your child's information passed along to a third party.

Be aware of the fact that your consent isn't necessary if the website is collecting your child's email address simply to respond to a one-time request for information.

You may wish to decide whether to approve information collection from your kids depending on new uses for the information. Remember that in the event that the website changes the terms of their use of information in a material or significant way, they are required to let you know about the need for a new consent.

Don’t forget to ask to see the information your child has submitted and remember that the site will ask you to verify your identity to ensure that your child's information isn't given out improperly.

You should also understand that you may revoke your consent at any time and have your child's information deleted.

In order to stop a website from collecting additional information from your child, you can revoke your consent. You also may ask a site to delete any personal information it has already collected from your child.

Afterward

The most important thing you can do to protect your children from the dangers of online predators and other risks from the Internet is use your own common sense. Rather then giving a stranger the opportunity to prey on your young ones, realize the predator is looking for someone who is vulnerable.

If you spend time with your children while they are online, educating them regarding the risks and letting them know you will be monitoring their time on the Internet, you should be fine. It's the children who are left unmonitored and uninformed regarding the risks involved who are most at risk.

The Internet allows for great opportunities but also offers great risks. The more time we spend with our children and the more we can educate our children, the better for everyone concerned.

Resources

Internet Service Providers that provide blocked access:

Integrity Online (http://www.integrityonline.com)

This.com (http://www.this.com)

Mayberry USA (http://www.mbusa.net)

Filtering Programs and Software:

Norton Internet Security: http://www.symantec.com/sabu/nis/nis_pe

Cyberpatrol: http://www.cyberpatrol.com

Net Nanny: http://www.netnanny.com

CyberSitter: http://cybersitter.com

American Family Filter: http://afafilter.com

WiseChoice: http://wisechoice.net

To report online exploitation of children:

National Center for Missing and Exploited Children (NCMEC):

http://www.missingkids.com

To report child pornography online:

The National Center for Missing and Exploited Children at http://www.cybertipline.com. To report instances of child exploitation, the center's hot line is 1-800-843-5678.

For more information on potential criminal activity on the Internet:

http://www.usdoj.gov/criminal/cybercrime/reporting.htm