Cyber-Safe Kids Cyber-Savvy Teens

Helping Young People Learn to Make Safe and Responsible Choices Online

Nancy E. Willard

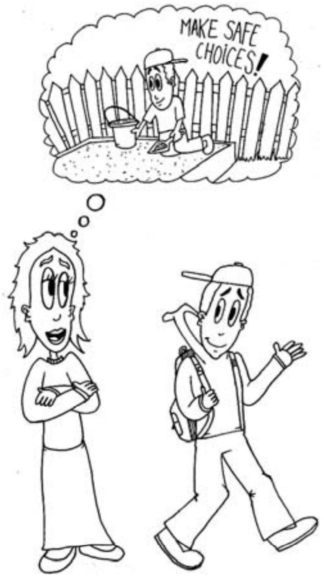
Author of: *Cyber-Safe Kids, Cyber-Savvy Teens: Helping Young People Learn to Make Safe and Responsible Choices Online*

Introduction

The Internet provides wonderful opportunities. It can enhance our children's lives and deepen their understanding of themselves, their friends, and the global community. The Internet has become an intregal part of our society.

But there are dark sides to this wonderful resource.

- Young people may be harmed by other people online.
- Some young people are making unsafe or irresponsible choices that result in harm to themselves or others.



Parenting in the Real World

Our children also face risks in the "real world" ~ sharp knives, speeding cars, bullies, weirdos at the park, pressure to engage in sex, drug pushers, and many more. Sometimes they simply do not make good choices.

When children are young, we keep them in safe places and teach them simple safety rules. As they grow, we provide them with the knowledge, skills, and values to independently make good choices ~ and we remain "hands-on" to ensure they do.

Effective Parenting in Cyberspace

Keeping children and teens safe online requires applying effective real world parenting skills to cyberspace.

- When children are young, they do not have the cognitive development or experience necessary to keep themselves safe online. *How:* Parents must establish a safe online environment and provide simple, easy to follow guidelines.
- As children grow and their online activities expand, it is necessary to make sure they know how to independently make good choices. *How:* They need to know what the risks are. They must know how to avoid getting involved in a risky online situation, how to detect if they are at risk, and how to respond effectively, including when to ask for help.
- They also must know the importance of engaging in responsible, ethical behavior. *How:* They must understand that it is important to keep themselves from harm, not cause harm to someone else, and make sure their friends are safe.
- Parents must pay attention to what their children are doing online.

"Digital Natives" and "Digital Immigrants"

Young people are the "natives" in this new online world. We adults are the "immigrants." Many young people don't tell adults about Internet concerns because they fear that adults will overreact, blame them, not know what to do, do something that will make things worse, and/or restrict their online access. It is essential to establish a trusting relationship and work in partnership with your child related to Internet activities.

Focus on the Positive

Most young people are having fun and engaged in healthy interactions with others online. Internet risks and concerns can be effectively managed through education and parental attention. This brief guide will provide you with an overview of Internet risks and concerns, recommended parenting approaches, and information about strategies to address foundational issues and key online risks and concerns. For more information on all issues addressed in this handbook, as well as other risks and concerns, please read *Cyber-Safe Kids, Cyber-Savvy Teens: Helping Young People Learn to Use the Internet Safely and Responsibly*.

More resources are available on the *Cyber-Safe Kids, Cyber-Savvy Teens* web site at http://cyber-safe-kids.com and on the Center for Safe and Responsible Internet Use site at http://csriu.org. Illustrations by Mike Novotny.

Internet Risks and Concerns

Internet risks and concerns range from situations where innocent young people are victimized by others to situations where young people have engaged in actions that are risky, irresponsible, harmful, and even illegal. The following are the key risks and concerns. *Remember:* All of these risks and concerns can be effectively addressed through education and parent attention.

Sexual Related

- Groomed by predators for sexual activities or pornography.
- Seeking sexual "hook-ups" with adults or other teens.
- Accidentally accessing online pornography.
- Intentionally accessing pornography in an addictive manner.
- Engaging in or receiving sexual harassment.
- Posting sexually provocative images or discussing sexual exploits.

Cyberbullying

- Being the target of nasty messages, cruel postings, impersonation, and other forms on online social aggression or engaging in such online aggression.

Scams

- Being deceived by an scam or identity theft.

Cyberthreats

- Posting material that raises concerns about the potential of committing violence towards self or others.

Unsafe Communities

- Interacting with online communities that support self-harm, including self-cutting, anorexia, drug use, and suicide.

Dangerous Groups

- Interacting with angry and violent online groups, including hate groups, gangs, or troublesome youth groups.

Online Gaming

- Excessive involvement in online games, especially violent games.

Online Gambling

- Engaging in "gambling 101" game activities or actual online gambling.

Hacking

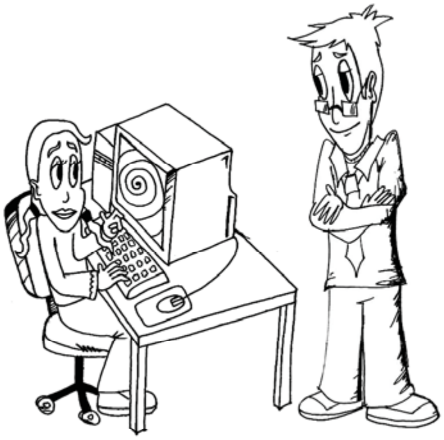
- Breaking into or damaging computer systems.

Plagiarism

- Inadvertently or intentionally using online information resources in an academically dishonest manner.

Copyright

- Inappropriately copying or disseminating someone's copyrighted work.



Online Activities

Social Networking Sites

Social networking sites allow young people to express their personal identity and maintain electronic connections with friends. Young people create profiles and blogs to share their interests and thoughts, establish friendship links, and engage in public or private discussions.

Popular social networking sites have:

- Excellent terms of use.
- Practices to allow users to control who has access to their profile and information.
- Procedures for complaints.

Social Networking Concerns

- Posting inappropriate material.
- Making unsafe connections with others.
- Engaging in or receiving sexual solicitation.
- Cyberbullying.
- Addictive behavior.
- Tweens lying about age to join teen sites.

Commercial Sites

Market Profiling

Commercial sites encourage users to disclose personal information, including demographics and interests. This is used to tailor advertisements. Sites frequently offer “gifts or prizes” in exchange for completing online marketing surveys.

Advertising

Website advertisements may promote unhealthy consumption, lifestyle, values, and behavior.

Stickiness

Web sites use specific strategies to enhance their “stickiness.” They entice young people to spend lots of time on their site and return often.

Online Advertising Techniques

- Advergaming ~ advertising integrated into online games and activities.
- Permission marketing ~ asking young people to sign up to receive newsletters and coupons.
- Viral marketing ~ encouraging young people to promote products and services to friends.

Other Activities and Technologies

Chat Rooms and Discussion Groups

In chat rooms and discussion groups teens can discuss issues with friends, acquaintances, or strangers.

The level of safety depends on the site, subject discussed, members, and whether there is a moderator.

Instant Messaging

Instant messaging (IM) is real time electronic communications.

The level of safety depends on who is on your child’s contact list.

Cell Phones and Personal Digital Devices

Many of today’s young people are totally wired. They can go online anytime, anywhere.

This limits your ability to effectively supervise.

Digital Cameras, Cell Phone Cameras, and Web Cams

Young people can easily capture, modify, send, and post images.

Inappropriate images posted by your child ~ or others ~ could damage your child’s reputation, attract an unsafe person, be used for cyberbullying, or lead to criminal charges.

General Internet Safety Guidelines

- Frequently discuss values and standards regarding online activities.
- Effectively address computer security.
- Keep the computer in a public area of your house, so you can peek over your child's shoulder from time to time.
- Establish standards regarding Internet use when you are not present.

Internet Use Through the Ages

Younger Children

Younger children should only use the Internet in safe places.

- Safe, bookmarked Web sites.
- Electronic communications limited to known friends.

Important Rules for Children

- Don't go outside the safe online places without an adult.
- Never type your name, address, or phone number online.
- If something "yucky" appears, turn off the monitor and tell an adult.

Older Children

Older children will want to expand their online activities.

- Involve your older child in deciding what sites are appropriate and why.
- Introduce safety and responsible use issues in a manner consistent with your child's development and online activities.
- Restrict communications to known friends or well-managed anonymous sites.

Tweens

Tweens are expanding their online activities even more. Many tweens want to participate in socisl networking sites for teens and adults ~ which is not advisable. Look for attractive and safe tween sites.

- Allow more freedom in finding new appropriate sites, continuing to focus on appropriate standards.
- Increase discussions of risks and protection strategies. By the time your child is a teen, he or she should have a good understanding of all risks and protective strategies.
- Continue restricting communications to known friends or well-managed anonymous sites.

Social Networking Protections

- Set profile to private ~ but emphasize that a private profile is still public!
- Limit friendship links to known friends and friends of friends.
- Regularly review your child's profile and friends.
- Promptly remove inappropriate material posted on their profile.

Early Teens

Early teens are at greater risk online because their online activities are significantly expanding, including on sites with older users.

- Consistently monitor your child's online activities.
- Make sure your child has a good understanding of risks and protection strategies. Discuss these issues frequently.
- Join their online world. Communicate with your child electronically. Set up your own social networking profile and link as "friends."

Older Teens

By this age, your child should know how to independently use the Internet safely and responsibly. This provides time for "fine-tuning" before your child turns 18.

- Allow your child to earn the right to have a computer with Internet access in his or her room or a personal digital device with Internet access ~ by demonstrating a history of good choices online and willingness to discuss online issues.
- Continue to discuss issues and, if concerned, check the history file.

I'm Your Parent. It's My Responsibility

Monitoring Online Activity

Parents should pay close attention to what children and tweens are doing online. They generally do not have concerns about privacy. Teens naturally are more concerned about their privacy. But it is important that you pay attention to what they are doing online. It is helpful to distinguish between public and private online activities. Here is a recommended strategy to approach monitoring with your teen:

> "It is necessary for me to be sure you are making good choices online because it is my responsibility. I will periodically review your history file and postings in public places. What you post in public is public. As I see that you are making good choices, I will reduce this monitoring. I will review your personal communications only if I have reason to suspect something is wrong. In most cases, I will discuss my concerns with you before any review."

Making Inappropriate Choices Online

These are some of the reasons teens might make inappropriate choices online.

"You can't see me."

Online users perceive they are invisible online or they can take steps to be anonymous. This reduces concerns about detection, which could lead to disapproval or punishment.

"I can't see you."

Online users do not receive tangible feedback about the consequences of online activities. This can interfere with the recognition they have caused harm and can result in the lack of remorse.

"I didn't think."

Teen's brains are a "work in progress" ~ developing the capacity for effective decision-making. Sometimes they are biologically incapable of thinking clearly.

"Who am I and where do I fit it in?"

The major life task for teens is establishing their personal identity, values, and relationships with others. Their profile allows them to experiment with different "personalities."

"Am I hot?"

Teens are exploring their emerging sexuality and personal relationships in online environments. They are exposed to highly sexualized advertising images.

"If I can do it online, it must be okay."

Teens may forget that "real world" values should control their online choices.

"Everybody does it."

Other teens and adults are making inappropriate online choices.

"I'm doing what they say."

Dangerous individuals and groups, as well as commercial sites, use sophisticated techniques to manipulate online users.

"Looking for love."

Teens who face "real world" personal challenges ~ including mental health issues, difficulties in school, and/or challenges in relationships with family or friends ~ are at high risk online. They frequently seek attention online. They are less likely to pay attention to obvious risks or make good choices. They are highly vulnerble to manipulation.

Not Equally at Risk Online

Young people are not equally at risk online.

- Many competent young people are making safe and responsible choices.
- Naïve tweens and teens could make mistakes as they begin to engage in social networking and other interactive teen sites.
- The young people who are at greatest risk online are the ones who are vulnerable because of "real world" personal challenges.

Protection Technologies

Computer Security

Parents must ensure that all family computers have effective security.

- Firewalls and protections against viruses and other “malware” (malicious software).
- Spam blocker.
- Browser configured to block pop-up ads.
- No peer-to-peer networking software because it is a significant source of malware.
- Search engine preferences set to filter search results.

Monitoring Software

Monitoring software can provide a full and complete record of where your child goes online, as well as all outgoing and incoming communications. Use of monitoring software could interfere with a relationship based on mutual trust.

- Might be an appropriate consequence if your child has engaged in irresponsible online behavior. Tell your child it has been installed and under what circumstances you will review the records.
- Might be useful if you fear your child is in danger from someone online and you need more evidence. It is likely best not to tell your child if you really think your child is in danger.

Time Limiting Software

Time limiting software can limit access when you are not present or late at night, when you are asleep. It can also be used to enforce time limits.

Filtering Software

Filtering software may provide some protection against accidental access. But it will frequently not block the most dangerous “porn traps” because the traps access new sites that have not yet been detected and blocked.

Filtering software will not deter a determined teen. Filters can be easily bypassed using proxy sites or the teen will simply use another computer or personal digital device. (Search for: bypass, internet, filter.)

Protection Strategies

The following pages will address:

Foundational Protection

- Protect privacy and personal information.
- Enhance information literacy.
- Prevent addictive access.
- Develop stranger literacy.

Strategies to Address Key Risks

- Sexual predators.
- Accidental access of online pornography.
- Scams and identity theft.
- Cyberbullying.

None of Your Business

Privacy and Personal Information

Some teens reveal personal information online in ways that present concerns. They appear to be unaware that public postings are public or that information shared privately in electronic form can easily become public. They appear not to recognize that this disclosure may place them at risk, damage their reputation, jeopardize relationships, or interfere with their future education and career plans.

Teach your child how to protect different kinds of personal information online. Make sure your child knows to tell others to remove any of their personal information ~ and to tell you if someone has posted this material and will not remove it.

Personal Contact and Financial Identity Information

- *What:* Full name, address, phone number, personal identity or financial account numbers, or passwords. *Protect:* Should only be provided on a secure site for an appropriate purpose. Children, tweens, and early teens should not post without parent permission. Older teens must know how to provide such information safely on secure sites. (Secure sites start with https://.)

Intimate Personal Information

- *What:* Private, personal, sensitive ~ comunicates "I am vulnerable." *Protect:* Tell your child never to post this on public sites ~ this is high risk. Although there is some risk, may be appropriate to share intimate information in a private message with a very trustworthy friend or anonymously on a professional online social support site.

Reputation-Damaging Material

- *What:* Any information or images that could damage your child's reputation or interfere with future educational and career plans. *Protect:* Tell your child to never post or send such material.

Personal Interest Information

- *What:* General information about personal interests and activities. *Protect*: Generally safe for teens to share this kind of information if they do not also provide personal contact information. This information will be used for market profiling and advertising.

Personal Information About Others

- *Respect:* Personal information about other people should not be shared online, publicly or privately.

Keeping Life in Balance

Addictive Behavior

Internet addictive behavior is an excessive amount of time spent using the Internet, resulting in lack of healthy engagement in other areas of life. Children and teens need to spend time with their family and friends ~ engaged in play, physical activities, arts, social service, or just "hanging out." Social networking and gaming sites can be highly addictive. Excessive time spent online is a risk, in and of itself, and an indicator of other risky behavior.

- Parent involvement is necessary to ensure your child's activities remain balanced.
- Develop a mutual agreement about the amount of time to be spent online and strategies to support engagement in other activities. Use time limiting software to support this arrangement, if necessary.
- Make sure your child is not surfing, gabbing, or gaming when there is homework to be done. This can interfere with effective learning.

Read With Your Eyes Open

Information Literacy

There are no “Cyberspace Truth Monitors.” Too many people determine credibility based on appearance ~ which can be very deceptive. Teach your child to access the accuracy of online information. *How:*

- Consider how important it is that the information be credible.
- Assess how controversial the issue is because this affects potential bias.
- Reflect on how you got to a site or received the information.
- Evaluate the source of the information looking for potential bias and what the source is seeking or has to gain if you agree with their information.
- Determine whether the information is fact-based or opinion-based.
- Determine whether the information is consistent with information found through other sources. If there is conflict, there is need for greater care.
- Find out who links to this site and thinks the information is credible.
- Ask for the opinions of others, especially parents, teachers, and librarians.
- Evaluate the information itself. Is it consistent with what is known to be true?

Don’t Take Candy From Strangers

Stranger Safety

Children and tweens should be protected against communications with online strangers, except on very well-moderated, anonymous sites. Teens can be expected to have online interactions with people who they do not know ~ or know only as an acquaintance or “friend of a friend.”

The vast majority of online strangers are perfectly safe. BUT some are not.

Protection Strategies

- Teens must learn to determine the safety and trustworthiness of an online stranger. *How:* Carefully review this person’s online postings and friends. If there are ever any concerns, block all communications from this person.
- Teens may want to meet with someone they met online and must know how to do so safety. *How:* Meet in a public place with trusted friend or parent nearby.

Unsafe Online Strangers

- Adult sexual predators or teens seeking sexual “hook-ups.”
- “Recruiters” for dangerous groups.
- “At risk” teens who are engaged in unsafe, irresponsible, or illegal activities.

STRANGER DANGER RED FLAGS

Teens must recognize the RED FLAGS!

> **“Watch out for anyone, especially an adult, who sends overly-friendly messages, tells you how special or wonderful you are, offers gifts or opportunities, tries to establish a special or secret relationship, asks for a sexy picture, or tries to turn you against your parents or friends. These are signs of danger!”**

Tell your child to save any “red flag” messages and show them to you. Promise your child in advance that you will not overreact or restrict their Internet access.

Don’t Hook-up With Online Losers

Sexual Predators

Online predators generally target teens, not children. Teens can more easily be groomed to engage in sex and can more easily travel to meet. Young people are more often sexually victimized by people from their own family or community. These “real world” predators could use the Internet to maintain control and could create child pornography using their child or teen victims. Teens may also be at risk from predatory teens who are seeking sexual “hook-ups.”

Predator Interest

- *Vulnerable Teens:* Emotionally vulnerable. Problems with family or friends. Publicly exploring sexual questions.
- *Interested Teens:* Post sexually provocative images. Use sexually inviting usernames. Go to sites where people arrange for sexual “hook-ups.”

Protection

- Pay attention to material your child is posting to make sure none of it indicates vulnerability or sexual interest. Also, review the sites your child visits through the history file top see if they are sexual in nature.
- Regularly review your child’s social networking and IM friends. Ask how they know each person.
- Seek professional assistance, if warranted.
- Your child must know to watch out for the online “Stranger Danger Red Flags” and respond appropriately. If your child does tell you about an inappropriate contact, do not overreact. Acknowledge and applaud their attention to potential danger.
- If you suspect that your child is communicating with a predator, contact the police. Do not inform your child that you are doing so. Your child could warn or run off with the predator. Create a safety plan for your child.

Avoid the Porn

Accidental Access of Pornography

Children or teens may accidentally access online pornography.

Prevention

Make sure you have implemented effective computer security. Protect your younger child by limiting access to bookmarked sites and closely supervising open explorations. Tweens and teens must know how to surf safely. *How:*

- Don’t click on a link, if you do not know what you will access.
- Don’t type a URL. Type the name of the site in a search engine.
- Can the porn spam. Don’t open suspicious email messages or click on links in email unless you are sure they are legitimate.

Response

- *Children:* If “yucky” material appears, immediately turn off the monitor (teach them how), and get your help.
- *Tweens and Teens:* Turn off the monitor, force-quit the browser, or turn off the computer, and tell you what happened, so you know it was a mistake.
- *After Any Incident*: Evaluate your computer security. Review what happened to prevent future incidents. Use the “teachable moment” to discuss values. Never punish your child for accidental access.

Too Good To Be True

Scams and Identity Theft

Scam Indicators

- "Too good to be true!" "Free lunch!" "Act now or you will lose!" "You could win!" "Business opportunity!"

What Scammers Want

- Personal contact or financial identity information.
- Participants for risky or illegal activities.

Market Profiling Scams

- Offers of free "goodies" and contests online are common techniques used to obtain personal and interest information to be retained in a market profile and used for advertising.

Protection

- Protect personal contact and financial identity information.
- Be alert to all scam indicators. If it looks like a scam, it probably is.

CyberbullyNOT

Cyberbullying

Young people are sending nasty messages, posting cruel material, impersonating others and engaging in other online aggression.

Cyberbullying can range from minor incidents to devastating harm. Cyberbullying may be more harmful than in-person bullying because it can happen 24/7, can be very public, and bullies can be anonymous. It may cause significant emotional distress, school failure and avoidance, suicide, and harmful retaliation.

Targets

Prevention and Detection

- Ensure your child does not post information that could be misused and communicates respectfully with others.
- Pay attention to the quality of your child's online communities and friends.
- Work with your school to stop any school bullying.
- *Signs of Concern:* Emotional distress during or after being online. Disrupted friendships. School avoidance.

Response

- Never Retaliate! Save the harmful material.
- *Responses to Minor Incidents:* Calmly tell the cyberbully to stop. Ignore or block the cyberbully. File a complaint with the web site or service. Tell your child to ask for your help if these steps do not work or the harm is significant.
- *Other Response Options:* Send the online material to the bully's parent with a demand that it stop. Ask for assistance from school. Contact an attorney or the police.

Bullies

- Deter your child from engaging in cyberbullying by emphasizing the importance of treating others kindly online and through monitoring.
- If your child has been unkind online, take proactive steps to ensure this does not continue. You can be held legally liable for harm caused by your child.

NEW TEXT: You @*$@! I'm gonna get you!
EMAIL: MIND YOUR OWN BUSINESS @*$@!

Bystanders

Encourage your child:

- Promote respectful communications.
- Assist those who are being cyberbullied.
- Tell a trusted adult.

Detecting and Responding to Concerns

Key “Red Flags”

- Appearing emotionally upset during or after Internet use.
- Disturbed relationships with parents, family, or friends.
- Spending too much time online, especially late at night.
- Excessively secretive behavior when you approach the computer or an empty history file. (Teens are likely to be somewhat secretive.)
- Receipt of packages or phone calls under strange circumstances.
- Subtle comments about online concerns. It is very important to respond carefully to such comments. Remain calm and try to encourage your child to talk further. Your child will likely be worried that you will overreact.

Responding

- Do not overreact! Take the time to calm down before doing anything,
- Investigate further. Use monitoring software if you think your child is at significant risk.
- Carefully engage your child in a conversation about Internet activities.
- Respond to unsafe or irresponsible behavior with an appropriate consequence that will remedy any harm and help your child learn to make better choices in the future.
- Seek professional assistance to create a safety plan, if warranted.
- If you find evidence of a predator or other dangerous individual, do not confront your child. Contact the police and create a safety plan.

What You Do Reflects on You

Making Good Choices Online

Common Values

Support your child in making good choices online by emphasizing important values and standards. Ask your child to review the standards set forth in the school Internet use policy and the terms of use agreements for sites and note how these standards are similar to your family’s values.

Teachable Moments

Use “teachable moments,” like news articles or incidents, to discuss online issues and problem-solving.

Ethical Decision-Making Questions

- Is this kind and respectful to others?
- How would I feel if someone did the same thing to me, or to my best friend?
- What would my mom, dad, or other trusted adult think or do?
- Would this violate any agreements, rules, or laws?
- How would I feel if my actions were reported in a newspaper?
- What would happen if everybody did this?
- Would it be okay if I did this in Real Life?
- How would this reflect on me?

Leadership

Encourage your child to be a leader. *How:* Model good choices. Talk with friends about their choices. Speak up for good values in social networking communities. Offer help to someone who is being harmed. Emphasize to your child the importance of reporting to you, or another trusted adult, if he or she witnesses online harm or thinks that someone is making or considering a bad choice.