



Susan Frasca

Cyber Safety

South Florida Parenting

Not that long ago, you could only see a movie in a theater, babies could ride in a car on someone's lap, there were no cordless - let alone cellular - phones and the library was pretty much the only place to do research on a topic.

Now we rent and buy feature movies to view from the comfort of our own sofa and make work-related phone calls while watching our children at soccer practice. Car seats, seat belts and air bags, when used properly, add safety to travel. Home computers can access information once available only at a local library.

As technology has responded to many of life's bigger and smaller obstacles, it also has created the need for responsible use. Just as you insist your children wear seat belts, it's wise to provide guidance, supervision and rules as children to use the limitless resources available on the Internet.

Any expert will tell you that the responsibility to teach, guide and supervise kids lies primarily with parents. However, most parents don't feel qualified when it comes to cyberspace because their kids know more about the Internet than they do.

Parry Aftab, Internet safety expert, author of two books on cyber safety and executive director of the web site CyberAngels.org, urges parents to make the time to "understand how the Internet works and understand what the risks are so they can take steps to minimize those risks." In its "Internet Crimes Against Children" bulletin, the Department of Justice notes that with an estimated 45 million kids online by 2002, "it is extremely important for parents ... to know as much as possible about the Internet so they can prevent victimization."

Exposure to pornography and unsolicited information along with interaction with predators are the biggest dangers kids face in cyberspace today. Invasion of privacy and financial theft also cause concern.

Invasion of Privacy

The slightest bit of information your child gives about himself could provide advertisers and strangers with more than you want them to know. Potentially harmful marketing and data collection from or about children under age 13 is prohibited by the Children's Online Privacy Protection Act, and is enforced by the Federal Trade Commission. However, strangers could gain access to personal information about kids through online chat and personal profiles. CyberAngels.org, widely considered the leading specialty organization on cyber crime, implores parents, educators and caregivers to carefully teach children not to share personal information online, whether on a profile or in a chat room. Personal information can include name, address, phone number, school or team names, parental work

information and so on. A seemingly harmless online conversation about your son's school football team and next practice could result in a visit from a total stranger.

Financial Theft

Online purchasing is generally considered safe, as long as parents follow a few rules. Children shouldn't have access to parents' passwords for their Internet service provider or to their user accounts on web sites. CyberAngels.org recommends shopping at secure sites only (those protected by SSL, a computer security language) and going to a site from a major search engine. AOL has an approved-vendor site and will refund any money lost in a transaction made with any of their approved vendors. Yahoo checks all sites it lists, using people, not search engines. Also, it is easier to detect fraud if you use only one credit card for online purchasing.

Unsolicited Information and Pornography

Most of us have heard the stories by now. A child doing a report on the president of the United States innocently ends up at a web address a far cry from 1600 Pennsylvania Ave. Simply changing the URL (.com, .org, .net) of a legitimate, inoffensive site can expose a child to the very things parents strive to shield them from. Children are likely to encounter hate, discrimination and pornography on the web because the web is global - what is illegal in one country might be legal in another. "But that doesn't mean that parents, educators and caregivers shouldn't be able to screen out some of these materials when they do not believe that their child is ready to be exposed to such information," Aftab says.

Filtering software can help screen out a great deal of unwanted material, but first parents need to know what they want from a filtering program. If you want to stop pornography and other unwanted material from reaching your family computer, a program that has a list of banned and acceptable sites is helpful. Customized word lists can be created by parents and downloaded into the filtering program. If an unacceptable word appears, filtering programs aim to block the transmission or alert parents via e-mail. Though not foolproof, they are a deterrent. The downside is that they may end up blocking useful, informative, "good" sites as well. Melanie Carter, founder of myndatease.org, a nonprofit organization dedicated to safety on the Internet, says that filtering programs sometimes block her site because it contains references to or information about inappropriate or objectionable content.

For parents who want to find out what their kids are doing online, there are programs that record every keystroke a child makes when at the computer and other programs that take screen shots of what the computer user is viewing. If time restrictions are a problem, parents can program the amount of time children spend online. They will be booted off, usually with warning, when time has expired. Recent technology has introduced filtering software that allows parents to supervise their children without directly accessing the monitored PC. This means that a parent can be at work, or even out of town, and still have the ability to know what their child is doing online in real time.

Carter says that it's a natural reaction for children to rebel against and bend rules. They need to know that their cyber activity will be monitored just as their friendships and activities are. Though some kids might consider this spying, experts encourage parents to inform children that they will be "watched" to protect and guide them as they learn their way safely about the Internet on their own. When it comes to safety, "parental rights and responsibilities usurp those of a child's right to privacy," Carter

says.

Predators

The issue of online predators has become a major Internet safety concern, particularly with the popularity of instant messaging. Kids leave their IM address (often, their login name) everywhere - in address books, on pieces of paper, on e-mails and on other computers they may use outside the home. Access to your child's IM address gives a predator or pedophile direct contact with your child. "Parents are still focused on chat, but the dangers are far greater with instant messaging," Aftab says. "It's the difference between their child being approached by a predator on a playground filled with children or alone on a quiet street."

The Justice Department bulletin reminds us that criminals now are also using modern technology, and that computers have made the predator's job easier. Technology has provided a new place, cyberspace, for pedophiles to target children and eliminated some of the risks they take in making person-to-person contact. Pedophiles and predators even share information with one another online about the various approaches they use to gain the trust of a child. Frighteningly, more and more kids are meeting strangers as a result of online "friendships" and in every reported case, have gone willingly to personally meet the predator.

CyberAngels assures parents that "even the most dangerous online predator hasn't yet mastered the technology to allow them to reach through the monitor and grab your children." Though emotionally damaging, predators only a physical threat if they meet a child offline. As parents, we can guard against this happening by talking to our children - over and over again. Talk at the dinner table, in the car and while they're online. Ask who they've been "talking" to online and if anyone they don't know has tried to talk with them. Aftab says that a clueless parent could be a child's biggest safety hazard. Filters and monitors have their merit, but we need to "arm our children with what they need to take out of the house with them," Aftab says.

Technology may have exposed our kids to a World Wide Web of problems, but it is also continually developing the tools to handle these problems. As our children grow and technology grows, we parents must learn to use these new tools, but not forget some of the oldest parenting tools in the book: listening and paying attention.