

unabridged version

Family Guide to
child safety
on the **internet**

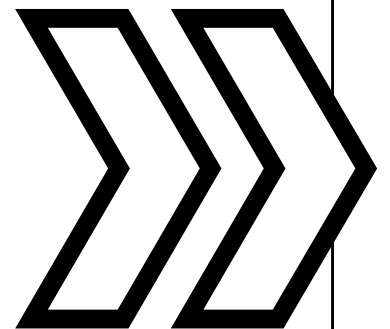
Brought to you by the Baltimore County community

Sponsored by:

The Baltimore County Public Schools

Baltimore County Public Library

Maryland Family Magazine



Dear Reader:

Our children are born digital natives. As they grow, they can access virtually any information they need from computers in their homes and schools, communicate instantly with anyone in the world from their cell phones and carry all their music on devices that fit in their hands. To educate and engage our children, the technology that is a part of their lives must also be a part of their learning experiences.

As described in our foundational document, the *Blueprint for Progress*, Baltimore County Public Schools embraces technology to enhance classroom teaching and learning, and prepare our students for higher education and careers. We are proud that state, national, and international organizations have honored our achievements in education technology.

This publication, *Family Guide to Child Safety on the Internet*, developed in partnership with Patuxent Publishing, is yet another step forward in our ongoing efforts to expand the safe and effective use of technology. In these pages, Baltimore County Public Schools staff, students, advocates, and partners share useful information and advice about ways that we can all work together to keep our children safe as they explore the technology that connects them to the world.

Just as keeping our classrooms safe is a primary responsibility of our school system, keeping our young people safe as they use technology is a primary responsibility for the entire community.

Sincerely,
Joe A. Hairston,
Superintendent

Table of Contents

Overview

Summary of the Internet's benefits and its potential hidden dangers to children 3

Parenting Online

Valuable information on safe online practices 5

Internet Safety Information

Online safety resources that parents can turn to for help in protecting their children 13

21st Century Learning Technology and Curriculum for Knowledge Workers

The Baltimore County Public School Department helps to guide students online 14

Helping Parents, Helping Kids

The Baltimore County Public Library helps children benefit from online resources 17

A Proactive Approach to Internet Security

How the Baltimore County Police Department is helping to protect children and tips on how to protect against identity theft 18

Students Share Their Internet Safety Thoughts

Three essay contest winners offer advice to fellow students and other students share their thoughts with excerpts from their essays 22

The Millennials: They're Confident, Pressured and Totally "Tech"

Understanding and protecting this new generation of savvy, high tech children 25

Parent On Board

One parent discusses ways to ensure children's online safety 27

Additional Resources 28

Overview

The world that we 30-somethings grew up in – with the birth of cable television, video games, and cassette tapes – must have been a frolic through the fields for our parents compared to how the parents of today must deal with emerging technologies. The day that the World Wide Web was spun was the day that would forever change the direction of how we communicate. Research papers once requiring a trek to the local library for information now would only take a matter of seconds to download facts from the convenience of one’s cozy home. Reaching out to a favorite relative across the country now could be accomplished with a few keystrokes and a send button. School documents for group projects now could be shared without the waste of our delicate paper resource.

A boundless source of benefits and convenience, the Internet is a vast information portal where access is granted 24 hours a day, 365 days a year. The Internet is considered a critical tool for children as it engages powerful interactive and intellectual qualities essential to their successful future. However, despite these great benefits, children who access the Internet are vulnerable to risks and hidden dangers that if not properly monitored, could have harmful, even sometimes fatal, effects.

This guide was established to educate parents on ways to make the best of the Internet’s benefits while protecting their children from these potential dangers.

The Internet opens the door to a world of endless possibilities for children. Our guide serves to educate parents on how vital it is to be aware of the potentially hazardous dangers of the Internet and how important it is to instill smart, safe online habits in their children. Through our guide, parents will learn how they can help their children get the most from their Internet use while remaining safe and unaffected by its hidden dangers. It also instructs parents on where they can go to get help for online safety issues such as: cyberbullying, online predators, child exploitation, and other potential dangers inherent within the Internet.

Critical Advice from Members of Your Community

Leaders in the fields of law enforcement, education, library systems, and telecommunications provide their expertise on where parents can go to get help, while a concerned parent and three inspiring students share their unique, personal perspectives.

WiredSafety.org, a web site created by Parry Aftab and dedicated to the safety and welfare of children online, is discussed and offers insight to parents on how children use technology. It also highlights safe practices to follow. The article offers valuable information for parents on how to monitor their children’s online activities, how to protect them against online abuse, and how to safeguard them against giving out personal information, especially when on popular interactive sites, such as myspace.com.

The **Internet Safety Guide** article will instruct parents on organizations they can turn to for help in keeping their children safe online. WiredSafety offers many access points of interest by **category** – parents, educators and librarians, law enforcement, woman’s issues, kids, tweens and teens or **hot topics** such as profiles, blogs, and social networks, cell phones, cyberdating, child pornography, scams and fraud, IM and SMS text messaging. **NetSmartz Workshop** is an interactive, educational safety resource from the National Center for Missing & Exploited Children® (NCMEC) and Boys & Girls Clubs of America (BGCA) for children aged 5 to 17, parents, guardians, educators, and law enforcement that uses age-appropriate, 3-D activities to teach children how to stay safer on the Internet.

The Baltimore County Library Information Services educates parents on the practices of online safety for children. They share how current telecommunications policies and instructional programs support the safe and ethical use of technology today.



Overview

The Baltimore County Public Library tells what the public library system is doing to support the use of technology and its safe use for students and their families.

The Baltimore County Police Department reveals how they are working to protect students from unsafe practices and offers safety tips and helpful resources parents can utilize if a violation occurs. We also have included information from the FBI about identity theft and what to do if you or your child becomes a victim.

Perry Hall Middle School shares three inspiring, candid essays written by students who were invited to give advice to incoming 6th grade students on the 'cool' uses of technology and how to use it safely. Other students also shared their thoughts by contributing excerpts from their essays.

A supervisor from the Library Information Services in Baltimore County Public Schools discusses the characteristics of our children's generation, otherwise known as the Millennials, and how through their very nature of being confident, trusting, and team oriented, they are open to technological vulnerabilities of which parents should be aware. He discusses how this generation uses technology and how parents can better become involved in their online habits.

A PTA member, proud parent of two children, and active Baltimore County Public School volunteer since 1995, reveals how she met the challenges of keeping her children safe while accessing the popular Web site, myspace.com. She discusses ways parents can ensure their children's safety while using technology in their home.

Recommended websites are offered to parents. These sites offer suggestions, advice and further resources to help guide parents about online safety. ■

Acknowledgements

Parry Aftab, Esq., Executive Director
WIRESAFETY

Della Curtis, Coordinator,
OFFICE OF LIBRARY INFORMATION SERVICES
BALTIMORE COUNTY PUBLIC SCHOOLS

Arthur Stritch, Supervisor,
LIBRARY INFORMATION SERVICES
BALTIMORE COUNTY PUBLIC SCHOOLS

Lieutenant Ralph Donahoe, Unit Commander of
Youth and Community Resources
BALTIMORE COUNTY POLICE DEPARTMENT

Joyce Caldwell, Library Media Specialist
PERRY HALL MIDDLE SCHOOL

Lynn Lockwood, Assistant Director
BALTIMORE COUNTY PUBLIC LIBRARY

Pam Moss, Project Manager
PATUXENT PUBLISHING COMPANY

Emiko Watanabe, Designer
PATUXENT PUBLISHING COMPANY

Dennise Cardona, Copywriter
PATUXENT PUBLISHING COMPANY

Parenting Online

by Parry Aftab, Esq.

What do we do when our eight-year-old knows more than we do about cyberspace? How do we guide our children safely through this new world? How do we set the rules when we don't even understand the risks? The childproof locks, seatbelts and helmets we use to help keep them safe in everyday life won't protect them in cyberspace. There we need new and different gadgets and safety tips.

Welcome to the new world of parenting online! It's your newest challenge. But don't worry...it's not as hard as you think and it's well worth the effort. Parenthood is never easy and the ground rules are always changing. We go from playing the role of confidante, to co-conspirator, to police chief, to teacher, to playmate and back...all in the same day. We barely have the chance to catch our breath!

The things we do to make sure our children stay safe are constantly changing too. When they crawl, we learn how to keep things off the floor. Then, when they pull themselves upright, we have to keep them safe from the new dangers at eye level. Training wheels have to be removed, and we have to watch while they pedal away (generally into the nearest tree). We watch their sugar intake, make sure they take their vitamins and keep small items out of their mouths.

That's our job, as parents. So the tried and true warnings, passed down from generation to generation, are repeated... "don't talk to strangers...", "come straight home from school...", "don't provoke fights...", "don't tell anyone personal information about yourself..." and "we need to meet your friends..." This is familiar territory after all. We know the dangers our kids face in the street or at the mall or in the school yard, because we faced them.

As in any large community, there are dangers our children encounter in cyberspace, too. But, since our children know more than we do about cyberspace, we worry about how we can teach them to avoid those dangers. Don't panic... those dangers can be managed using the same old warnings we've always used. We just need to translate them into cyberspace terms...

And there are wonders around every cyber-corner too...

The Internet is the largest collection of information in the world, always available without a charge and delivered to your home computer. Every question you might have can be answered online. When your child asks you how deep the ocean is or why the sky is blue, you can "ask the Internet," together.

You and your children can communicate with others too, worldwide and in every language, with the click of your mouse. Their artwork can be displayed, their news reporting published and their poems posted on the largest "refrigerator door" in the universe, where 700 million people can appreciate them.

You can research your family tree and build a family Web site. And, best of all...the most complicated homework assignment can be researched online (even last-minute on the Sunday night before it's due). You can search online for just about anything and any information you want. The easiest way to do that is by using search engines. You can type your search into one of the search engines and often will find what you are seeking. Just as often, though, you will find sites that are trying to get your or your children's attention. Pornographers are the most frequent abusers of search engines, registering and coding their sites to trick people into visiting them, thinking they are Disney, Pokemon or even the White House.

Most of the search engines now have filtering options. By selecting one of these options, most inappropriate content is filtered out and the search results are typically kid-friendly. Two commercial search engines were designed just for kids, though, and are wonderful places to begin your child's search online. Yahoo!igans!, Yahoo! kid-sized search engine hand-selects the sites, making sure nothing slips through. It is best for younger children, ten and under. Ask Jeeves for Kids is Ask Jeeves kid-sized search engine. Although not as scrubbed clean as Yahoo!igans! hand-selected sites, it contains many more sites which make it perfect for slightly older children. I recommend it for children ten and older.



Parenting Online

In addition, most full-size search engines have a filtered option you can select. But remember that even if you use a search engine filter, if the kids search for images, they can find things you wish they hadn't. That's when using a filtering product that can block images too might come in handy.

In addition to kid-sized search engines, there are many wonderful family-friendly site lists. WiredSafety has one of its own, where the sites are selected and reviewed by our specially-trained volunteers. You can even recommend your favorite sites to be added.

There are some entertaining sites that teach children online safety, as well. Although we prefer our www.WiredSafety.org, www.StopCyberbullying.org and www.InternetSuperHeroes.org the best, (she says modestly...) there are some very special ones we want to point out. Disney's www.Surfwelldisland.com teaches online safety Disney-style. Mickey Mouse, Donald Duck, Minnie Mouse and Goofy all find themselves involved in tropic island cyber-challenges relating to viruses, privacy, netiquette (cyber-etiquette) and responsible surfing. Lesson plans, online safety worksheets and other wonderful resources are all available without charge at the site.

Looking for homework help? Check out www.Discovery.com, www.Nationalgeographic.org, www.PBSkids.org and The National Gallery of Art kids' page www.nga.gov/kids/kids.htm. And ask your school librarian or the librarian at your public library for sites they recommend.

Librarians and library media specialists are the guides to valuable and safe online resources for children. And if you need something you can't find, send me an email at "Ask Parry," my Internet-syndicated online safety column. Drop by www.WiredSafety.org to find out how to submit a question.

CyberSense...translating common sense for cyberspace

Don't talk to or accept anything from strangers. That's the first one we learn while growing up, and the first one we teach our children. The problem in cyberspace though is teaching "stranger danger." Online, it's hard to spot the strangers. The people they chat with enter your home using your computer. Our kids feel safe with us seated nearby. Their "stranger" alerts aren't functioning in this setting. Unless they know them in real life, the person is a stranger no matter how long they have chatted online. Period. You need to remind them that these people are strangers, and that all of the standard stranger rules apply. You also must teach them that anyone can masquerade as anyone else online. The "12-year-old" girl they have been talking to may prove to be a forty-five year old man. It's easy for our children to spot an adult in a schoolyard, but not as easy to do the same in cyberspace.

Come straight home after school. Parents over the generations have always known that children can get into trouble when they wander around after school. Wandering aimlessly online isn't any different. Parents need to know their children are safe, and doing something productive, like homework. Allowing your children to spend unlimited time online, surfing aimlessly, is asking for trouble. Make sure there's a reason they're online. If they are just surfing randomly, set a time limit. You want them to come home after they're done, to human interaction and family activities (and homework).

Don't provoke fights. Trying to provoke someone in cyberspace is called "flaming." It often violates the "terms of service" of your online service provider and will certainly get a reaction from other people online. Flaming matches can be heated, long and extended battles, moving from a chat room or discussion group to email quickly. If your child feels that someone is flaming them, they should tell you and the sysop (system operator, pronounced sis-op) or moderator in charge right away and get offline or surf another area. They shouldn't try to defend themselves or get involved in retaliation. It's a battle they can never win.

Don't take candy from strangers. While we don't take candy from people online, we do often accept attachments. And just like the offline candy that might be laced with drugs or poisons, a seemingly innocent attachment can destroy your computer files, pose as you and destroy your friends or spy on you without your even knowing it. Use a good anti-virus, update it often and try one of the new spyware blockers. You can get a list of the ones we recommend at www.WiredSafety.org. Practice safe computing!



Parenting Online

Don't tell people personal things about yourself. You never really know who you're talking to online. And even if you think you know who you are talking to, there could be strangers lurking and reading your posts without letting you know that they are there. Don't let your children put personal information on profiles. It's like writing your personal diary on a billboard. With children especially, sharing personal information puts them at risk. Make sure your children understand what you consider personal information, and agree to keep it confidential online and everywhere else. Also teach them not to give away information at web sites, in order to register or enter a contest, unless they ask your permission first. And, before you give your permission, make sure you have read the web site's privacy policy, and that they have agreed to treat your personal information, and your child's, responsibly. We need to get to know your friends. Get to know their online friends, just as you would get to know their friends in everyday life. Talk to your children about where they go online, and who they talk to.

R-E-S-P-E-C-T. We all know the golden rule. We have a special one for cyberspace. Don't do anything online you wouldn't do offline. If you teach your child to respect others online and to follow the rules of netiquette they are less likely to be cyberbullied, become involved in online harassment or be hacked online. You can learn more about the ways to combat cyberbullying at our new website, www.StopCyberbullying.org or at www.WiredSafety.org's cyberstalking and harassment section. Remember that it is just as likely that your child is a cyberbully (sometimes by accident) as a victim of one. Let them know they can trust you not to make matters worse. You have to be the one they come to when bad things happen. Be worthy of that trust.

Remember that the new handheld and interactive gaming devices you buy have real risks too. Your children can send and receive text-messages from anyone on their cell phones or text-messaging devices and interactive games allow them to chat, on Internet phone, to anyone who wants to talk with them. The new Bluetooth devices let your child receive messages from anyone in a 300 foot range, and could be a problem if they play the new Bluetooth handheld games in a mall. Think about the features you are buying when you buy new devices for your children. Check into privacy and security settings. Our Teenangels (teenangels.org) are working on new guides for parents and other teens on what to look for and think about before you buy a new interactive device. Look for them at your local retailer or on the www.WiredSafety.org and www.Teenangels.org websites.

Don't just set up the computer in the corner of their bedroom, and leave them to surf alone. Take a look at their computer monitor every once in awhile, it keeps them honest. Sit at their side while they compute when you can. It will help you set rules that make sense for your child. It also gives you an unexpected benefit...you'll get a personal computing lesson from the most affordable computer expert you know! And it's worth the effort. When our children surf the Internet, they are learning skills that they will need for their future. They become explorers in cyberspace, where they explore ideas and discover new information. Also, because there is no race, gender or disability online, the Internet is the one place where our children can be judged by the quality of their ideas, rather than their physical attributes.

What Tech Tools Are Out There?

Blocking, filtering and monitoring...when you need a little help

There are many tools available to help parents control and monitor where their children surf online. Some even help regulate how much time a child spends playing computer games, or prevent their accessing the Internet during certain preset times.

I've listed the types of protections that are available. But, most of the popular brands now offer all of these features, so you don't have to choose. Recently, given parents' concerns about strangers communicating with their children online, monitoring software has gained in popularity. Although it might have its place in protecting a troubled child, it feels more like "spyware" than child protection. But it's ultimately your choice as a parent. The newest trend is to use products supplied by your ISP called parental controls. AOL's parental controls were the first of these to be developed and used. MSN 8.0 launched the first set of parental controls for MSN. To read more about the various products and services we have reviewed, visit WiredSafety.org.



Parenting Online

Blocking Software

Blocking software is software that uses a “bad site” list. It blocks access to sites on that list. They may also have a “good site” list, which prevents your child from accessing any site not on that list. Some of the software companies allow you to customize the lists, by adding or removing sites from the lists. I recommend you only consider software that allows you to customize the list, and lets you know which sites are on the lists.

Filtering

Filtering software uses certain keywords to block sites or sections of sites on-the-fly. Since there is no way any product can keep up with all of the sites online, this can help block all the sites which haven’t yet been reviewed. The software blocks sites containing these keywords, alone or in context with other keywords. Some companies allow you to select certain types of sites to block, such as those relating to sex, drugs or hate. This feature engages special lists of keywords that match that category. As with the “bad site” lists, the lists of keywords used by the filtering software should be customizable by the parent, and every parent should be able to see which terms are filtered.

Outgoing Filtering

No...this doesn’t mean your software had a sparkling personality :-) (that’s cyberspace talk for “grin” and means you’re supposed to smile at my brilliant humor, and if you want to learn more about this stuff...you need to read my Ms. Parry’s Guide to Correct Online Behavior). It means that your child won’t be able to share certain personal information with others online. Information such as your child’s name, address or telephone number can be programmed into the software, and every time they try to send it to someone online, it merely shows up as “XXXs.” Even with kids who know and follow your rules, this is a terrific feature, since sometimes even the most well-intentioned kids forget the rules.

Monitoring and Tracking

Some software allows parents to track where their children go online, how much time they spend online, how much time they spend on the computer (such as when they are playing games) and even allows parents to control what times of day their children can use the computer. This is particularly helpful when both parents are working outside of the home, or with working single-parents, who want to make sure their children aren’t spending all of their time on the computer. Many parents who don’t like the thought of filtering or blocking, especially with older children and teens, find monitoring and tracking satisfy their safety concerns. They can know, for sure, whether their children are following their rules. We particularly recommend using monitoring software and then forgetting it’s installed. Think of it as the security video camera in the corner of the bank. No one views the tapes until the bank is robbed. If something bad happens, you can play back the monitoring log and see exactly what occurred, and who said what, and in dire situations, where your child went to meet an adult offline. We particularly like www.Spectorsoft.com, because their products can monitor all instant messaging platforms, which is key to keeping your children safe online. Parents have to remember, though, that these tools are not cyber-babysitters. They are just another safety tool, like a seat belt or child safety caps. They are not a substitute for good parenting. You have to teach your children to be aware and careful in cyberspace. Even if you use every technology protection available, unless your children know what to expect and how to react when they run into something undesirable online, they are at risk. Arming them well means teaching them well.

Your Online Safety “Cheatsheet”

Some Basic Rules for You to Remember as a Parent . . .

- Make sure your child doesn’t spend all of his/her time on the computer. People, not computers, should be their best friends and companions.
- Keep the computer in a family room, kitchen or living room, not in your child’s bedroom. Remember that this tip isn’t very helpful when your children have handheld and mobile Internet and text-messaging devices. You can’t make them keep their cell phones in a central location. So make sure that the “filter between their ears” is working at all times.
- Learn enough about computers so you can enjoy them together with your kids.



Parenting Online

- Teach them never to meet an online friend offline unless you are with them.
- Watch your children when they're online and see where they go.
- Make sure that your children feel comfortable coming to you with questions and don't over react if things go wrong.
- Keep kids out of chat rooms or IRC unless they are monitored.
- Encourage discussions between you and your child about what they enjoy online.
- Discuss these rules, get your children to agree to adhere to them, and post them near the computer as a reminder.
- Find out what email and instant messaging accounts they have and (while agreeing not to spy on them) ask them for their passwords for those accounts.
- "Google" your children (and yourself) often and set alerts for your child's contact information. The alerts will e-mail you when any of the searched terms are spotted online. It's an early warning system for cyberbullying posts, and can help you spot ways in which your child's personal information may be exposed to strangers online. To learn how to "Google" them, visit www.InternetSuperHeroes.org.
- Teach them what information they can share with others online and what they can't (like telephone numbers, address, their full name, cell numbers and school).
- Check your children's profiles, blogs and any social-networking posts. Social-networking websites include www.xanga.com, www.livejournal.com, www.facebook.com and www.buddyprofile.com. They shouldn't be used by preteens and should be only carefully used by teens.
- Get to know their "online friends" just as you get to know all of their other friends.
- Warn them that people may not be what they seem to be and that people they chat with are not their friends, they are just people they chat with.
- If they insist on meeting their online friend in real life, consider going with them. When they think they have found their soul mate, it is unlikely that your telling them "no" will make a difference. Offering to go with them keeps them safe.

Once you understand enough about cyberspace and how your children surf the Internet, you can set your own rules. These are the basic rules, even though you may want to add some of your own. Some kids like setting the rules out clearly in an agreement. Here's one you can use, and post near your computer to help them remember how to surf safely.

- I want to use our computer and the Internet.
- I know that there are certain rules about what I should do online.
- I agree to follow these rules and my parents agree to help me follow these rules:
 - I will not give my name, address, telephone number, school, or my parents' names, address, or telephone number to anyone I meet on the computer.
 - I understand that some people online pretend to be someone else. Sometimes they pretend to be kids, when they're really grown ups. I will tell my parents about people I meet online. I will also tell my parents before I answer any emails I get from or send emails to new people I meet online.
 - I will not buy or order anything online without asking my parents or give out any credit card information.
 - I will not fill out any form online that asks me for any information about myself or my family without asking my parents first.
 - I will not get into arguments or fights online. If someone tries to start an argument or fight with me, I won't answer him or her and will tell my parents.



Parenting Online

- If I see something I do not like or that I know my parents don't want me to see, I will click on the "back" button or log off.
- If I see people doing things or saying things to other kids online I know they're not supposed to do or say, I'll tell my parents.
- I won't keep online secrets from my parents.
- If someone sends me any pictures or any emails using bad language, I will tell my parents.
- If someone asks me to do something I am not supposed to do, I will tell my parents.
- I will not call anyone I met online, in person, unless my parents say it's okay.
- I will never meet in person anyone I met online, unless my parents say it's okay.
- I will never send anything to anyone I met online, unless my parents say it's okay.
- If anyone I met online sends me anything, I will tell my parents.
- I will not use something I found online and pretend it's mine.
- I won't say bad things about people online, and I will practice good netiquette.
- I won't use bad language online.
- I know that my parents want to make sure I'm safe online, and I will listen to them when they ask me not to do something.
- I will help teach my parents more about computers and the Internet.
- I will practice safe computing, and check for viruses whenever I borrow a disk from someone or download something from the Internet.
- I won't post my cell number on my away message, and will check with someone before posting something personal about me on my blog or on a networking site.
- I will Stop, Block and Tell! if I am harassed online or cyberbullied.
- I will Take 5! before reacting to something that upsets me or makes me angry online.
- I will practice responsible "thinkB4Uclick" rules. (I know I can find out more about these things at www.InternetSuperHeroes.org and www.StopCyberbullying.org.)
- I will learn how to be a good cybercitizen and control the technology, instead of being controlled by it.

I promise to follow these rules (signed by the child).

I promise to help my child follow these rules and not to over react if my child tells me about bad things in cyberspace (signed by parent).

From Parry:

I am asked questions about kids' online safety at least a hundred times a day. Is the Internet a dangerous place? Are there predators out there looking to set up a meeting with my child? How can we find good and reliable content online? How can I supervise my child's surfing when I can't even turn on the computer? These and many other questions like these fill my inbox daily. If you have a question of your own, visit www.WiredSafety.org and click on "Ask Parry."

Here is the one simple answer: The single greatest risk our children face in connection with the Internet is being denied access. We have solutions for every other risk. That bears repeating, over and over, especially when we



Parenting Online

hear about Internet sexual predators, hate, sex and violence online. But our children need the Internet for their education, careers and their future. Happily, most of the risks are easily confined. In each and every case when children encounter Internet sexual predators offline, they go willing to the meeting. They may think the person is a cute fourteen year old girl or boy, but they know they are meeting someone they don't know in real life. That means we can prevent 100% of these crimes. Merely teach our children not to meet Internet strangers offline. If they are set on meeting that person anyway, go with them. That way, if the person turns out to be a cute fourteen year old, you are the hero. And if they aren't, you're an even *bigger* hero.

Our WiredKids, WiredTeens and Teenangels programs, in addition to being fun and educational sites, are also volunteer programs where children and teens are taught online safety and privacy and responsible surfing. They then use these skills to help other children and teens learn to surf safely, as well. Talk to your children about what they do online (and offline also), and let them know you are there to help if things go wrong. You will note that in our safe surfing agreement parents have to promise only one thing...not to overreact if their children come to them for help. Earn their trust, and be worthy of it. Register your children at www.WiredSafety.org, our children's online safety site, and we will make sure they learn what they need to know about enjoying the Internet safely and privately. It's not about technology at all...it's about communication and good parenting. Remember, we're all in this together!

Parry Aftab, Esq., Executive Director

WiredSafety and its family of sites and programs, including www.WiredSafety.org and www.CyberLawEnforcement.org

WiredSafety is a 501c-3 non-profit organizations formed under the laws of the State of New York.

This publication is copyrighted to Parry Aftab, Esq. All rights reserved. For permission to duplicate this publication, contact parry@aftab.com.

Parenting Wireless

You've already heard the tips about keeping your kids safe online. But, now...all bets are off. Welcome to the wonderful new world of wireless! Our families can carry powerful computing in handheld devices the size of a pack of playing cards (or smaller!). They can download and play music, movies, and games. They can shoot, store and share photos, video and audio. They are always in touch, always connected, and always engaged. (And the newest hottest teen social network, Yfly.com, is using broadcast text-messaging to keep teens connected to their nearest and dearest friends through their mobile devices and MySpace and Facebook are using text-to-profile posting technologies now too.)

Great! Except the most often repeated safety tip warns parents to keep the computer in a central location to keep an eye on what's going on. So, how are we supposed to keep our kids safe when they are carrying access and communication devices in the palms of their little hands? Are we supposed to tell them to keep their cell phone or other handheld device in a central location? Of course not. At this point, it's less about standing over their shoulders and more about improving the "filter between their ears."

You can do this by being proactive and informed (not rocket scientists, just informed...). Luckily, it all comes down to 3 key issues. I call these the "3C's" – Communication, Content, and Commercialism. Every digital device or interactive service involves at least one of them, some involve all 3. Once you find the Cs involved, spotting the risks and solutions is easy.

Start by reviewing all your interactive technology devices and services. If you are shopping for a new device or service, ask the salesperson these questions before plunking down your hard-earned money.

Communication: Does this device or service allow you to communicate with others? Does it allow others to communicate with you? If so, how? What controls exist to block, filter or monitor these communications? How can I implement them? (Text-messaging and voice capabilities fall into the first "C." So do email, interactive features on profiles and on blogs.)

Content: What content or images can be accessed or shared using the device or service? Can you surf the Web,



Parenting Online

access blog or profile sites, post your blog or profile sites or download media? Can you store images, personal information, video, songs, etc.? What controls exist to rate, block, filter or monitor the content? How can I implement them? (Music and video downloads, pictures taken by the mobile device, adult content, content on profiles and on blogs fall into this second “C.”)

Commercialism: Can this device/service cost me money? If so, how much? Are there ways to spend money or buy things using the device/service? Are there ways to control costs or prevent my kids from spending money or buying things without my approval? What controls exist to block, filter or monitor these costs or spending ability? How can I implement them? (Ring tones, music downloads, text-messaging and games fall into this third “C.”)

Next, you need to refer to the common sense tips our grandmothers taught our parents and they taught us – we just need to translate them from “Grandma-speak” to “cyberspeak.”

- **Don’t talk to strangers.** It’s easy for our children to spot an adult in a schoolyard, but not as easy to do the same in cyberspace, or on text-messaging. Our kids need to learn that unless they know the people in real life (“RL”), the person has to be treated like a stranger no matter how long they have chatted online. Period.
- **Come straight home after school.** When kids wander around, unsupervised, after school they inevitably get into trouble. Allowing your children to spend unlimited time surfing or texting aimlessly is no different. Set a time limit. Create a “no texting” zone, where they spend time with their real life friends and engaging in family activities (and homework).
- **Don’t steal.** Illegal music, movie and game downloads. Enough said!
- **Don’t start fights.** Cyberbullying is when one minor uses interactive technology to harass, frighten or humiliate another minor. They may even spread into RL. Our children should be taught to Stop (don’t do anything to make matters worse), Block (the offender) and Tell (you or another trusted adult). (You can learn more about this at www.stopcyberbullying.org.)
- **Don’t take candy from strangers.** While we don’t take candy from people online, we do often accept attachments. A seemingly innocent attachment can contain a virus, spyware or a hacking tool. Many of the good anti-virus programs have mobile versions. They are worth the investment.
- **Don’t share personal information with others.** Our children often post their cell number on their instant messaging “away page.” Mobile device cameras can be used to take a picture and post it online. Make sure your children understand what can and cannot be shared. Remember...The more information you give your children, the less information they’ll give a stranger.
- **Look before they leap.** Check things out before your child starts using a new interactive device or technology or activity. Let them know what features you don’t want them using and which ones are safe. And remind them that you will be watching. This is a matter of parental choice and control. The wireless industry is providing some significant help here too. They have voluntarily adopted a set of principles relating to mobile content provided by the carriers themselves, rating them as “restricted” (for those over the age of 18). Restricted content is only available with authentication, allowing parents stay in control. Disney has a new cell phone service and phones launching in June, 2006 too. (Visit www.disneymobile.com and www.ctia.org for more information.)
- **Do unto others as you would have them do unto you.** It is too easy for our children to act out online knowing that they may never have to face the other person in real life. Not having to look them in the eyes makes it easier to be rude, lewd or hostile. This is a good time to remind your children to treat others online and off with R-E-S-P-E-C-T.

Now...go have some fun and play a little! And if you are still tech-challenged, ask your kids for help.

And for more cybersafety tips and help or to book a program for your community, visit www.WiredSafety.org, the world’s largest Internet and wireless safety and help group or contact Parry Aftab directly at parry@wiredsafety.org. ■

Internet Safety Information

By Della Curtis

WiredSafety

www.wiredsafety.org

WiredSafety is directed by Parry Aftab (also a volunteer), a mom, international cyberspace privacy and security lawyer and children's advocate. Parry is the author of *The Parent's Guide to Protecting Your Children in Cyberspace* (McGraw-Hill), which has been adapted and translated around the world. WiredSafety is a 501c3 program and the largest online safety, education and help group in the world. It is a cyber-neighborhood watch that operates worldwide in cyberspace through more than 9,000 volunteers worldwide (WiredSafety is run entirely by volunteers). Their work falls into four major areas:

- Help for online victims of cybercrime and harassment
- Assisting law enforcement worldwide on preventing and investigating cybercrimes
- Education
- Providing information on all aspects of online safety, privacy and security

WiredSafety offers many access points of interest by category – parents, educators and librarians, law enforcement, woman's issues, kids, tweens and teens or hot topics such as profiles, blogs, and social networks, cell phones, cyberdating, child pornography, scams and fraud, IM and SMS text messaging. WiredSafety is the place to get help. It provides links to reporting cybercrime, live help, interactive forum, and the *Ask Parry* service. Also, check out other special areas of Wired Safety such as WiredKids, Cyber Law Enforcement, Stop Cyberbullying, and Internet Super Heroes.

NetSmartz Workshop

www.netsmartz.org

NetSmartz is an interactive, educational safety resource from the National Center for Missing & Exploited Children® (NCMEC) and Boys & Girls Clubs of America (BGCA) for children aged 5 to 17, parents, guardians, educators, and law enforcement that uses age-appropriate, 3-D activities to teach children how to stay safer on the Internet.

FBI Innocent Images National Initiative

www.fbi.gov/publications/innocent.htm

The Innocent Images National Initiative (IINI), a component of FBI's Cyber Crimes Program, is an intelligence driven, proactive, multi-agency investigative operation to combat the proliferation of child pornography/child sexual exploitation (CP/CSE) facilitated by an online computer. The IINI provides centralized coordination and analysis of case information that by its very nature is national and international in scope, requiring unprecedented coordination with state, local, and international governments, and among FBI field offices and Legal Attachés.

Online Lingo (Acronyms)

www.missingkids.com/adccouncil/lingo.html

The Center for Missing and Exploited Children – CyberTipline provides an up-to-date listing of acronyms commonly used by kids in Instant Messenger (IM) and chatrooms. Also, take an Internet safety quiz for adults or kids.

CyberTipline (National Center for Missing and Exploited Children)

www.cybertipline.com

This organization is responsible for handling leads from individuals reporting the sexual exploitation of children. A convenient link to report an online predator is provided as well as excellent information on how to protect your child, statistics, and reports. ■

21st Century Learning Technology and Curriculum for Knowledge Workers

By Della Curtis
Baltimore County Public Schools

Technology is becoming increasingly prevalent in our everyday lives as well as the workforce. Recent studies predict that by the year 2010 almost every job in the American workplace will require some use of technology. Our schools mirror this trend. Our challenge is to prepare students to use technology as a tool for problem solving in the information age where our students must learn to make choices between the information goldmines or landfills, ethical or unethical use of intellectual property, and privacy of personal information or broadcasting to worldwide populations.

Choice #1: Information Goldmine or Landfill

The 2003 study from the University of California at Berkley School of Information Management and Science provides some startling statistics. The exponential growth of information is at a rate of 5 exabytes per year. Let's use the Library of Congress as a framework to understand the scope of this statistic. The Library of Congress houses 17 million books. 5 exabytes would translate to 37,000 new Library of Congress collections. The rate of digital content produced via the Internet is a similar story. The World Wide Web (WWW) is 17 times the size of the Library of Congress, with a growth rate of 30% per year. The study concludes that the knowledge base doubles every 7 years. This information explosion trend will continue, thus making it increasingly important for all to make wise choices regarding the validity of information, effective search strategies to locate needed information, and how to manage "information overload."

Choice #2: Ethical or Unethical Use of Intellectual Property

Access to vast amounts of "free" information from around the globe may be misinterpreted as authorization to use all or any part of another's intellectual property for one's own purposes. Technological tools make it easy to copy/paste as opposed to "deep reading" for understanding and synthesizing to communicate new knowledge. The copy/paste behavior is the antithesis of knowledge-worker behaviors. Further exasperating the temptation is the availability of sources where students can download a complete term paper on any topic needed. A Google search ("free term papers") on 3/31/06 provided web links to 346,000 choices.

Choice #3: Privacy of Personal Information or Broadcasting to a Global Audience

Because Millennials are trusting by nature, freely share information using their technological devices, and know that adults will protect them unconditionally with rules, laws, and policies in their physical world, they are confident that their virtual world is the same. Giving out personal information such a name, age, sex, address, phone number, likes and dislikes, photos, etc. is done with little reservation knowing there will be no consequences. After all, *I am anonymous in my virtual space, I can be whomever I want to be – real or not real – and I'm in my house and safe in my room.*

Meeting the Shared Challenge

Our challenge is to prepare our students to become effective information consumers and producers of information who will make ethical, responsible, and safe choices. This requires more than learning to operate a computer, but how to use it as a tool for problem solving – learning to be a knowledge worker who uses cognitive skills for lifelong learning, productivity, and achievement in this information-based global economy.



21st Century Learning Technology and Curriculum for Knowledge Workers

Leadership with Vision

Dr. Hairston, Superintendent of Baltimore County Public Schools, who received the 2006 Technology Administrator of the Year Award, clearly has the vision for technology in Baltimore County Public Schools. The BCPS *Blueprint for Progress* mirrors the conditions essential to a knowledge-worker learning environment. These are:

- Integrate technology in the teaching and learning process
- Provide teachers with professional development opportunities for using and integrating technology into curriculum and instruction
- Provide opportunities for all students so they will acquire and apply information through the use of educational media, including technology and media centers
- Identify and consistently implement a common core of research-based instructional practices resulting in more purposeful and engaging work for students

Technology Standards

There are essential conditions required to create a knowledge-worker learning environment in our schools. According to the International Society for Technology in Education, these conditions are:

- Educators skilled in the use of technology for learning
- Content standards and technology integrated curriculum
- Student-centered approaches to problem-based learning
- Instruction in ethical and safe use of information networks
- Access to contemporary technologies, software, and telecommunications networks
- Vision with support and proactive leadership

Problem Solving Framework

Along the great strides in creating technologically equipped schools, it is important that students are equipped with a problem-solving model. The model provides a framework to help them learn the process each step of the way – to effectively search for information, to read critically, to question information authenticity, to organize and produce new information, and to document information sources. The BCPS *Information Literacy Process Model* is more than a framework of what should be done. It is a tool to support teachers, students, and families in teaching essential 21st century skills. www.bcps.org/offices/lis/models/tips/index.html

Online Research Models

The framework is just the beginning. It, like technology, must be integrated into teaching and learning, thus the BCPS Online Research Models that are collaboratively designed by teams of library media specialists and teachers during summer curriculum workshops for the past 7 years. In 1999, the Maryland Business Roundtable recognized these Online Research Models as one of the best practices in technology integration in Maryland.

See models for each level at the following URLs:

- Elementary School: www.bcps.org/offices/lis/models/elem.html
- Middle School: www.bcps.org/offices/lis/models/middle.html
- High School: www.bcps.org/offices/lis/models/highcore.html

The onLINE Website

In 1991, the Office of Library Information Services designed the first BCPS website to connect educators, students, and their families to evaluated Internet resources that directly support the teaching and learning of BCPS Essential Curriculum. With the revision of Maryland learning standards...the *Voluntary State Curriculum* ...another first leap to serve the same purpose was completed in July 2005. Not only does this source link to authoritative text-based Internet resources, but also to the newer digital content of “learning objects,” multimedia, simulations, and tutorials. www.bcps.org/offices/lis



21st Century Learning Technology and Curriculum for Knowledge Workers

MDK-12 Digital Library

The Enhancing Education Through Technology Grant provides ALL Maryland students 24/7 access to a core of “quality” digital content such as full text magazines, newspapers, multimedia, videos, and evaluated websites. Additional digital content accessible 24/7 to BCPS students, families, and teachers is funded by BCPS. These resources include *e-Science Reference Books*, *Historical Newspapers*, *Literature Resource Center*, *World Book*, and *BrainPop*. www.bcps.org/offices/lis/feebased/index.html

Telecommunications Policy

The BCPS policy outlines a code of behavior for knowledge-worker students to practice safe, ethical, and responsible use of telecommunications. The *Acceptable Use for Students* is included in the BCPS Student Handbook that is annually sent home to all families for their review and signature. See policy 6166P and rule 6166R - *Telecommunications Access to Electronic Information, Services, and Networks* at www.bcps.org/system/policies_rules/6000toc.htm

Below is a summary of the expectations the school system has for all students who use telecommunications:

STUDENTS SHALL:

- Use telecommunications for educational purposes
- Communicate with others in a courteous and respectful manner
- Maintain the privacy of personal name, phone number, password(s), and respect the privacy of others
- Use only telecommunications accounts and passwords provided by the school
- Report any incident of harassment to the supervising employee
- Agree to the review of communications, data, and files by the Baltimore County Public Schools
- Comply with copyright laws and intellectual property rights of others

STUDENTS SHALL NOT:

- Knowingly enter unauthorized computer networks or software to tamper or destroy data
- Bypass the school system’s filtering server
- Access or distribute abusive, harassing, libelous, obscene, offensive, profane, pornographic, threatening, sexually explicit, or illegal material
- Install personal software on computers
- Use telecommunications for commercial, purchasing, or illegal purposes
- Use telecommunications in any other manner that would violate School Board disciplinary policies

www.bcps.org/system/policies_rules/forms_exhibits/6000Series/FORM6166-A.pdf

Our shared challenge is to prepare all students to be productive, successful, responsible, and contributing citizens in a global-based economy. The *Blueprint for Progress*, the written master plan for Baltimore County Public Schools, sets forth the vision and strategies to build curriculum and technological capacity for a 21st century knowledge worker global economy. The information goldmines or landfills, ethical or unethical use of intellectual property, and privacy of personal information or broadcasting to a global audience – all choices – will be easier through education at home, school, and the community. ■

Helping Parents, Helping Kids

The Baltimore County Public Library

The Baltimore County Public Library with 17 branches throughout the county has always been a quality resource for parents and kids alike. In 2005, BCPL was again rated one of the top five large library systems in the country for its customer service and efficiency. Whether providing parents with programs or information to assist in preparing their children for school, or providing kids the resources to complete their schoolwork or expand their horizons, your local library is ready to help.

Public computers

All of BCPL's branches have computer terminals available for public use and many branches offer courses on basic Internet and database usage. Please check our quarterly Calendar of Events for specific branch classes and schedules. Our computers are situated to be highly visible and close to library information desks. Staff routinely circulates in the area to answer questions and provide guidance on doing research and exploring resources. While we take care to use computer filters and try to monitor individual usage to help protect children from inappropriate material, the ultimate responsibility for monitoring children's use of the Internet rests with parents or caregivers. If you have any questions or concerns about your child's use of our computers, please contact your local branch manager.

Online resources

BCPL's motto is "Where you find it" and this is especially appropriate concerning the needs of young students. We offer online librarian support through the AskUsNow reference service, giving students the ability to communicate with an actual librarian through live online chat sessions 24 hours a day seven days a week. AskUsNow can help students with questions, research guidance and navigating the Internet. The library's Kids Catalog of available materials is easily accessed by young readers as they look for their next great reading adventure.

We have developed a Kids Page on our Web site (www.bcpl.info) with specific information areas to find materials related to homework assignments or just to browse in pursuit of hobbies or interests. Children can find reading ideas by subject area or author, games, and other activities that will all challenge their minds and broaden their reading skills. Included on the Kids Page is a Parents Corner with helpful advice on exploring the Internet with your child and preparing your young ones for entering school.

BCPL subscribes to many databases, including some that are ideal resources for young students and can be accessed free of charge in your local branch or remotely from home or school. The Kids Page includes a section called Got Homework? with links to the World Book Encyclopedia Online, the Merriam-Webster Online Dictionary and the Discovery Channel's online resource www.DiscoverySchool.com. Other databases include Kids Search and Searchasaurus for elementary and middle school students.

Your local librarian would be happy to help you find the right online resource for your needs or those of your children.

Reading programs

BCPL is a strong proponent of preparing young children for school and fostering the growth of their reading and comprehension skills beginning at a very early age. The better they are able to read, the better they will be able to make use of online resources for their education and personal enrichment. Therefore we regularly present programs for kids and parents/caregivers aimed at developing and improving these critical skills all year long, not just during the school year.

Our Summer Reading Club program encourages children and teens to continue their classroom reading activities by using a fun theme and offering small prizes when they complete reading tasks. With mascot Sneaks the Cat leading the way, children have fun reading while maintaining their reading skills between school sessions. Parents/caregivers of babies and toddlers can participate in the program by reading to them which familiarizes preschoolers with books and reading activities. We work in conjunction with the Baltimore County public schools and area private schools to make sure students are recognized for their reading achievements during summer break, creating another incentive to read year round.

The Baltimore County Public Library has a long history of providing quality materials and information to customers of all ages, including through the use of the Internet and other online resources. This tradition is especially important for the development of literacy skills and a love of reading in our children. By our giving them the tools and appreciation of reading, they can benefit from the vast information resources that will foster their lifelong learning and personal growth. ■

A Proactive Approach to Internet Safety

Baltimore County Police Department

The Baltimore County Police Department takes online safety very seriously, especially when it comes to children. They suggest that taking a proactive approach is perhaps the single best tactic to protecting a child's safety. There are many steps parents can take to ensure that their children safely enjoy the endless benefits of the Internet.

Lieutenant Ralph Donahoe, Unit Commander of the Baltimore County Police Department's Youth and Community Resources Section, points out that the Baltimore County Police offers presentations on Internet safety. The Police Athletic League (PAL), created to provide a safe and structured environment for the youth throughout Baltimore County and provide an opportunity for these young people to interact with police officers in a positive setting that offers an outlet for educational and athletic programs, holds Internet safety talks with their youth members. Lt. Donahoe further adds, "It's really the parents' responsibility to be a parent. He urges parents to "monitor their children's online activity and to take an active role in their lives." When a problem does arise, he says, "We urge parents to call 911 so that we can take an initial report and, when substantiated, investigate the case even further."

Online Safety Tips from the FBI

The FBI advises parents to take the following precautions when their children go online:

- Have children show you their favorite online destinations
- Keep your computer in a common area of the house, not in children's bedrooms
- Use your local service provider's parental controls and/or blocking software
- Maintain access to children's online accounts and randomly check their email
- Instruct children to never arrange a face-to-face meeting with someone they met online, to never upload pictures of themselves to the Internet, to never give out identifying information, and to never download pictures from an unknown source

Identity Theft & Steps a Child Can Take to Avoid Being a Victim

All someone needs is your children's name, address, birth date, or social security number to steal their identity. The best line of defense against this devastating crime is awareness. If you or your child becomes a victim, law enforcement officials suggest that you contact the Federal Trade Commission (FTC), which is the federal clearinghouse for complaints by victims of Identity Theft, at: 1-877-IDTHEFT.

Turn to the National Center for Missing and Exploited Children for Guidance.

The National Center for Missing & Exploited Children® (NCMEC) and Boys & Girls Clubs of America (BGCA) have created The NetSmartz Workshop, an interactive, educational safety resource to teach kids and teens how to be safe on the Internet. NetSmartz combines the newest technologies available and the most current information to create high-impact educational activities that are well received by even the most tech-savvy kids. Visit them at: www.netsmartz.org or visit the NCMEC website for more online safety information at: www.missingkids.com.



A Proactive Approach to Internet Safety

Identity Theft: A Quick Reference Guide

What is Identity Theft?

Identity theft involves acquiring key pieces of someone's identifying information, such as name, address, date of birth, social security number and information enabling the identity thief to commit numerous forms of fraud which include, but are not limited to, taking over the victim's financial accounts, opening new bank accounts, purchasing automobiles, applying for loans, credit cards and social security benefits, renting apartments, and establishing services with utility and phone companies.

What to do if you become a victim:

- Set up a folder to keep a detailed history of this crime.
- Keep a log of any contacts you make and make copies of all documents.
- Contact all creditors, by phone and in writing to inform them of the problems.
- Notify the US Postal Inspector if your mail has been stolen or tampered with:
US Postal Inspection Service (410-715-7700)
US Postal Inspection Service-Local Post Office (See listing under Federal Government.)
www.usps.gov/websites/depart/inspect
- Contact the Federal Trade Commission to report the problem. www.consumer.gov/idtheft – The FTC is the federal clearinghouse for complaints by victims of identity theft. The FTC helps victims by providing information to help resolve financial and other problems that could result from identity theft. Their hotline telephone number is 1-877-IDTHEFT (1-877-438-4338).

Sample "Courtesy Notice:"

(Date)

Dear (Creditor Name/Collection Agency Names):

On (Date), I received your letter demanding payment of (\$\$amount). I did not open this account and incur this unpaid balance. Someone, other than myself, wrongfully used my personal information to obtain a line of credit/service. Your company extended a line of credit/services to someone, other than myself. Your company is a victim and should file a police report in the appropriate jurisdiction.

You are hereby notified that on (Date), I filed an identity theft report with the Baltimore County Police Department. The case # is (_____), a copy of which can be obtained by contacting the Baltimore County Police Central Records Unit at 410-887-2215

Closing,

(Your Name and address)

- Call each of the three credit bureaus' fraud units to report the identity theft. Ask to have a "Fraud Alert/Victim Impact" statement placed in your credit file asking that creditors call you before opening any new account.
- Request that a copy of your credit report be sent to you.

Credit Bureaus:

EQUIFAX

www.equifax.com

PO Box 740241

Atlanta, Georgia 30374

To order report, 1-800-525-6285

To report Fraud, 1-888-766-0008

EXPERIAN

www.experian.com

601 Experian Parkway

Allen, Texas 75013

To order report, 1-888-397-3742

To report Fraud, 1-888-397-3742

TRANS UNION

www.transunion.com

PO Box 390

Springfield, PA 19064

To order report, 1-800-888-4213

To report fraud, 1-800-680-7289



A Proactive Approach to Internet Safety

- Alert your banks to flag your account and contact you to confirm any unusual activity.
- Request a change of PIN and a new password.
- If you have any checks stolen or bank accounts set up fraudulently, report it to the following companies:
 - National Check Fraud Service: 1-843-571-2143
 - CheckRite: 1-800-766-2748
 - SCAN: 1-800-262-7771
 - CrossCheck: 707-586-0551
 - TeleCheck: 1-800-710-9898 or 1-800-927-0188
 - International Check Services: 1-800-526-5380
- Contact the Social Security Administration's Fraud Hotline at 1-800-269-0271.
- Contact the state office of the Department of Motor Vehicles to see if another license was issued in your name. If so, request a new license number and fill out the DMV complaint form to begin the fraud investigation process.
- Obtain description of suspect (if known).
- Obtain witness information.
- What is the financial loss to you? Attach all supporting documentation.

Preventive Actions

- Promptly remove mail from your mailbox after delivery.
- Deposit outgoing mail in post office collection mailboxes or at your local post office. Do not leave in unsecured mail receptacles.
- Never give personal information over the telephone, such as your social security number, date of birth, mother's maiden name, credit card number, or PIN code, unless you initiated the phone call. Protect this information and release it only when absolutely necessary.
- Shred pre-approved credit applications, credit card receipts, bills and other financial information you don't want before discarding them in the trash or recycling bin.
- Empty your wallet of extra cards and IDs, or better yet, cancel the ones you do not use and maintain a list of the ones you do.
- Order your credit report from the three credit bureaus once a year to check for fraudulent activity or other discrepancies. (Maryland Law allows you to get one free copy a year from each credit bureau.)
- Never leave receipts at bank machines, bank counters, trash receptacles, or unattended gasoline pumps. Keep track of all your paper work. When you no longer need it, destroy it.
- Memorize your social security number and all of your passwords. Do not record them on any cards or on anything in your wallet or purse.
- Sign all credit cards upon receipt.
- Save all credit card receipts and match them against your monthly bills.
- Be conscious of normal receipt of routine financial statements. Contact the sender if they are not received in the mail.
- Notify your credit card companies and financial institution in advance of any change of address or phone number.
- Never loan your credit cards to anyone else.
- Never put your credit card or any other financial account number on a post card or on the outside of an envelope.
- If you applied for a new credit card and it hasn't arrived in a timely manner, call the bank or credit card company involved.
- Report all lost or stolen credit cards immediately.
- Closely monitor expiration dates on your credit cards. Contact the credit card issuer if replacement cards are not received prior to the expiration date.
- Beware of mail or telephone solicitations disguised as promotions offering instant prizes or awards designed solely to obtain your personal information or credit card numbers.
- Balance your checkbook on a monthly basis for possible fraudulent charges on your debit card number. The bank limits the time period in which complaints can be filed and you are reimbursed for fraudulent charges.



A Proactive Approach to Internet Safety

INFORMATIONAL WEBSITES

Federal Trade Commission
www.ftc.gov

State of Maryland
Office of the Attorney General
Consumer Protection Division
www.oag.state.md.us/consumer

Privacy Rights Clearing House
www.privacyrights.org

U.S. Government Account Office
www.gao.gov

U.S. Postal Inspection Service
www.usps.gov/postalinspectors

International Association of Financial
Crimes Investigators
www.iafci.org (go to links section)

Internet Fraud Complaint Center
www.ic3.gov

Internet and On-Line Services

Use caution when disclosing checking account numbers, credit card numbers or other personal financial data at any Website or on-line service location unless you receive a secured authentication key from your provider.

When you subscribe to an on-line service, you may be asked to give credit card information. When you enter any interactive service site, beware of con artists who may ask you to “confirm” your enrollment service by disclosing passwords or the credit card account number used to subscribe. Don’t give them out!

Your BcoPD Case Number is _____

Make note of this case number in your detailed history folder and reference it when you have contact with any business or law enforcement agency concerning this report.

If the crime occurred in our jurisdiction and there are workable leads, such as witnesses and suspect information, an investigator will be assigned to the case. Unfortunately, not all cases will be assigned to an investigator because there are no significant leads to identify the suspect.

For more information on Identity Theft contact:
Baltimore County Police Department
Economic Crimes Team
700 East Joppa Road
Towson, Maryland 21286
410-887-2190

CR 8-301(b)-Personal Identifying Information

b. A person may not knowingly, willfully, and with fraudulent intent obtain or aid another person in obtaining personal identifying information of an individual without the consent of that individual for the purpose of using that information or selling or transferring that information to obtain any benefit, credit, goods, services, or other item of value in the name of that individual.

c. A person may not knowingly and willfully assume the identity of another:
With fraudulent intent to obtain any benefit, goods, services, or other item of value:
With fraudulent intent to avoid payment of a debt or other obligation: or
To avoid prosecution for a crime. ■

Students Share Their Thoughts

On Internet Safety in an Essay Contest

When asked to submit a letter to give advice to incoming 6th grade students on the 'cool' uses of technology and how to use it safely, many students at Perry Hall Middle School stepped forward to offer their input. Joyce Caldwell, Library Media Specialist at the Middle School said, "It was great to see the kid's thoughts on Internet safety and to hear what they had to recommend to fellow students." Caldwell said the 1st, 2nd, and 3rd place winners will be recognized in an upcoming parent bulletin, Pawprints, and they will also be able to share excerpts from their essays with other students over the morning announcements.

1st

1st Place Winner: Olivia
Cyberspace Predators – Cyber Stalking

With new technology advancements every day, many, many people have access to things like the 'world wide web' or the Internet. Did you know in the United States alone, there are 80 million adults and 10 million children who have access to the Internet? Out of those 90 million, some of them are Cyberspace predators. These people will prey on any victim who happens to respond to their instant message or email. That's how it all starts – a simple "hello" or "what's up." Later on, if you keep responding to them, they might ask you for personal information (ex. address, phone number, or email address). No matter what, you don't want to give out personal information, even if they say they want to "hang out." Always ask an adult before giving out personal information. It may sound dumb, but you will end up being much safer.

Another way Cyberspace predators try to harass you is by asking for passwords and user names to get on your "Xanga" or MySpace." Giving passwords out to predators is like giving them the key to part of your personal life. Now they know your daily feelings, your school, your address, and your friend's personal information. You shouldn't give anyone, including your friends, your passwords to anything. Even your Internet service provider (Comcast, AOL, MSN, etc.) will never ask you for your passwords. Even though Cyberspace harassment is a growing issue, there are some easy ways to keep yourself safe. Like I've already mentioned, never ever give out your passwords or personal information to anyone. Also, if you have instant messaging, you want to have a genderless screen name. Most cyber predators go for young women, so don't go for a screen name like "Little Miss Princess 06." The less strangers know about you, the better off you are.

When you are on any website, you don't want to try to "win big" on any pop ups. Pop ups are merely there for other people to make some extra money, or to get email addresses. Like anything else, never give out any more information than you have to. Also, if you need a password to have a file on any site, words like "hi" or "password" aren't going to work. Predators know all the easy passwords, so they aren't going to get you anywhere. Use a favorite celebrity, pet's name, or a combination of letters and numbers that you can remember.

There is a lot out there to watch out for on the Internet. But, with my simple advice, you can be confident on the World Wide Web. Cyberspace Predators, watch out!

Sources for information:

- www.wsdj.gov/criminal/cybercrime/cyberstalking.htm, "1999 Report on Cyber Stalking: A New Challenge for Law Enforcement and Industry"
- www.writing.fsv.edu/oow/2001/protecting.htm, "Protecting Yourself"

2nd

2nd Place Winner: Blake
Sharks in Cyberspace! Beware of Surfing on the Web

According to the news reports, there are many dangers lurking about in your computer such as viruses, hackers, and even predators. Without a doubt, using the Internet can be dangerous, but knowing what to avoid will help to make it safe.



Students Share Their Thoughts

On Internet Safety in an Essay Contest

Viruses/Hackers:

Initially, one of the ways to stay safe is to not download or open pop ups. This will stop viruses or hackers from attacking your computer and stealing personal information. Don't ever give out credit card numbers or banking information. Even email and instant messaging that seems friendly could actually be intruders.

Also avoid chat rooms that don't have clearly written guidelines. Many chat rooms are filled with violent and illegal conversations that are inappropriate for everyone, but especially for preteens and teens. There are people online who talk about very disturbing things.

Resist the urge to post a picture of yourself or type personal information on a site open to the public. Someone could actually take your picture and do strange and awful things with it, and then post it on another site. If you type in things like your age, address, or telephone, strangers – who you should not trust – could use this information. Sharing personal information online is like letting someone read a love note you wrote for a special person, to a million people. That would be awful!

Predators:

Last but not least, never agree to a face-to-face meeting with someone you only met online. People can very easily lie about their age and their intentions. Believe it or not, even inmates in jail have access to the Internet. Criminals are constantly looking for their next victim on the web. So just because the person you have been chatting with says they are a 12 year old girl, think again. They could actually be a 40 year old man.

Finally, this is a chance for you to impress your parents. So take responsibility and learn how to protect yourself while you're on the Web. Remember, if you want to avoid sharks in the ocean, stay away from unknown waters. If you want to avoid viruses, hackers and predators in the Internet, stay away from unknown sites. Always stay safe in Cyberspace.

Helpful Sites and #'s:

- www.safekids.com
- www.netismartz.org/safety/safetytips.htm
- Teen Safety on the Information Highway 800-843-5678



3rd Place Winner: Vivian Internet Safety

Evidently, statistics are showing that once students are in middle school, it seems that they are using the Internet at home more often than they did in elementary school. From my experience, most elementary school students use the Internet for entertainment and personal interests in addition to researching information for educational purposes. However, as they grow older, they become more proficient with computers and the Internet. Most of the students I know that use the Internet during leisure time use it for instant messaging their friends, emailing, and blogging.

What has been occurring on the news about pre-teens and teenagers using the Internet to communicate with others was found quite appalling. The stories and interviews on the news about the subject were generally all the same. They were about pre-teens and teenagers instant messaging people they didn't know. The end results were rather drastic; in one of the cases, there were strangers who invited the teenager, (through a chat room) to come to where they live and be friends, or to hang out, but they ended up killing the teenager. Others who had blogs were being asked to put some strangers' email address on their contact list. A number of students use an online social networking website, such as 'myspace.com', to post personal information, and simply write about what's been going on in their life. With that information, it is quite easy to locate that person for the wrong



Students Share Their Thoughts

On Internet Safety in an Essay Contest

reasons. To those who eventually become 6th graders and enter middle school, here are some suggestions to staying safe online:

- Use your online resources responsibly and wisely.
- If you are in the middle of instant messaging, and some stranger's screen name comes up asking you to talk to them, just block them off. If you have already entered the room by accident or mistake, just automatically leave the room.
- If the person said something to you in an inappropriate manner, uses foul language, or harassment, tell an adult.
- Do not email or instant message to anyone you don't know.
- Never reveal your identity, such as your name, age, sex, phone number, address, or school to any stranger online via email or chat room.
- Never answer or discuss any personal or family business with the stranger such as parents' names, profession, their incomes, work schedule, etc.
- If the stranger asks for your email or personal information through your blog, do not answer him.
- Do not hesitate to shut off the computer if you feel uncomfortable with anything happening online.

With this information in mind, students should be able to minimize the risks associated with online security.

INTERNET SAFETY STUDENT ESSAY CONTEST – HONORABLE QUOTES from other students at Perry Hall Middle School

For example, the website myspace.com, it's not safe. To have an account with them your address, name, date of birth, and phone number are required and shown on the site. This is displayed to everyone. Also on myspace.com you have blogs which tell what you did that day or what you are doing the next day. Having this kind of information displayed on the internet, doing this can put you at risk for being kidnapped. If strangers talk to you online, block them or tell an adult. Stay safe. (Stevie)

If you ever plan on making a website, be sure to not post information about yourself because that can be dangerous. Also, you should not download movies and music because it is against the law and you could go to jail if you get caught. (Emily)

Another thing to be careful of is unknown emailers or people IMing you or in a chat room. They could be trying to lure you into their clutches or even try to hurt you. Make sure you know who you are talking to! The computer is a great thing to enjoy but you must be cautious. (Eman)

Everyone gets those post cards in the mail with the headliner "Have you seen me?" Can you see yourself on one of those cards? Neither could those children. But it happens, every day a child is kidnapped, abused, or they end up dead. Online activities could be a big factor as to why those children's lives are or have been changed forever. (Deavon)

We were talking later that night to one of our friends online and told her about this guy that we had met in the chat room and she said that she had talked to him, too. He was not a fourteen year old boy like he told us. He was about thirty. She knew this because he had asked to meet her at the mall on a Friday night. She was smart enough to take about seven friends with her when she met this "fourteen year old boy" so she didn't get hurt and I am glad that we didn't either. (Kendra)

If you go to a website, be careful with pop ups because something like a pop up will get you a series of trouble. I went to this website and this chat line pop up with a grown adult saying "Can you help me? I'm not used to this," and I exited out of it because I told my mom about it and I hold her I exited out and she was proud of me. (Eric) ■

The Millennials: They're Confident, Pressured & And Totally "Tech"

Understanding and protecting this new generation of savvy, high tech children

by Art Stritch
Baltimore County Public Schools

America proudly hails its generations with names like Glorious, Enlightened, Awakened, Progressive, Booming and now Millennial, the eighteenth American Generation. Historically Millennials are slated to be our next Hero generation. Heroes come of age during a Crisis, enter midlife during a High and begin their later years during an Awakening. The G.I. Generation that fought World War II is an example of a Hero generation. Heroes are conventional, extremely powerful, devoted to serving the state and trust authority.

This generation doesn't just use technology but approaches life differently because of technology. (*NetDay* survey 2004, Conclusions). That is not to say that every Millennial is using all of the available technologies in the same way at the same time, but that their whole online life is much bigger than merely the Internet. They have grown up in a world that has always had computers, touchtone phones, cassette tapes, color television, and VCR's just to name a few. The Vietnam War is almost ancient history to them. They are the most sheltered of generations. Think of all the child protection polices that have emerged since 1982; automobile restraint and helmet laws, video and music ratings, Amber Alerts, Megan Laws, child-proof homes, V Chips, drug free and tobacco free zones near schools. These are merely a few policies that have spawned a number of safety devices available to parents too numerous to mention and has gone as far as even home drug testing kits. Millennials only know of "safe schools" and "accountable environments" (allergy free classrooms and cafeterias) and a continued delivery of health and social services. None of this can be considered bad or over-protecting; it is what they have known and helps to explain how they perceive the world around them.

Millennials are confident, trusting and team oriented. This generation has seen a significant drop in suicide rates compared to their counterparts of the mid-seventies. They have replaced the word "I" with the word "We" almost completely opposite of the preceding Generation X'ers. During the elections of 2004 64% of them voted in 10 states where tight races were predicted. This generation can be described as more traditional than their parents and grandparents in both lifestyles and attitudes. Millennials are the most "scheduled" generation in history, they are shuttled to soccer games, dance lessons, piano practice, and tutoring sessions. As a result they have become high achievers with over 79% of all tenth graders anticipating a four year college degree (National Center for Educational Statistics, 2004). The number of AP exams with grades of 3, 4 or 5 has increased 124% in all U.S. Public Schools in eight years, (College Board, 2005). Millennials represent nearly 1/3 of the current U.S. population and spend nearly \$170 billion dollars a year. They are multi-taskers who watch TV, listen and download music, instant message a number of contacts simultaneously all while doing their homework.

The online world is not a separate universe to Millennials. By the time they were in fourth grade the use of the Internet was a common practice in most classrooms, public libraries and was quickly becoming a typical resource in most Middle American households. Computer skills, basic software applications and search strategies were being integrated into daily instructional experiences. The entire world is available to them on a fifteen inch computer screen, many with real time voice capabilities to communicate with anyone in any part of the world.

World wide communication is quickly adapted to their own purposes, permitting close communication with any one they meet, anywhere and growing exponentially. There are no



The Millennials: They're Confident, Pressured & And Totally "Tech"

Understanding and protecting this new generation of savvy, high tech children

longer strangers but merely friends they haven't met. Popular search engines now provide the opportunity to join groups, contribute to blogs, search images, video, and online webcams. The ability to access information readily, email almost anywhere, and share communications has prompted the Millennials to share the most intimate details of their personal and emotional lives anytime of day with anyone. Software has been developed to allow kids with online access to create their own "web-blogs" at almost no cost. The student's entries are archived and made available to anyone with the address or link. The "dark side" of society is now able to enter any household and never use the front door. All of this activity by young people exists behind a veil of sharing. Millennials have no problem with the concept of sharing data. Why not? They are inherent team players. They file share music downloads, copy-cut-and paste text from online databases, share pictures downloaded from cell phones with little caution to copyright or personal safety. How dangerous could it be, they are not physically face to face with anyone. Besides, they have been chatting with all their contacts for months and have become great friends. This trusting generation unknowingly has opened a portal for anyone to enter into their personal life.

As parents and guardians what resources are available to you? Open communication with your millennial child is the best way to learn. Share with them your cautions and the limits you expect to be respected when they are conducting activity online. Another resource is "pull the plug." There is nothing wrong with limiting and/or refusing access to online activity. If your student is unwilling to share with you what, where and with whom they are visiting online then it is time to remove the network cable or disable their wireless modem access. Enabling them to continue practicing dangerous behavior because they can't do their homework without online access may be inconvenient for everyone; however, it will bring focus to the issue that as teens/students/kids there are expectations regarding behavior and practice that must be met. This is a savvy generation; they will rise to your challenge.

Arthur Stritch
Supervisor, Library Information Services
Baltimore County Public Schools

REFERENCES

- Howe, Neil. "Today' Millennial Generation" Presented August 19, 2002 Capital University.
- Prensky, Marc. "The Emerging Online Life of the Digital Native: What they do differently because of technology, and how they do it." ©2004 Marc Prensky.
- Wallis, Claudia. "The Multitasking Generation." *Time*. March 27, 2006.

Parents on Board

Do you remember the overwhelming responsibility you felt to insure that your infant traveled safely in the car; you carefully strapped them into their car seat and proudly displayed the “Baby on Board” sign? Our children quickly outgrow the car seat and before we realize it they are putting on their own seatbelt, this time in the driver’s seat. The years in between find parents cruising along relying on their common sense, the advice of well meaning friends and relatives, and all the parenting tips they can possibly absorb. Our confidence builds as we successfully meet each new challenge of parenting. Just when we think we have earned a chance to relax we find ourselves faced with new situations that scream out the reminder that parental guidance is crucial to insure our child’s safe journey through life. I highly suggest that every parent place an imaginary “Parent on Board” sign on their computer as a family reminder that all of our parental advice on safe and responsible behavior in the neighborhood must apply to the extended neighborhood of cyberspace.

I am just a mom who thought I was pretty aware of the challenges of raising a preteen and teenager in today’s world. Throughout their childhood I had laid the groundwork for acting responsibly and thinking independently. I involved myself in their school and extracurricular activities, knew their friends, discussed current events, and tried to understand the current trends much to the amusement of my children. I admit that I am technology challenged by all the latest devices that the youth of today handle with such ease. I never fully realized to what extent that many of these tech savvy kids had abandoned parental advice as they enjoyed unsupervised use of their gadgets, until I watched a Dateline Episode, “Why Parents Must Mind MySpace,” which aired on January 27, 2006.

My daughter, a seventh grader, watched the Dateline episode with me. At the conclusion of the show I learned that she had recently created a MySpace account. Since she was under the age of 14, she had lied to complete the free registration form. As per my request she immediately closed the account. My son, a high school student, informed me that he did not have an account. Ten minutes after the show aired I felt relieved that I had successfully addressed the MySpace issue and assumed I could relax for several days until I was presented with the next parental challenge. When I awoke the next day I found that I could not forget this Dateline episode. I experienced the overwhelming need to gain a better understanding of why the popular social networking sites were so appealing to adolescents.

I immediately began to familiarize myself with MySpace. You can imagine my surprise when several days later I inadvertently discovered a MySpace profile page for my son. This profile page indicated that this account had been opened the day after the Dateline episode aired. When my son returned home from school, I was even more surprised to learn that a good friend, as a joke, had created this page without my son’s prior permission and had even impersonated my son to comment to other friends. At my request this friend, who held the password, immediately removed

the profile page. Although his intention was not malicious and no actual harm was done, it was proof that our very smart tech savvy kids can and do display very poor judgment when using the Internet. It also made me aware that there were many other aspects of Internet use to consider and investigate beyond personal safety and predators such as issues of identity theft, harassment, cyberbullying, slander, and copyright infringement.

My curiosity has led me on an interesting research journey and has helped me to confirm what I had felt along. The problem is not the existence of the Internet, social networking sites, instant messaging, cell phones and all of the other communication devices available to our children. The problem is the inappropriate and unsafe manner in which our children choose to use these technological devices. I am sure many parents have no idea how much personal information their children are posting or the manner in which their children are expressing their private thoughts for millions of people to see. The solution is parental involvement.

Since each family has their own unique dynamics, each parent will need to reach their own decisions as how to best deal with all the challenges presented by their children’s use of these devices and the amount of time that is acceptable for these activities. Parents need to educate themselves about the Internet, visit the popular sites to see for themselves the ease with which they can be navigated and the personal content posted, and then initiate a meaningful discussion with their children regarding the safe and responsible use of the Internet. There are many nonprofit organizations’ websites that provide Internet safety information and tips for parents.

Every generation has had to deal with the reoccurring conflicts that exist between parents and adolescents. Remember when we were adolescents? We thought we were invincible. We thought we knew it all. We challenged our parents’ authority, yet we secretly acknowledged how smart our parents really were. We successfully transitioned from adolescence into adulthood and the same will hold true for our children. The current challenge we now face is how to successfully blend our vast parental knowledge of life experiences with our children’s incredible knowledge of technology. We truly need to learn from each other.

By researching the social networking aspect of Internet use I feel that I have been transformed from “just a mom” into “one smart mom” and with enough time I’ll eventually become “one even smarter mom.” The reality is that parents will never understand the Internet and technological gadgets as well as our children. However, there is a lot of satisfaction in knowing that when our children use the chat abbreviation *pos*, *parent over shoulder*, we can confidently respond *pob*, *parent on board*!

Nancy L. Ostrow
Proud Parent for seventeen years & PTA Member and Baltimore County Public School volunteer for the past 11 years

Additional Resources

Here are resources specifically for parents and caregivers should they have questions or require assistance while helping their children learn about navigating through cyberspace.



Books and Pamphlets

Parents Guide to the Information Superhighway
The Children's Partnership
www.childrenspartnership.org

Librarian's Guide to Cyberspace for Parents and Kids
American Library Association
www.ala.org/parentspage

A Parent's Guide to Protecting Your Children in Cyberspace
Parry Aftab
www.familyguidebook.com

The Internet Kids & Family Yellow Pages
Jean Armour Polly
www.netmom.com

Web Sites

National Center for Missing & Exploited Children (NCMEC)
www.missingkids.com

Protecting Children in Cyberspace
www.protectkids.com

Maryland AskUsNow
www.askusnow.info

Phone Numbers

Baltimore County Police (non-emergency)
410-887-2222
www.baltimorecountyonline.info/agencies/police

Baltimore County Public Library
410-887-6100
www.bcpl.info

Maryland State Police
Computer Crimes Division
410-290-1620

Maryland Center for Missing Children
1-800-637-5437
www.mdsp.org

FBI – Federal Bureau of Investigation
Baltimore Line: 410-265-8080
www.fbi.gov

National Center for Missing & Exploited Children (NCMEC)
Cyber TipLine: 1-800-843-5678
www.missingkids.com