Internet Safety Tips for Parents

1. Communicate and talk to your child about victimization and online danger.
2. Spend time with your children online. Have them teach you about their favorite online destinations.
3. Keep the computer in a common room in the house, not in your child's bedroom. (Remove the mouse at bedtime).
4. Utilize parental controls provided by your service provider and/or blocking software. Do not rely totally on software for protection.
5. Use of chat rooms should be heavily monitored.
6. Always maintain access to your child's online account and randomly check his/her email for safety concerns. Be open with your child and let them know about your monitoring.
7. Teach your child the responsible use of the resources online.
8. Instruct your child to never arrange a face-to-face meeting with someone they met online.
9. Instruct your child to never upload (post) pictures of themselves onto the internet or online services to people they do not personally know.
10. Instruct them to never give out identifying information such as their name, home, address, school name, or telephone number.
11. Instruct them to never respond to messages or bulletin board postings that are suggestive, obscene, or harassing.
12. Remind them often that whatever they are told online may or may not be true.

National Center for Missing and Exploited Children

Cyber Tipline - 1-800-843-5678

Http://www.missingkids.com/cybertip

Top 10 Rules for Kids' Internet Safety

1. Never give out identifying information such as your address, phone number, school name, town, etc., in chat rooms, blogs, email, instant messages, bulletin boards, or questionnaires.
2. Never agree to meet anyone in person that you have met online.
3. Never reply to any email, chat message, or forum item that makes you feel uncomfortable.
4. Never send information or pictures to anyone over the internet that you do not know.
5. Never give your password to anyone except your parents no matter who they say they are.
6. Be aware that people may not be who they say they are. Someone who claims to be a child may really be an adult.
7. Never click on links or attachments in emails from people who you don't know.
8. Don't order anything or give anyone credit card information without your parents' permission.
9. Always tell your parents if someone upsets you or makes you uncomfortable.
10. Always follow your parents' rules regarding computer use.

Thomas W. Pyle Middle School

6311 Wilson Lane

Bethesda, Maryland 20817

Phone: 301-320-6540

Montgomery County Public Schools

Kids and Internet Safety and Security

All uses of computer facilities, networks, and other technology resources must be for educational purposes only and are subject to MCPS review in accordance with IGT-RA

Cyber Safety

Kids learn very quickly that the internet is a place where they can exchange information and interact socially with other users anywhere around the globe. Through tools such as email, instant messaging (IM), surfing, blogging (web logging or journaling), and chatting, kids discover that they can express their thoughts and feelings in any manner they wish and someone will read, relate and respond to what they are saying. With this tremendous resource comes the potential for serious danger.

Dangers

Viruses, spy ware, identity theft, spam, cyber stalking, cyber bullying, pornography, sexual exploitation, are just a few of the hazards of internet. The internet has the potential to make any user a victim of crime. You can protect yourself and your kids by being vigilant and establishing safe internet practices.

Protect your computer

Email. Email is one of the means of introducing viruses and spam to your computer.

Viruses can cause severe damage to your computer hardware and software costing you thousands of dollars and the loss of data. If you use email, you should have virus protection software and anti-spam software installed on your hard drive and you MUST keep the updates current. Never download attachments from sources you don't know. Even be cautious of any unsolicited attachments from people you do know as many viruses are transported by infected address books. If there is any question about an email attachment, do not open it. Deleting it will protect you. Periodically, check the anti-virus websites for tips on how to avoid the traps.

See *http://www.symantec.com or http://www.mcafee.com*

Protect yourself and family

Spyware/Identity theft. Spyware is software that is attached to websites and downloads to you computer when you click on a site or advertisement. Spyware circumvents encryption designed to protect your personal and financial information. Once inside your computer, an intruder has access to anything you have on your hard drive. The intruder can install or read anything at will and monitor your internet interests which then generates spam and popups.

You can protect yourself from spyware by installing a firewall and spyware protection software. Some browsers offer minimal protection through file settings and updates.

Computers located in a multi-user environment are vulnerable to local intruders. In a multi-user environment, users should take appropriate safeguards to protect their logins and passwords. Users should never leave a workstation logged in and unattended where intruders can intentionally or unintentionally cause problems by ignoring any safety procedures, deleting, adding or corrupting files.

You can password protect your data by setting up logins and passwords for all users of the workstation, never share your login and password, never leave your computer unattended and log off the computer workstation completely if you need to be away from the machine for a period of time.

If an intruder gains access to your workstation through spyware, closely monitor your credit and financial information. Report any unauthorized activity to these institutions immediately.

Cyberstalking. Every parent who has a child who uses the internet, should discuss the dangers of posting personal information on the web and sharing information with strangers. Even kids who are careful fall into the traps like filling in surveys about their likes and dislikes. Their responses can provide a predator with enough information to make them easy prey. Something as simple as naming a favorite recording artist or sport team and a connection to a school can provide a predator with a way to initiate contact.

Giving personal information, your full name, address, phone number, photos, descriptive information such as your school, what time you get home, and the times that your parents get home, etc. may seem harmless, but it is too much information to provide to a stalker or predator.

Cyberbullying is sending or posting harmful or threatening text or images using the internet or other digital communication devices. Cyberbullying comes in many forms, such as:

- Flaming—Sending angry, rude, vulgar messages directed at a person or persons privately or in a public forum.
- Harassment– Repeatedly sending a person offensive messages.
- Masquerade– Pretending to be someone else and sending or posting material that makes that person look bad or places that person in potential danger.
- Outing and Trickery—Sending or posting material about a person that contains sensitive, private, or embarrassing information, including forwarding private messages or images.

Cyberbullying material may be posted on personal web sites, in blogs, and on third party web sites. Messages may be transmitted through email, discussion groups, chat, instant messaging, newsgroups and text or digital image messaging via mobile devices. Cyberbullying is emerging as one of the more challenging issues facing educators and parents as young people embrace the internet and other mobile communication technologies.

Legal considerations related to cyberbullying

Law enforcement officials should be contacted whenever cyberbullying involves death threats or threats of other forms of violence to a person or property; excessive intimidation or extortion; threats or intimidation that involve any form of bias or discrimination based on race, religion, gender, sexual orientation; any evidence of sexual exploitation.

Victims have a legal right to claim damages for defamation, invasion of privacy, intentional infliction of emotional distress. In most states parents can be held financially liable for damages caused by their children.

If you are a victim of cyberbullying, save the evidence. Make a screen shot of the offending text. Include all identifying tags, screen names, etc. Contact law enforcement if there are threats of violence. Contact school authorities to report any threats that involve the school or to report incidents that occurred during school hours utilizing school resources. Identify the perpetrator. Change your email address. Contact the perpetrator's ISP and request the account be terminated.

i.e. abuse@*<domain name or provider>*.com