SAFE INTERNET

Nathan H. Lyons and the entire Carroll County Commonwealth's Attorney's office would like to offer some tips on how to have a safe and pleasant internet experience.

OVERVIEW

Parents need to be aware that children can go online from their computer at home, at a friend's house, in school, at the public library, at a club, at an internet cafe, and from any number of different handheld communication devices from laptop computers to cell phones. Many game consoles can also be connected to the internet and be used for chatting and other online interactions. In other words, children do not have to be in the company of responsible adults to use the internet.

There are no censors on the internet. Anyone in the world - companies, governments, individuals, and organizations - good and bad, responsible and irresponsible - can publish material on the internet. Your computer and Internet Service Provider (ISP) links you to these sites, but cannot fully control or censor what is on them. Most people who go online have mainly positive experiences, but, like any other endeavor, there are some risks involved and some annoyances. The online world, like the rest of society, is made up of a wide array of people. Most are decent and respectful, but some may be rude, obnoxious, insulting, or even mean and exploitive. Children get a lot of benefits from being online, but they can also be targets of crime, exploitation and harassment in this as in any other environment. Children and teenagers need supervision and common sense advice to make sure that their experience in cyberspace is happy, healthy and productive.

THE RISKS

There are real risks involved for children, and especially teenagers, who use the internet unsupervised. Teens are more likely to participate in online discussions regarding companionship or sexual activity. Some specific risks include:

Exposure to inappropriate material.
Your child may be accidentally exposed to material considered to be sexual, hateful, violent, or material encouraging illegal or dangerous activities. Some children may intentionally seek out

such material, but all could come across it on the web, in chat rooms, in email, or even instant messaging.

Physical molestation.
Your child might provide information or arrange an encounter or meeting possibly risking his or her safety or the safety of other family members. In some cases child molesters have used chat areas, email, and instant messaging to gain a child's confidence and then arrange a face-to-face meeting.

Harassment and bullying.
Your child might encounter messages via chats, email, or their cell phones that are belligerent, demeaning, or harassing. Bullies, typically other young people, often use the internet to bother their victims.

Legal and financial.
Your child could do something that has negative legal or financial consequences, such as giving out a family member's credit card number or doing something that may violate another person's rights. Legal issues aside, children should be taught good netiquette, which means to avoid being inconsiderate, mean or rude on the internet.

Viruses and hackers.
Your child could download a file containing a virus that could damage the computer or increase the risk of a hacker gaining remote access to the computer. This could jeopardize your family's privacy and safety.

Here's a little quiz on Phishing Attacks or **How to Spot a Scam**

It is important that you and your teenager understand how a phishing attack works. Phishing is a technique that hackers use to steal information by duplicating legitimate websites with copies that are almost exactly the same; some are very, very convincing. A phished website may pose as a bank or other financial institution and ask for private or personal information in an attempt to steal your identity or worse. The following is a five-question quiz run in the 10/17/2007 Wall Street Journal. See if you can spot the phony websites.

Here are five Web addresses. Can you tell which are real and which are fake (run by a hacker)?

1) http://ebay.verification.com
2) http://www4.da-us.chase.com/cgi-bin
3) http://secure.citibanking.net
4) http://pages.ebay.corn/services/forum/feedback.html
5) http://www.secure-account.com/regionsbank

Quiz answers:

1) Fake
2) Legitimate

3) Fake
4) Legitimate
5) Fake

The part of the address that matters comes just before the ".com " or ".net", so in the first example, the site is really verification.com, and has nothing to do with eBay. Many legitimate sites have letters other than www before the company name, so the web address in sample # 2 is fine. Anything that comes after a "/" just represents a page off of the main site.

HOW YOU CAN REDUCE THE RISKS

While children need a certain amount of privacy, they also need family involvement and supervision in their daily lives. The same general parenting skills that apply in the real world also apply online. Just as you would if you had a concern about your child's regular activities, if you have cause for concern regarding their online activities you must take action. Talk to your children about the pitfalls of the internet. Seek out the advice and counsel of teacher, librarians, and other internet and online service users in your area. Having open communication with your children about using computer resources as well as getting online yourself will help you to obtain the full benefit of these systems and will help to alert you to any potential problem that may occur with their use. If your child tells you about an upsetting message, person or website, don't blame your child, but help him or her avoid problems in the future.

Beyond these basics there are some specific things you should know about the internet. For instance, did you know that there are chat areas, newsgroups, and web sites that have hateful or violent material or material otherwise considered to be inappropriate? It is very possible to stumble across this type of material while doing research. Remember, search engines (Google, Yahoo, Ask, Dogpile, etc.), websites commonly used for legitimate research, do not filter out material that might be bad for children. If your child winds up at an inappropriate site, tell them to immediately leave that page by pushing the Home icon, by going to another site, or shutting down the browser software.

Some Internet Providers allow parents or guardians to limit their children's access to certain services and features, such as adult-oriented chat rooms, bulletin boards and websites. There may be an area just for children where it is less likely for them to stumble onto inappropriate material or get into an unsupervised chat. At the very least, you should keep track of any files that your children download to the computer, consider sharing an email account with your child (to oversee their email) and consider joining them when they are in chat rooms.

In addition, there are ways to filter or control what your children can see and do online - although no filter is 100% foolproof. Customized software will never take the place of good parental supervision, but you can find a directory of filtering programs at http://kids.getnetwise.org/tools/.

Another option is to use a rating system that relies on website operators to indicate the nature of their material. Internet browsers can be configured to only allow children to visit sites rated at the level parents or guardians specify. The advantage to this method is only appropriately rated

sites can be viewed. The disadvantage is that many appropriate websites have not submitted themselves for a rating and will therefore be blocked.

Regardless of whether you choose to use a child-friendly Internet Service Provider, a filtering program or an internet rating system, the best way to assure your children are having positive online experiences is to stay in touch with what they are doing. One way to do this is to spend time with your child while they are online. Have them show you what they do and ask them to teach you how to use the internet or online service. You might be surprised how much your children know and also how much you can learn from your children.

GUIDELINES FOR PARENTS OR GUARDIANS

By taking responsibility for your children's online computer use, parents or guardians can greatly minimize any potential risks of being online. Make it a rule to:

Keep your family computer in a family room rather than in a child's bedroom. Shining the light of day on your child's online surfing habits may be enough to keep them out of harms way.

Never give out identifying information, such as home address, school name, or telephone number in a public message such as a chat or newsgroup. Be sure you know who you are dealing with when you give that kind of information out via email. Think carefully before revealing any personal information to anyone. Do not post photographs of your children in newsgroups or on websites available to the general public. Consider using a pseudonym (an alias), and avoid listing your child's name or email address in any public directory or online profile.

Get to know the internet services your child uses. If you don't know how to log on, get your child or an internet savvy friend to show you. Have your child show you what he or she does online, and become familiar with all of their activities online. Find out if your children have free, web-based email accounts (such as an email account from Yahoo.com, Hotmail.com, Gmail.com, etc.) or their own personal websites (MySpace.com, Facebook.com, Friendster.com, etc.). If they do have such accounts, learn their user names and passwords and check up on their usage. It also may be helpful to learn the places, such as the school, library, or friend's houses, where your children can routinely access those accounts.

Never allow your child to arrange a face-to-face meeting with someone they first meet on the internet. If you decide to disregard that advice and decide to allow a meeting, make the first one in a public place and be sure to accompany your child.

Never respond to messages that are suggestive, obscene, belligerent, threatening, or make you feel scared, uncomfortable or confused. Encourage your child to tell you if they encounter such messages. If you or your child receives a message that is harassing, of a sexual nature, or threatening, forward a copy of the message to your Internet Service Provider (ISP) and ask for their assistance. Instruct your child not to click on any hyperlinks contained in email messages from persons that they do not know. Such links could lead to sexually explicit or otherwise inappropriate websites or could initiate a computer virus.

People online may not be who they seem or claim to be. Because you cannot see or hear the person you are corresponding with it is easy for someone with bad intentions to misrepresent themselves. Thus, someone indicating online that they are a 12-year old female could, in reality, be a 40-year old man.

Everything you read or see online may not be true. Just as with offers received in the mail or seen on television, any offer online that is "too good to be true" probably is. Be extremely careful

Set reasonable rules and guidelines for computer use by your children. You may want to print out a copy of My Rules For Online Safety and post them near your computer as a reminder. Remember to monitor your children's compliance with these rules, especially when it comes to the amount of time your children spend online. Personal computers and online services should not be used as electronic babysitters.

Check out blocking, filtering, and ratings applications to see if they will be of assistance to your family.

Always use, and keep current, Anti-Virus and Anti-Adware software on your computer.