

Computer Tech Talk

Safety on the Internet

By Dennis Henson

Physical Safety. If you have a teenager and internet access, your teen probably spends a great deal of time chatting with friends online. Are they talking to any strangers or someone pretending to be someone else? According to the "Crimes Against Children Research Center", one in five U.S. teenagers who regularly logon to the Internet say they have received an unwanted sexual solicitation via the web. As a parent, should you prohibit your child from getting on the internet altogether? Common sense advice from the FBI suggests, "There are dangers in every part of our society. By educating your children to these dangers and taking appropriate steps to protect them, they can benefit from the wealth of information now available online." The internet is the world's information at your finger tips; the good, the bad, and the ugly.

Chatting-Webcamming. Online services like MSN, AOL, and Yahoo provide instant communications between you and a list of people you have designated. Text typed by you appears instantly on their screen. With an internet enabled camera (called a webcam), you can exchange live audio and video -- the new video-telephone. What's your teen saying, sending, and seeing?

Bloggng. Your teen probably has a blog. Anyone can, for free, publish an online journal called a weblog or blog, complete with text, pictures, video, and audio. Make sure your teen sets up their blog so that visitors are required to be in their list of "friends". Use a site that requires each visitor to be "accepted". Popular services include Xanga, MySpace, and FaceBook. What's in your teen's blog? Who's in their lists of friends? Is any personal or sensitive information published?

Chat Rooms. You can also communicate online via virtual meeting places called chat rooms. These sites are usually associated with special interest groups. Do your teens use chat rooms? With whom do they speak? What info do they share?

Parent Involvement. There is excellent advice available on the internet for parents to educate and protect children from internet dangers.

Let's start with the FBI. Go to www.fbi.gov and type "internet safety" in their search window. Open "The Parent's Guide to Internet Safety".

Recommendations for parent involvement include: 1. Always use a secure website* Communicate with your child about online dangers. 2. Spend time with your child online. 3. Keep the computer in a common room of your home. 4. Use service provider controls or purchase parental control programs. 5. Maintain access to your entire child's online accounts, web-logs, email, etc. Look at what they publish. I would add: be careful what websites you visit and how you search. Search results can sometimes be quite surprising.

Important Nevers. Instruct your child to: never arrange a meeting with someone they met online; never upload pictures of themselves on the internet to someone that you do not know; never provide identifying information like full name, address, phone number; never download pictures from an unknown source; never respond to emails, bulletin board postings, or chat room discussions that are obscene, offensive, or suggestive; Remind your teen anything they are told online may or may not be true.

Other Useful Sites. Visit the Web Wise Kids at www.wiredwithwisdom.org and click on the "For Parents" link. Also go to www.staysafe.org and click on the "Parents" menu item. Staysafe discusses parent's actions to safeguard children online. If these sources are insufficient, go to www.google.com and search for "internet safety" to pursue this topic on your own.

Identity and Data Confidential. Clean your computer of sensitive data before you dispose of it. Use an overwrite program or remove the hard drive. A hard drive is the size of a paper back book and can be removed and secured. Unplug the PC first!

Theft. Do you have important sensitive financial, medical, or personal data on your computer? Is it safeguarded? A very good article by the "Public Safety and Emergency Preparedness Group of the Canadian Government" (IN04-002) lists "Best Practices for Preventing Online Identity Theft" for consumers. Their best practices include: 1. Install and frequently update a proven anti-virus product. I would add: scan regularly for spyware using a proven product like Spybot-S&D. 2. Ensure your browser and operating system are updated with the latest fixes. 3. Be suspicious of unsolicited email requesting financial data. 4. Don't fill out forms in emails that ask for financial data. 5. Don't click on links supplied to

you via email. Go to the original company site yourself. 6. Be cautious of fake internet sites attempting to mimic the FBI legitimate site, often entered by using an online search engine. 7. 1. Always use a secure website* when transmitting sensitive financial data like social security numbers, credit card and other account numbers. 8. Contact the company via the telephone if there is any doubt. 9. Always report "phishing" emails.

6. Be cautious of fake internet sites attempting to mimic the FBI legitimate site, often entered by using an online search engine. 7. 1. Always use a secure website* when transmitting sensitive financial data like social security numbers, credit card and other account numbers. 8. Contact the company via the telephone if there is any doubt. 9. Always report "phishing" emails.

Phishing. Phishing is a term used to describe unsolicited email, claiming to be from a legitimate company, to trick the user into providing private information (for identity theft). You would not provide your credit card number or bank account number to a stranger calling you cold on the phone, so why would you send them the same information in an e-mail?

Data On Your PC. Protect sensitive data on your PC just as you would printed documents. Most financial programs like Quicken and Microsoft Money have a password you can activate. Consider using a hard drive formatted for enhanced security (NTFS) and encrypt sensitive files and folders. Shred printouts that are sensitive and no longer needed. Delete sensitive files after they are no longer required. Remember that deleting does not remove the file. Deleting either moves the file to the recycle bin (still readable), or hides how to find the file. To prevent all attempts at data recovery, an "overwrite" program must be used to write over the sensitive section of the hard drive. Popular programs you can buy include DataEraser, Diskwiper PE, and PC Confidential.

Clean your computer of sensitive data before you dispose of it. Use an overwrite program or remove the hard drive. A hard drive is the size of a paper back book and can be removed and secured. Unplug the PC first!

Victim of Identity Theft? The Social Security Administration has an electronic fact sheet that provides guidance if you think you have been a victim of identity theft. Go to www.ssa.gov, click on "search" and look for "identity theft".

Questions and comments about this article may be emailed to: hcs@mchsi.com

*Encryption is indicated in Internet Explorer by the "lock" symbol in the lower right corner of the browser. The best secure websites maintain 128-bit SSL encryption of data between you and the site.