Preparing Your Child for the 21st Century

Safely Using the Internet

Vicki L. Sauter, Ph.D.

Big Picture

1. Remember that being online is no more safe than "real life." Practice safety online with your children as you would walking down the street. Everything that can happen in "real life" can start on the computer.
2. Be in charge.
    - Set rules that give you access to their usage
        - Studies show that children are more likely to be more responsible when parents set clear Internet rules
        - You should have their current passwords
    - To take charge, you must know what you are discussing, and must stay up to date
    - Explain to kids that you are responsible for their safety and well-being and what they post online represents your family
    - Tell them you will monitor their behavior
        - Kids who know they are being monitored are less likely to engage in risky behavior
    - Monitor their behavior at irregular intervals
        - Logon to their accounts and see what they see
            - You should have their current passwords
    - Keep computers in public spaces
        - The "walk by" rule: If they change behavior when you walk by, find out why
        - Keep phones/laptops/notebooks in public spaces after "lights out"
3. Be online where your kids are online.
    - Options today: eMail, Facebook, Twitter, Web, chat
    - Get accounts and use them so you know what it is
    - Make sure you are attached ("friended") to all of your child's accounts
    - Check your child's profiles
    - Be respectful of your child
        - Scold "off line"
        - Don't read boyfriend/girlfriend private messages
        - Don't discuss messages unless there is a problem
4. "Google" your child's name
5. Know the signs of cyber bullying
    - Red flags include:
        - child spends longer hours online and seems tense about it
        - suspicious phone calls, e-mails, and plain wrapped packages
        - your credit card statement lists suspicious purchases
        - child stops typing, covers the screen, hits delete, shuts down the computer when he knows you're close
        - child suddenly stops using cell phone or email, web, social networking devices
        - child withdraws from friends or wants to avoid school
        - child is suddenly sullen or shows a marked change in personality or behavior

6. Know the jargon: Chat room jargon is much like texting jargon
    - P911: Mom or Dad in room
    - PA: Parent alert
    - POS: Parents over shoulder
    - PIR: Parent in room
    - PAW: Parents are watching
    - 1,2,3,4,5 (Typing the numerals 1 to 5): Parent reading the screen

Strangers, Penpals, Friends

1. Allow your children to have email contact *only* with friends, relatives and acquaintances
    - Predators pretend to be children and have conversations with your child
    - Children are very trusting if they think the person at the other end of the email of Facebook discussion is also a child and may reveal personal data that could make them identifiable
2. Require your child to tell you immediately if they get an inappropriate email from an adult
3. Require your child to tell you immediately if unknown people are suddenly emailing them
4. Require that all list signups go to your email, or a common family email (so children's email addresses are not registered anywhere)

Computers

1. Keep current with updates to your operating system and to all programs
2. Use virus protection
3. Use malware protection
4. Be cautious about what you do on your computer while using an open WiFi connection

Passwords

1. Always use a "strong password" – passwords are difficult for someone to guess.
    - The stronger the password, the more difficult it is to guess (The locks on your home do not make it impossible for someone to break in, but the better the locks, the more difficult it is for someone to break in.)
    - Strong passwords should be at least 8 characters; the longer the password, the stronger it is.
    - Strong passwords should include both upper and lower case letters
    - Strong passwords should include numbers
    - Strong passwords should include special characters (some will allow no special characters or only certain special characters, while others will allow anything on the keyboard)
2. Avoid easy to guess passwords
    - Do NOT include your name
    - Do NOT include your spouse's or children's pet's name
    - Do NOT include birthdates, anniversary dates
    - Do NOT include other easily guessable items
    - Do NOT include repetitions of the same character (such as "cccccc" or "123456")
    - Do NOT include words in a dictionary

3. Build a password
    - Try using a phrase: instead of using "Mike" as a password, try a phrase, "I am Mike's Mom."
    - Most computers do not like spaces in a password, so you would have to connect the words either by running the phrase together, "IamMike'sMom" or by putting some character between the words, such as "I_am_Mike's_Mom".
    - Do some substitution of letters with numbers (again, the more "different" kinds of characters you have, the stronger the password). Have fun with it. Instead of the "i" in Mike, use a "1" (one) and instead of the "o" in Mom, use a "0" (zero). So, now the password is "I_am_M1ke's_M0m". These are not words in any dictionary.
    - Perhaps intentionally misspell a word, like "Mik" rather than "Mike" or use some shorthand or other substitution, such as "I_am_M1ke3s_M0m".
4. Best Practices
    - Do not use the same password for all of your accounts
        - I group my accounts into "types" or "purposes" and use the same passwords for each type, but different passwords across types. It is not as good as different ones, but it is more practical.
    - Always have a unique password for very important accounts, such as my work account or my bank account.
    - Change your passwords regularly. You can do this by appending or substituting words or characters to your phrase, or having different phrases each time.
    - If you use a public computer for your internet use, do not allow the computer to save your passwords; this only allows the next person to use them too.
    - Do not keep a list of your passwords under your keyboard or next to your computer if other people have access to your space. I keep mine in an electronic notebook, but access to the list is password protected.
    - Check the strength of your password. Sometimes you will get feedback from the organization for which you are selecting a password. Or, you can check it with a trusted online service, such as Microsoft (https://www.microsoft.com/security/pc-security/password-checker.aspx).

Email

1. Understand spam and scams!
    - Spam in unwanted advertising messages
        - Spam also comes from friends and relatives
        - Be sure what you pass on is REAL
            - Lots of emails and Facebook postings about lost children, golden opportunities and people are FALSE
            - Always check the veracity of information at sites like Snopes (http://www.snopes.com) Or other urban legend sites
    - Scams are emails intended to steal your money or identity
        - If it sounds too good to be true, it is
        - Do not give your information, credit card or other identifiers until you are sure who it is

2. NEVER click on a link in an email!
    - Emails can be faked so that the link you read is not the link to which the email points
    - Often these links go to sites that *appear* like a legitimate site and ask you to login or provide account numbers or such so they can steal them
3. Never open an attachment from someone you do not know (and be cautious about attachments even when you know the author
    - Email addresses can easily be faked

Facebook

1. USE your privacy settings
2. To see your security settings
    - select the small arrow to the right of "home" in the upper right hand corner of the screen
    - scroll down to "privacy settings"
    - select the first option, labeled "How you connect"
    - press "edit settings."
    - select the last option, which is labeled,"Who can see Wall posts by others on your profile?"
3. Secure photos of your children to be seen only by your friends
4. Secure what your children post so that can only be seen by friends
5. Do not click on links that are sensational or promise to provide you with "free tickets on Southwest Airlines," a "$1000 Visa Card, " My Funny Name," "My Name Talks," and "Coke Giveaway."
6. Cautiously link to games and other applications
7. “Like” Facecrooks for updates about current scams and problems

Questions?

Email: vicki.sauter@umsl.edu
Facebook: Vicki TheGeek Sauter
Blog: http://internetuseforseniors.wordpress.com
LinkedIn: Vicki Sauter
Webpage: http://www.umsl.edu