

## **Kids – Practice Safe Behavior Online**

You can *never* be sure whom they are speaking with on the Internet:

### **Rules:**

- 1) Never give out any personal information over the internet including:
  - a. Name
  - b. Address
  - c. Phone Number
  - d. Age
- 2) Never share other information that can be used to identify you such as:
  - a. Where you go to school
  - b. Where you are going to be, or usually hang out (Mall, Park, etc.)
  - c. Where your parents work
  - d. Landmarks around your house (I live by...)
  - e. Similar information about friends or family
- 3) Never agree to meet & greet offline...period.
- 4) If you receive an E-mail from someone you do not know, don't open it and ask a trusted adult for help.
- 5) Never fill out membership forms w/o parents or lab supervisor's permission.
- 6) Chat rooms are like shouting on the Internet – even if you are talking with someone you know from school – others can be watching & listening, so don't use personal information or discuss specific plans on the Internet.
- 7) Be Respectful & Polite – the Internet is a community much like your neighborhood. Don't be mean or rude on the Internet.
- 8) When you see anything on the Internet that makes you feel weird, sad, or uncomfortable, turn off the monitor (do not delete the message) and tell a parent or your lab supervisor immediately and they can respond accordingly or notify law enforcement.
- 9) If someone tries to share this type of information with you or asks you to reveal any type of personal information, Turn off the monitor (do not delete the message) and tell a parent or your lab supervisor immediately and they can respond accordingly or notify law enforcement.

### **Some helpful websites for teaching young children Internet safety:**

<http://www.getnetwise.org/> for online safety guide, tools, and web sites for kids

<http://www.netsmartz.org> - for age specific teaching tools for children

<http://www.cybersmart.org/home/> - K-8 curriculum & sections for parents, teachers, & children

<http://www.msn.staysafeonline.com> - cartoon about computer safety & quiz

<http://www.cybercitizenship.org/4kids/4kids.html> - List of other sites helpful for teaching kids

## **Parents – How to Reinforce safe behavior online**

*Parental involvement is crucial to the safety of children online. Just as children are taught how to be safer when they are traveling to school or in their neighborhoods, parents must talk with their kids about the rules for staying safer online. Children are naturally curious and being introduced to technology at young ages. Thus it is important that adults address their children's safety regarding online technologies.*

- 1) Print, Sign, and periodically review house rules regarding computer and Internet use. Posted them on or near the monitor. Age specific examples available at <http://www.netsmartz.org/>.
- 2) Consider using filtering or monitoring software for your computer.
  - a. <http://www.getnetwise.org/tools/> - Search for tools that
    - i. Limit time online
    - ii. Monitor activities
    - iii. Filter content (such as Hate, Violence, Sex, & Illegal Activities)
    - iv. Block outgoing content
    - v. Kid friendly browsers
  - b. Types of Monitoring Software
    - i. List-Based Website Filtering
    - ii. Rules-Based Filtering
    - iii. Permission Filtering (Kidsnet)
    - iv. Other Filtering (IM, email, Chat)
    - v. Application Filtering (KaZaA)
    - vi. Spying (Watching kids screen from another PC)
  - c. PC Mag's Recommendations for Monitoring Software – July 2003
    - i. Cybersitter 2003 – from Solid Oak Software - Price: \$39.95
    - ii. CyberPatrol 6.0 - from SurfControl - Price: \$39.00
    - iii. Kidsnet - from Kidsnet Inc. - Price: \$40.00 per year
- 3) Look into safeguarding programs or options your online service provider might offer. These may include monitoring or filtering capabilities. (MSN, AOL, Earthlink, Yahoo!, etc.)
- 4) Web sites for children are not permitted to request personal information without a parent's permission. Talk to your children about what personal information is and why you should never give it to people online.
- 5) Keep the computer in the family room or another open area of your home.
- 6) Let your children show you what they can do online, and visit their favorite sites or chat rooms
- 7) Have your children use child-friendly search engines when completing homework
- 8) If you suspect online "stalking" or sexual exploitation of a child, report it to your local law-enforcement agency. The National Center for Missing & Exploited Children (NCMEC) has a system for identifying online predators and child pornographers and contributing to law-enforcement investigations. It's called the CyberTipline at <http://www.missingkids.com/cybertip/>.

Leads forwarded to the site are acknowledged and shared with the appropriate law-enforcement agency for investigation.

- 9) Be aware of any other computers your child may be using.
- 10) Know who your children are exchanging E-mail with, and only let them use chat areas that you have visited. NetSmartz recommends limiting chat room access to child-friendly chat sites, for children in this age group. Know their friend's usernames and check w/ their parents.
- \* Be aware of the issues regarding your child's access to Spam. "Spam" refers to junk mail, what some companies euphemistically call "Unsolicited Commercial Email", "Targeted Email" or other honey-coated expressions.

Spam often contains information, links, or even images not suitable for children. One in five children opened and read spam and more than half of them checked e-mail without parental oversight.

#### Preventing Spam

- Never reply to a message from a stranger.
- Never respond to the Spam email's instructions to reply with the word "remove."
- Never use a preview pane when browsing through your Spam folder.
- Use Spam filtering applications ([www.GetNetWise.org](http://www.GetNetWise.org))
- Use disposable addresses from a free email service for the email you share online

#### ISP, Mail Client, & Software Solutions

- Check for ISP filters first – AOL, MSN, Earthlink
  - Employ mail client features –
  - MS Outlook or Mac OS X Mail
  - Software if nothing else works - (Recommendations from [ConsumerReports.org](http://ConsumerReports.org) – “E-mail spam blocking” - August 2003)
    - Bloomba – Free, but technical to install
    - Mailshell – \$20
    - Blue Squirrel – \$30
    - Symmantec – \$70 (packaged w/ antivirus & firewall software)
- 11) Be particularly sensitive to any change in behavior. Amount of time online. Urgency to begin IM or chat, when they return home, etc. (Source: Jim Louderback – ExtremeTech)
  - 12) Be aware of the "boss screen." These screens depict an innocuous spreadsheet or word-processing document, and can be popped up instantly with just a keystroke. (Source: Jim Louderback – ExtremeTech)
  - 13) Internet accounts should be in the parent's name with parents having the primary screen name, controlling passwords, and using blocking and/or filtering devices.
  - 14) Children should not complete a profile for a service provider and children's screen names should be nondescript so as not to identify that the user is a child.
  - 15) With older kids, discuss issues like copyright & piracy when applicable to writing reports and downloading media.



**Protect your family and your computer – [www.staysafeonline.info](http://www.staysafeonline.info)**

**1. Use protection software "*anti-virus software*" and keep it up to date.**

Make sure you have anti-virus software on your computer! Anti-virus software is designed to protect you and your computer against known viruses so you don't have to worry. But with new viruses emerging daily, anti-virus programs need regular updates, like annual flu shots, to recognize these new viruses. Be sure to update your anti-virus software regularly! The more often you keep it updated, say once a week, the better. Check with the web site of your anti-virus software company to see some sample descriptions of viruses and to get regular updates for your software. Stop viruses in their tracks!

**2. Don't open email from unknown sources.**

A simple rule of thumb is that if you don't know the person who is sending you an email, be very careful about opening the email and any file attached to it. Should you receive a suspicious email, the best thing to do is to delete the entire message, including any attachment. Even if you do know the person sending you the email, you should exercise caution if the message is strange and unexpected, particularly if it contains unusual hyperlinks. Your friend may have accidentally sent you a virus. Such was the case with the "I Love You" virus that spread to millions of people in 2001. When in doubt, delete!

**3. Use hard-to-guess passwords.**

Passwords will only keep outsiders out if they are difficult to guess! Don't share your password, and don't use the same password in more than one place. If someone should happen to guess one of your passwords, you don't want them to be able to use it in other places. The golden rules of passwords are: (1) A password should have a minimum of 8 characters, be as meaningless as possible, and use uppercase letters, lowercase letters and numbers, e.g., xk28LP97. (2) Change passwords regularly, at least every 90 days. (3) Do not give out your password to anyone! [Try the song method]

“Three Blind Mice, See how they run” = 3BM,Chtr!

“Take me out to the ball game” = Tmo2tBG

“Can you take me to...Funky Town” = Cutm2\_FT?

**4. Protect your computer from Internet intruders -- use "*firewalls*".**

Equip your computer with a firewall! Firewalls create a protective wall between your computer and the outside world. They come in two forms, software firewalls that run on your personal computer and hardware firewalls that protect a number of computers at the same time. They work by filtering out unauthorized or potentially dangerous types of data from the Internet, while still allowing other (good) data to reach your computer. Firewalls also ensure that unauthorized persons can't gain access to your computer while you're connected to the Internet. You can find firewall hardware and software at most computer stores nationwide. Don't let intruders in!

**5. Don't share access to your computers with strangers. Learn about file sharing risks.**

Your computer operating system may allow other computers on a network, including the Internet, to access the hard-drive of your computer in order to "share files". This ability to share files can be used to infect your computer with a virus or look at the files on your computer if you don't pay close attention. So, unless you really need this ability, make sure you turn off file-sharing. Check your operating system and your other program help files to learn how to disable file sharing. Don't share access to your computer with strangers!

**6. Disconnect from the Internet when not in use.**

Remember that the Digital Highway is a two-way road. You send and receive information on it. Disconnecting your computer from the Internet when you're not online lessens the chance that someone will be able to access your computer. And if you haven't kept your anti-virus software up-to-date, or don't have a firewall in place, someone could infect your computer or use it to harm someone else on the Internet. Be safe and disconnect!

**7. Back up your computer data.**

Experienced computer users know that there are two types of people: those who have already lost data and those who are going to experience the pain of losing data in the future. Back up small amounts of data on floppy disks and larger amounts on CDs. If you have access to a network, save copies of your data on another computer in the network. Most people make weekly backups of all their important data. And make sure you have your original software start-up disks handy and available in the event your computer system files get damaged. Be prepared!

**8. Regularly download security protection update "*patches*".**

Most major software companies today have to release updates and patches to their software every so often. Sometimes bugs are discovered in a program that may allow a malicious person to attack your computer. When these bugs are discovered, the software companies, or vendors, create patches that they post on their web sites. You need to be sure you download and install the patches! Check your software vendors' web sites on a regular basis for new security patches or use the new automated patching features that some companies offer. If you don't have the time to do the work yourself, download and install a utility program to do it for you. There are available software programs that can perform this task for you. Stay informed!

**9. Check your security on a regular basis. When you change your clocks for daylight-savings time, reevaluate your computer security.**

The programs and operating system on your computer have many valuable features that make your life easier, but can also leave you vulnerable to hackers and viruses. You should evaluate your computer security at least twice a year -- do it when you change the clocks for daylight-savings! Look at the settings on applications that you have on your computer. Your browser software, for example, typically has a security setting in its preferences area. Check what settings you have and make sure you have the security level appropriate for you. Set a high bar for yourself!

**10. Make sure your family members and/or your employees know what to do if your computer becomes infected.**

It's important that everyone who uses a computer be aware of proper security practices. People should know how to update virus protection software, how to download security patches from software vendors and how to create a proper password. Make sure they know these tips too!

- \* **Wireless Security—Four Steps You Need to Take – (Linksys - <http://www.linksys.com/edu/page10.asp>)**
  - Change the default SSID.
  - Disable SSID broadcast.
  - Change the default password needed to access a wireless device.
  - Enable MAC address filtering.

There are other security measures you can take as well, but these four are the most essential. For more information on additional security features, such as Wired Equivalent Privacy (WEP) encryption, and details on how to implement these four steps, refer to the User Guides for your wireless products.