KNOW THE RULES... INTERNET SAFETY QUIZ FOR ADULTS

1. Where is the best place to locate your family computer?

- A. Child's bedroom
- B. Family room
- C. Office in remote area of the home

Answer B. The safest location for the computer is in a room where there is sufficient adult supervision. But don't stop there. It's also critical to know what other access your child may have including friends' homes, libraries, schools, and cellular telephones and other wireless devices. They may even connect on gaming consoles. Thus have a plan in place to closely supervise and monitor your children's online activity no matter where they are accessing the Internet.

2. Which is the best example of how to protect your children when online?

- A. Post clear, simple, easy-to-read rules on or near the monitor; closely supervise your children's online activity when they are using the family computer; and monitor your children's online activity when they access the Internet from other locations
- B. Only allow your children to use the computer at the public library or school
- C. Do not allow your children to "surf" the Internet without having a friend nearby

Answer A. Posting clear, simple, easy-to-read rules is an excellent way to set boundaries for your children's Internet use. Consider having your children and you sign the rules, which should be periodically reviewed. Visit **www.NetSmartz.org** for examples of rules. This website provides animated videos, real-life stories, and safety tips to help you better understand the many different areas of the Internet. If you have questions about the online world, visit **www.NetSmartz411.org** for guidance customized to your situation. Remember nothing beats your supervision of and attention to what your children do while online.

3. Your children are completely safe if they only visit child-friendly chatrooms. True or False?

Answer False. It is not recommended that children visit chatrooms since the potential risks are particularly high on these websites. Realize anyone may access these websites. Those who wish to harm children have been known to entice children in child-oriented chatrooms. Nothing should replace your supervision.

- 4. What should you do if your children tell you someone they have "met" online has asked for their telephone number and wants to meet them in person?
 - A. Take away their computer privileges.
 - B. Praise them for telling you this, and discuss with them the reasons why it is unsafe to meet in person with someone they have first met online without your supervision. Then make a CyberTipline[®] report if you suspect this person is an adult attempting to meet a child.
 - C. Tell them it's okay to meet their friend as long as you know where they are going.

Answer B. Rewarding your children for being forthcoming with information is an excellent way to keep the lines of communication between your children and you open. Furthermore, your acceptance and praise of this may encourage them to report incidents to you in the future. You should remind your children not to give out personal information or meet anyone in person without your prior knowledge and consent. If you want to consider a meeting, ask to talk to the other child's parents/guardians. If you agree to the meeting, accompany your child and meet with the other child and his or her parents/guardians in a public place. If you suspect this person is an adult trying to meet a child, go to www.cybertipline.com or call 1-800-843-5678 to make a report.

5. Of the choices below, which is the best screenname for a child?

1-800-THE-LOST® (1-800-843-5678)

www.missingkids.com

- A. katie_ny13
- B. CuteLitlAngel
- C. Pkdg_329

Answer C. Those online who wish to harm children often use screennames to select their potential targets. A screenname should never reveal any identifying information about a child especially things such as name, age, location, year of birth, school name, and year of graduation. Something more benign and innocuous, such as answer C, would be the best choice for a









screenname to avoid calling attention to the user. To make strong screennames or passwords, NetSmartz411SM recommends using the first letter of each word of a phrase or an acronym that is easy to remember. Visit www.NetSmartz411.org for more information.

- 6. How many children, in a one-year period of time, received an online sexual solicitation where the solicitor made or tried to make contact with the child offline via the telephone, mail, or in person?
 - A. 1 in 7 children
 - B. 1 in 25 children
 - C. 1 in 100 children

Answer B. As reported by Janis Wolak, Kimberly Mitchell, and David Finkelhor in Online Victimization of Youth: Five Years Later. Alexandria, Virginia: National Center for Missing & Exploited Children, 2006, page 1, accessed March 26, 2009, at www.missingkids.com/en_US/publications/NC167.pdf.

7. If you are not familiar with computers and the Internet you should

- A. Visit www.NetSmartz411.org to help educate yourself
 - B. Sit down with your children to have them show you websites they visit and how they navigate through the InternetC. Both

Answer C. NetSmartz411 is the premiere Internet-safety helpdesk and hotline for answers to parents' and guardians' questions about computers, Internet safety, and the Web. Ask an expert online at www.NetSmartz411.org or call 1-888-NETS411 (638-7411) to speak to an Analyst. Furthermore, sitting down with your children at the computer is not only an excellent way to learn, it is also a great way to connect with them. And it could be a pleasurable experience for both your children and you.

8. What should you do if you suspect online "stalking" or sexual exploitation of a child?

- A. Ignore it, and hope it goes away
- B. Report it to your local law-enforcement agency and the CyberTipline
- C. Change Internet Service Providers

Answer B. Immediately report the information to local law enforcement and the CyberTipline at www.cybertipline.com or 1-800-843-5678. The Federal Bureau of Investigation recommends — if your children or anyone in your home has received pornography depicting children, your children have been sexually solicited by someone who knows your children are younger

than 18, or your children have received sexually explicit images from someone who knows your children are younger than 18 — you keep the computer screen turned off in order to preserve any evidence for future law-enforcement use. Unless directed to do so by law enforcement, you should not attempt to copy any of the images and/or text found on the computer. These recommendations are reported in *A Parent's Guide to Internet Safety*. Calverton, Maryland: U.S. Department of Justice's Federal Bureau of Investigation, 2000, page 4, accessed March 26, 2009, at www.fbi.gov/publications/pguide/parentsguide.pdf.

9. It is OK for your children to post pictures of themselves on their own personal website, especially if they promise to only give the website address to people they know. True or False?

Answer False. Tell them it is not safe to put photographs or any type of personally identifying information on websites. Remember anyone in the world may access a Web page, and doing these things could make children targets for abduction or sexual exploitation. It is safer to publish photographs on a website where you are able to use privacy settings to share them



with trusted family members and friends only, but this is no guarantee the photographs will not be saved and used in ways you may not realize. If your children are members of a group with a website, photographs of children published online should not be accompanied with identifying information. Group shots are preferable to individual pictures. The group may be identified as "Members of the basketball team." Remember, even a first name may be a tool empowering those who use the Internet to identify and stalk children. Also many schools are now posting individual information about students in Internet yearbooks. Check with your children's school(s) to determine their policy about posting information online.

Copyright © 2003, 2006, and 2009 National Center for Missing & Exploited Children. All rights reserved.

This project was supported by Grant No. 2007-MC-CX-K001 awarded by the Office of Juvenile Justice and Delinquency Prevention, Office of Justice Programs, U.S. Department of Justice. Points of view or opinions in this document are those of the author and do not necessarily represent the official position or policies of the U.S. Department of Justice. National Center for Missing & Exploited Children[®], 1-800-THE-LOST[®], and CyberTipline[®] are registered service marks of the National Center for Missing & Exploited Children. PDF-8A.