Top Ten Tips for Parents to Protect Kids from Online Predators

Many parents today are struggling with how to provide their children with the benefits of access to the Internet while protecting them from the potential hazards of online predators. In order to help parents, the Cybercrime Committee of the Criminal Justice Section of the American Bar Association has developed a list of "Top Ten Tips." Since no one size fits all situations, the tips below must be considered in light of the child's age and maturity.

1.   Set up a computer with Internet access in an open public area, such as the living room. Avoid positioning a computer in a private area, such as a child's bedroom, or an out-of-the way area, such as a basement.

2.   Talk with your child about basic rules to use while on the Internet, such as instructing them on not giving out their name, home or school address, phone number, age or other personal information. Urge your children to ask your permission before sending photos of themselves over the Internet or setting up a social networking profile. Teach your child that people can easily lie about who they really are, and that they should tell you if anyone says or does anything online that makes them uncomfortable

3.   Don't assume that one conversation is enough.   Some parents may wish to reinforce these guidelines by making a sign that the child can decorate; post it near the computer. Others may wish to write up a "contract" with the child (samples can be found online), which can be periodically renewed.

4.   Consider using filters on your computer. Filters may be available through one's Internet Service Provider or through a search engine, such as Google.

5.   Engage your child about his or her online activities. Be mindful of unusual behavior, such as if a child changes the screen when you enter the room, or if a child spends lengthy amounts of time on the Internet.

6.   Monitor a child's activities on the computer. The Internet browser features history files, for example. Parents may also wish to consider purchasing and using monitoring software (often called "spy" software), or just checking a child's email.

7.   Consider other computer usage by your child – at school, at the library, at homes of friends, and even via cell phones. Talk to your children about where they use the computer and what they do in those places. Make sure you're comfortable with the environment in which your child spends time online, such as at a particular friend's house.

8.	Be alert for unusual activities aside from your child's time on the computer. Pay attention if your child receives mail, gifts, or packages from someone you don't know, or receives calls from or makes calls to people you don't recognize. Another warning sign may be that he or she becomes withdrawn from the family.

9.	Heed the possible warning signs, including finding pornography on your child's computer, or your child receiving phone calls from people you don't recognize; address these situations and don't just ignore the problem or hope it will go away.

10.	Report apparently illegal activity. In case of emergency, contact your local, state or federal law enforcement and others such as the National Center for Missing and Exploited Children. Trust your instinct and report activities to the relevant law enforcement, or report suspicious activities to the CyberTipLine (www.CyberTipline.com, or 1-800-843-5768), operated by the NCMEC.

If you want to educate yourself further on these issues, check out http://www.NetSmartz411.org/, presented by the National Center for Missing & Exploited Children ("NCMEC").