Office of the Santa Barbara County District Attorney
Joyce E. Dudley, District Attorney

TIPS FOR PARENTS

What can you do as parents to help protect your child online?

Parents need to educate themselves and become comfortable with the Internet. Communicate the dangers and risks of being online with your children.

Supervise your children on the Internet just as you would monitor what movies and TV shows they watch and the places they go with their friends.

You would not let your children open the door to a stranger, so don't let them spend long hours online alone.

Using products that can be purchased in computer stores and on the Internet, you can track your child's use of the Internet and block objectionable material from reaching your household. But remember; no product can fulfill all your needs. There is no substitute for your involvement.

Pay attention to your children because, if you don't, someone else might.

Here are a few tips to help you get started:

1. Place your computer in a common area of the house.
   This is probably the most important thing you can do. Do not let your children be in their rooms all night on the Internet.

   The mere presence of parents can have a tremendous effect on a child's online activities. It's much more difficult for a computer sex offender to communicate with a child when the computer screen is visible to a parent or other member of the household.

2. Educate yourself about computers, "smart-phones" and the Internet.
   You need to know how to use the Internet in order to know what your children are doing on it. Take a basic computer class or buy a book about the Internet. Check with your ISP (Internet Service Provider) for information on using all of their services.

3. Spend time with your children online.

Ask your children how they use the Internet and have them teach you about their favorite destinations. Make "surfing the Net" a family experience. Just as you look for good television programs for your children, take the time to find the best and most useful websites for them.

4. Make reasonable rules and set time and use limits. Enforce them.
   You should set guidelines about what your children can and cannot do on the Internet. Try to understand their needs, interest and curiosity. But, you must set limits on when they may use the Internet and for how long.

5. Educate yourself and your child about the dangers of the Internet.
   Teach your children about sexual victimization and other potential dangers of the Internet. Talk openly and honestly with your children about what they are doing on the Internet and what your concerns are.

6. Do not allow your child to go into private chat rooms, especially when you are not present.
   Computer sex offenders will often meet potential victims using chat rooms. Later, they'll attempt to communicate with children by way of e-mail or instant messaging. If you can, try to keep your child out of chat rooms altogether. You never know who is in a chat room watching and waiting for a victim.

7. Reinforce the guiding rule, "Don't talk to strangers."
   Tell your children what they are told online may, or may not, be true. No matter how much their online "buddies" seem like friends who share interests, they are still strangers. Remember, cyber-molesters pretend to be children.

8. Put accounts in your name and know your child's passwords.
   The Internet account and primary screen name should be in your name, not your children's names. It's also a good idea to know your children's passwords and let them know you will check their online activity.

9. Never allow your children to arrange a face-to-face meeting with someone they met online without your permission.
   Many predators want to meet a child for sexual contact. Your child should never meet a stranger alone in a face-to-face meeting. If you ever do agree to a meeting, make sure it is in a public place and accompany your child.

10. Do not let your child give out any personal information of any kind on the Internet.

    Children should never give out their name, home address, telephone number or school name. They should be aware that even naming a friend, local sports team, shopping mall or community event could give away their identities.

11. Do not let your child download or upload pictures without your permission.

    Predators will often send photographs or visuals to children as part of a grooming process to gain trust. Some of the photographs may be pornographic and may even involve child pornography.

12. Utilize your Internet Service Provider's parental controls and commercial blocking and filtering software tools.

    Most ISP's have parental controls – use them. Other filtering and monitoring software programs can be purchased separately. Monitors show a history of use so you can see where your child has been on the Internet. Filters block access to objectionable material. Remember, while parents should utilize monitors and filters, do not totally rely upon them. There is no substitute for parental guidance and supervision.

13. Be sensitive to changes in your children's behaviors that may indicate they are being victimized.

    Be alert to personality changes. If victimized online, children may become withdrawn from their families or secretive about their activities. Computer sex offenders work very hard at driving a wedge between children and their parents.

14. Be alert to a teenager or adult who is paying an unusual amount of attention to your children or giving them gifts.

    Most sexual offenders are not just satisfied with the computer. Eventually, they want to talk to the children on the telephone, engage in "phone sex" and set up a meeting. As part of a "seduction" process, a sexual offender may send letters, photographs, gifts or packages to potential victims. Some offenders have even sent children digital cameras and plane tickets.

15. Be aware of other computers or "smart-phones" your children could be using.

    Your children probably use computers at the library, school, and friends' houses – maybe even cyber-cafés. Be aware that "smart-phones" are just like computers – they access the Internet, send e-mails, post messages to Facebook, blogs,

chat-rooms, and more – just like any other computer. Talk to your children about their "smart-phones" and other computers they use.

16. Be aware of your child using another person's screen name.

    Watch for your child using an online account belonging to someone else in order to bypass filters or monitors on your computer. Computer sex offenders may provide potential victims with a computer account for communication with them.

17. Develop a "contract" with your children about their Internet use.

    You may want to develop an agreement or "contract" with your children about their use of the Internet. A pledge from your children to follow certain rules on the Internet may develop trust.

18. Review the use histories or logs of your computer to see where your children have been.

    Sometimes, you can trace where your child has been on the Internet by checking different areas of your computer. By clicking on Windows Explorer and checking such files as Cookies, Temp History, Internet History or Cache files, you can see what your children have been doing online. You can also check the recycle bin or deleted files to see what's been erased. If you suspect your child is deleting material, some programs will "undelete" files. Remember that some things are not stored unless a person saves or prints it, e.g., instant messages and chat conversations.