The Eleven Commandments of Internet Safety

The following safety tips will lessen the chance of your child to enter into dangerous areas of the Internet. Think of these safety tips as another measure similar to learning traffic rules, or the common "don't talk to strangers" conversation you have had with your son or daughter.

1. Keep the Internet computer in a common area like the kitchen, dining room or den. Do not let your child have access to Internet alone in their bedroom. This does not mean that you must sit next to your child while they are surfing, but be THERE. You should be able to view the monitor from across the room to check in every once in a while to see where they are. Today most homes have several computers. If your child has a computer in their bed room, do not have a hook up for the Internet there. Your child is still able to do their homework, or play offline computer games, and when the need arises to use the Internet, allow them access to the common computer.

2. Instruct your child to never give out specific personal information. This includes, address, birthday, social security number, first and last name, and what school they attend. This might seem obvious to us, but it is not clear to most children that if they provide this information, the extent that it could be distributed. For some websites, a degree of personal information is needed. If your child wants to make a purchase, or have something mailed to them, then, obviously, some personal information is required. I would highly suggest that you fill in the requested information. Personally, I enjoy the convenience of online shopping. However, you should set up as much security as possible for online purchases. I set up a PO box for this purpose. If the goods I ordered were going to be delivered UPS or Fed Ex, and could not be delivered to a post office box, then I had them sent to my place of employment. If you do not have the ability to do this, contact your local UPS store. They might be willing to allow you to have something delivered there. If not, get creative. The bottom line is, do whatever you can to not provide your actual street address. If you have to, be very selective. Read the website's agreement and disclosure statement to determine if they give your information to other parties.

3. Instruct your child to not give out their phone number nor call the new online friend. The ultimate goal of the predator is to make contact with your child, and ultimately arrange a meeting with your son or daughter. These cunning predators have already figured out that most parents have implemented some guidelines on distributing their personal information, so they inform your child that they understand they are not permitted to reveal their phone number, so they have your child call them. If you do not have caller block on your phone, you can bet the pedophile has caller ID and the first time your child contacts them, your phone number is on their caller ID. According to the FBI, a large percentage of abductees called the pedophile, and several predators set up toll free numbers to prevent detection on the phone bill.

4. Instant messages have risks too. These are a combination of a chat room and e-mail, the interaction between your child and the buddy is slightly more secure, due to the buddy list component. Your son or daughter has to allow the buddy access, but do not get a sense of complete comfort. It is not predator proof. In order to be a buddy, your son or daughter had to give permission to be included, but the profile of their new buddy is whatever information that buddy entered. It may or may not be true. My suggestion would be to know the profile names of your child's friends, and then contact their parents for confirmation.

5. Sole password security. Most ISP providers have password access for the user to enter the Internet. Several authorities suggest that you instruct your child to give their password information to no one. A better suggestion is to preclude the password from your child completely. You and your spouse should be the only ones with knowledge of the password. This greatly limits your son or daughter's ability to access the Internet without your knowledge. After all, the Internet is only one aspect of the computer. They would still be able

to play offline games, or write e-mails and save them to send when they are allowed online. This measure will not be the most popular, but it will be the safest.

6. Use the security controls provided by your Internet service provider. Your ISP is certain to offer some type of screening, filters, blocking, and monitoring software. There are hundreds of options available and they can be overwhelming. Decide what level of security you need, then go from there. These measures are to be used as tools, not relied upon solely. The truth is, the only absolute safe measure is parental control and supervision. Think of these measures as the door to your home. When you sleep at night, without some kind of security the door is wide open. Adding these controls closes the door, but does not lock it. The parent holds the key to locking the predator out.

7. Maintain access of your child's Internet trails. This includes their e-mail account, buddy names on instant messaging, chat areas they visit, and friends names. Check these areas frequently. It does not take a 12 year old long to figure out they can change their passwords in these areas. If your child changes one of these without your knowledge and you try and access it, pull the plug. This means literally pulling the plug from the computer and demand their new password. This is an extremely serious matter. It might seem insignificant to your child, but the risk is too great to overlook. Get the new password information, and enforce the message that if they change these with out your permission again, then they will lose Internet privileges indefinitely.

8. Screen your son or daughter's e-mail and US mail. The e-mail screening can be accomplished by accessing their e-mail account, or securing an e-mail software filter that transports their e-mail messages to your account before it goes to them. You then review which e-mails you want them to receive. Depending on your schedule, or relationship with your child, the transport e-mail does take a small amount of time. Another option is to sit with your child when they open it, review the contents, then let them open their e-mail. The security you choose as a parent is an individual one, but the point is to have control over the content of their mail. In addition to screening the e-mail, also screen the US mail. The predator will contact your child by US mail if they have developed rapport with them. The goal is to lure your child and the predator uses a guerilla tactic on their approach, they will use the Internet, phone, and snail mail. The Internet sexual predator will mail gifts, photos of porn, and in several instances the online predators have sent air plane tickets to children they were grooming for abduction.

9. Communicate with your child. This is the most important of all. With direct communication, your child can understand the dangers present. They will be able to follow through with the training you gave them. If you want to implement a safety measure and your child objects, listen to the reasons why. The solution might be simple. For example, one mother tried to get her daughter to agree to the e-mail filter. The daughter was against the idea. Not because she wanted to hide something from her mother, but because her mother worked afternoons. When her daughter got home from school, she could not access her e-mail until later in the evening. To a parent this might seem minor, but imagine what is was like when you were 11 years old. You passed notes between friends, and if you had to wait until the next day to get the note, you would have been disappointed. The solution was that the daughter had to let the baby sitter review her e-mail each day. This solution suited both mom and daughter. And, greatly reduced the likelihood that her daughter would set up an e-mail box without her mother's knowledge.

10. Have a "No matter what you tell me, I won't get angry" policy in place. Make it very clear to your child that no matter what they tell you, you will listen to them. Children, when they have entered into an area of being uncomfortable, tend to think they have done something wrong. They either think they did something to encourage the predator or they think because they have been in contact with the predator they will get into trouble. Be prepared for the jolt you will get when your child confesses something horrendous to you. Suppress your reaction until you are away from your child's view. The goal is to keep your child safe, and your reaction to the insidious experience they may have had, can be dealt with later. The only issue needed to

be dealt with is assuring the safety of your child.

11. Be aware and wary. Know the guidelines your child's school uses when it comes to Internet security. You should know the supervision your child will receive at their friends homes. Know if your child has access to the Internet at church functions. Several priests have confessed to using photographs of porn from the computer to desensitize the child they were grooming for molestation. The computer was something they were both comfortable with and the predator used it to his advantage. Access to the Internet has become viable in many locations, coffee shops, airports and shopping malls have Internet stations where online time can be accessed. Be informed about the opportunities that are presented for your child to access the Internet without your knowledge, they have become quite numerous and readily available.