Online Safety
How to Protect Yourself and Your Family

Introduction

Surfing the internet can be a very positive experience, it opens up a world of possibilities for everyone, expanding our horizons by exposing us to different cultures and ways of life. The experience for most are usually positive, but like any of life endeavours, like attending school, cooking, riding a bicycle, or traveling in a car, there can be some risks involved. We need to be mindful that the online world just like the rest of society, is made up of a wide assortment of people, some are polite, decent and respectful, others can be rude, obnoxious, insulting, or even mean and abusive.

Being Safe - Basic Safety Rules to follow

1. Decide where your child can and can't go on the Internet.
2. Increase your computer security to aid privacy.
3. Monitor where your child go online.
4. Remind your child not to communicate to strangers online.
5. Encourage your child to keep their passwords secret.
7. Always use a first name or nickname to identify yourself online.
8. Never disclose a phone number or give an address to people you don’t know.
9. Never send photographs of yourself to strangers.
10. Never agree to meet someone they met online without adult supervision.

Risks Associated with Children Being Online

1. Exposure to Inappropriate Material
   A child may be exposed to inappropriate material that is sexual, hateful, or violent in nature, or encourages activities that are dangerous or illegal. Children could seek out such material but may also come across it on the web via chat areas, social networking sites, E-mail, or even instant messaging if they’re not looking for it.

2. Physical Molestation
   A child might provide information or arrange an encounter that could risk his or her safety or the safety of other family members. In some cases child molesters have used chat areas, E-mail, and instant messages to gain a child’s confidence and then arrange a face-to-face meeting.
3. **Harassment and Bullying**
   A child might encounter messages via chat, E-mail, on their social networking site or their cellular telephones that are belligerent, demeaning, or harassing. “Bullies,” typically other young people, often use the Internet to bother their victims.

4. **Viruses and Hackers**
   A child could download a file containing a virus that could damage the computer or increase the risk of a “hacker” gaining remote access to the computer; jeopardizing the family’s privacy; and, perhaps, jeopardizing the family’s safety.

5. **Legal and Financial**
   A child could do something that has negative legal or financial consequences such as giving out a parent’s credit-card number or doing something that could get them in trouble with the law or school officials. Legal issues aside, children should be taught good “netiquette” which means to avoid being inconsiderate, mean, or rude.

**Signs That a Child Might Be At Risk Online**

The following guide was prepared from actual investigations involving child crime victims. More information can be gotten from “Child Safety on the Information Highway” and “Teen Safety on the Information Highway”.

1. **Your child spends large amounts of time online, especially at night.**
   Most children that fall victim to computer-sex offenders spend large amounts of time online, particularly in chat rooms. They may go online after dinner and on the weekends. They may be the kids whose parents have told them to go home after school and stay there, without any supervision. They go online to chat with friends, make new friends, pass time, and sometimes look for sexually explicit information. While much of the knowledge and experience gained may be valuable, parents should consider monitoring the amount of time these children spend online.

   Children online are at the greatest risk during the evening hours. While offenders are online around the clock, most work during the day and spend their evenings online trying to locate and lure children or seeking pornography.

2. **You find pornography on your child's computer.**
   Pornography is often used in the sexual victimization of children. Sex offenders often supply their potential victims with pornography as a means of opening sexual discussions and for seduction. Child pornography may be used to show the child victim that sex between children and adults is "normal." Parents should be conscious of the fact that a child may hide the pornographic files on diskettes from them. This may be especially true if the computer is used by other family members.

3. **Your child receives phone calls from men you don't know or is making calls, sometimes long distance, to numbers you don't recognize.**
   While talking to a child victim online is a thrill for a computer-sex offender, it can be very cumbersome. Most want to talk to the children on the telephone. They often engage in "phone sex" with the children and often seek to set up an actual meeting for real sex. While a child may be hesitant to give out his/her home phone number, the computer-sex offenders will give out theirs. With Caller ID, they can readily find out the child's phone number.
4. **Your child receives mail, gifts, or packages from someone you don't know.**
   As part of the seduction process, it is common for offenders to send letters, photographs, and all manner of gifts to their potential victims. Computer-sex offenders have even sent plane tickets in order for the child to travel across the country to meet them.

5. **Your child turns the computer monitor off or quickly changes the screen on the monitor when you come into the room.**
   A child looking at pornographic images or having sexually explicit conversations does not want you to see it on the screen.

6. **Your child becomes withdrawn from the family.**
   Computer-sex offenders will work very hard at driving a wedge between a child and their family or at exploiting their relationship. They will accentuate any minor problems at home that the child might have. Children may also become withdrawn after sexual victimization.

7. **Your child is using an online account belonging to someone else.**
   Even if you don't subscribe to an online service or Internet service, your child may meet an offender while online at a friend's house or the library. Most computers come preloaded with online and/or Internet software. Computer-sex offenders will sometimes provide potential victims with a computer account for communications with them.

---

**What to Do if You Suspect Your Child Is Communicating With a Sexual Predator Online**

1. Consider talking openly with your child about your suspicions. Tell them about the dangers of computer-sex offenders.

2. Review what is on your child's computer. If you don't know how, ask a friend, coworker, relative, or other knowledgeable person. Pornography or any kind of sexual communication can be a warning sign.

3. Use the Caller ID service to determine who is calling your child. Most telephone companies that offer Caller ID also offer a service that allows you to block your number from appearing on someone else's Caller ID.

4. Devices can be purchased that show telephone numbers that have been dialed from your home phone. Additionally, the last number called from your home phone can be retrieved provided that the telephone is equipped with a redial feature.

5. Monitor your child's access to all types of live electronic communications (i.e., chat rooms, instant messages, Internet Relay Chat, etc.), and monitor your child's e-mail. Computer-sex offenders almost always meet potential victims via chat rooms. After meeting a child online, they will continue to communicate electronically often via e-mail.

---

Should any of the following situations arise in your household, via the Internet or online service, you should immediately contact your local police and inform them of the following.

- Your child has received child pornography from another individual or adult.
- Your child is being sexually solicited by someone who knows that your child is under 18 years of age.
- Your child has received sexually explicit images from someone that knows your child is under the age of 18.
If one of these scenarios occurs, keep the computer turned off in order to preserve any evidence for law enforcement use. Unless directed to do so by the police, you should not attempt to copy any of the images and/or text found on the computer.

Steps to Prevent Victimization of Your Child Online

1. Communicate, and talk to your child about their computer activity and stay open to their questions and curiosity. It is never too early to foster open and positive communication with children when it comes to sexual victimization and potential online danger.

2. Spend time with your children online. Have them teach you about their favorite online destinations.

3. Keep the computer in a common room in the house, not in your child's bedroom. It is much more difficult for a computer-sex offender to communicate with a child when the computer screen is visible to a parent or another member of the household.

4. Utilize parental controls provided by your service provider and/or blocking software. While electronic chat can be a great place for children to make new friends and discuss various topics of interest, it is also prowled by computer-sex offenders. Use of chat rooms, in particular, should be heavily monitored. While parents should utilize these mechanisms, they should not totally rely on them.

5. Always maintain access to your child's online account and randomly check his/her e-mail. Be aware that your child could be contacted through the mail. Be up front with your child about your access and reasons why.

6. Teach your child the responsible use of the resources online. There is much more to the online experience than chat rooms.

7. Find out what computer safeguards are utilized by your child's school, the public library, and at the homes of your child's friends. These are all places, outside your normal supervision, where your child could encounter an online predator.

8. Understand, even if your child was a willing participant in any form of sexual exploitation, that he/she is not at fault and is the victim. The offender always bears the complete responsibility for his or her actions.

9. Instruct your children:
   - to never arrange a face-to-face meeting with someone they meet on-line;
   - to never upload (post) pictures of themselves onto the Internet or online service to people they do not personally know.
   - to never give out identifying information such as their name, home address, school name, or telephone number.
   - to never download pictures from an unknown source, as there is a good chance there could be sexually explicit images.
   - to never respond to messages or bulletin board postings that are suggestive, obscene, belligerent, or harassing.
   - that whatever they are told online may or may not be true.
Frequently Asked Questions:

Q: My child has received an e-mail advertising for a pornographic website, what should I do?
A: Generally, advertising for an adult, pornographic website that is sent to an e-mail address does not violate any laws. However, if the sender knows the recipient is under the age of 18, it might be against the law in your country and therefore you can report the matter to your local law authorities.

Q: Is any service safer than the others?
A: Sex offenders have contacted children via most of the major online services and the Internet. The most important factors in keeping your child safe online are the utilization of appropriate blocking software and/or parental controls, along with open, honest discussions with your child, monitoring his/her online activity, and following the tips in this pamphlet.

Q: Should I just forbid my child from going online?
A: There are dangers in every part of our society. By educating your children to these dangers and taking appropriate steps to protect them, they can benefit from the wealth of information now available online.

Q: What is an internet filter?
A: An internet filter program or service does exactly what it says - it filters your internet content according to your selected parameters. The internet makes all information available to everyone, even when it is dangerous or inappropriate. Therefore, younger children and impressionable teenagers have access to more and more of this information without the benefit of adult direction and explanation. Internet filtering has become more and more attractive to parents and schools and helps you, as a parent, guardian or teacher; introduce your child or teenager to the world and its potential perils in a more appropriate way.

Q: Can I filter internet content about drugs and alcohol?
A: Internet Filtering software companies often offer a block or filter on sites that are related to drugs and alcohol. The internet filter will target websites that promote the use of alcohol recreationally. These could be online liquor stores, beer and alcohol companies or bartender sites. The filters will also block out sites that encourage illegal drug use or sites that promote the sale or growth of illegal drugs.

Q: How do I get rid of pop-ups?
A: More than 95% of web surfers use Internet Explorer, which contains popup blocker capability. Unfortunately, it usually is turned off by default, and most users’ don’t change the settings on their web browsers. Take the time to look in the help files on your browser, find out if it has pop-up blocker tools, and turn them on.

Q: How can I protect myself from viruses and Trojan horse programs?
A: Any unknown file is a potential threat to your information security or data security. Treat any file attachments that might contain executable code as carefully as you would any other new files: save the attachment to disk and then check it with up-to-date internet security software before opening the file.

Q: How do I make sure my password is secure?
A: When you are choosing a password to ensure your email or online security, give the matter some careful thought. The object when choosing a password is to make it as difficult as possible for a cracker to make educated guesses about what you’ve chosen. This leaves him no alternative but a brute-force search, trying every possible combination of letters, numbers, and punctuation. A search of this sort, even conducted on a machine that could try one million passwords per second (most machines can try less than one hundred per second), would require, on the average, over one hundred years to complete.

Q: What can an internet report show me?
A: One way to supervise the computer use in your home is to install an internet filter and then to review the reporting it provides. These internet filtering reports, which should be tamper proof, offer a glimpse of the sites
being blocked and why. It will also show you any sites that users attempted to view and were blocked. It will show the percentage of time spent on various sites and will show you a snapshot of the "types" of websites your family is visiting the most.

**Q: Can internet filtering block good or informational websites?**
A: It’s important to remember when you are installing internet filters that some good or informational sites may be blocked from view. For instance if you have an internet filter on your computer, your young student might not be able to access a site about breast cancer because it uses the term, "breast." Of course, there are many other ways to conduct research on a topic and for the most part, your internet filtering software will merely prevent your child from seeing sites that might be potentially damaging or dangerous.

**Q: How can I protect my computer's data?**
A: Ideally, serious information security demands that you back up your entire system on a regular basis. If this isn’t practical, at least backup files that you can’t afford to lose or that would be difficult to replace: documents, bookmark files, address books, important E-mail, etc.

**Q: What should I do if I think my computer is infected by a virus?**
A: If your computer is infected by a virus, don’t panic. Just follow the directions in your Internet Security Software anti-virus program for cleaning it. If you have backup copies of the infected files, use those to restore the files and your data security. Check the files you restore to make sure your backups weren’t infected.

**Q: What organizations exist to help combat computer crime?**
A: The Internet Service Provider (ISP) you choose can have an impact on your computer security. Select an ISP that offers online virus, spam filters and content email filters on their main computers ("server side") or use an email service that does. If you are using a dial-up Internet connection, consider moving to DSL or cable to make it easier and faster to use the automatic update features of Windows, anti-virus, and other internet security software and privacy software.