

Keeping Your Kids Safe Online

TABLE OF CONTENTS

INTRODUCTION.....	4
1 THE INTERNET.....	5
HISTORY OF THE INTERNET.....	5
INTRANETS AND THE WORLD WIDE WEB.....	6
NETWORKS AND THE THREE-LEVEL HIERARCHY.....	7
WHERE CHILDREN ACCESS THE INTERNET.....	7
2 DANGERS OF THE INTERNET.....	8
POSSIBLE THREATS.....	8
DATA THEFT.....	8
MALICIOUS SOFTWARE.....	9
INAPPROPRIATE CONTENT.....	9
SEXUAL PREDATORS.....	10
CYBER BULLYING.....	10
DRUGS AND GAMBLING.....	11
3 STATISTICS.....	12
THE STATISTICS.....	12
TYPES OF CRIMES AGAINST CHILDREN.....	13
4 LEARNING THE BASICS.....	14
ABBREVIATIONS AND ACRONYMS.....	14
TRACKING COMPUTER ACTIVITY.....	16
TRACKING EMAIL.....	16
PARENTAL INVESTIGATION.....	17
TRACKING TOOLS.....	17
COOKIES.....	18
BEACONS AND BUGS.....	18
PARENTAL TRACKING VERSUS ONLINE TRACKING.....	19
5 PLACES CHILDREN ACCESS THE INTERNET.....	20
WHERE CHILDREN USE COMPUTERS.....	20
SCHOOL.....	20
FRIENDS' HOMES.....	21
CELL PHONES.....	21
HOT SPOTS.....	22
6 POPULAR NETWORKING TOOLS AND SITES.....	23

PEER-TO-PEER SYSTEMS	23
EMAIL	24
CHAT ROOMS AND FORUMS	24
ONLINE GAMING.....	25
OTHER POPULAR NETWORKING VENUES	25
PROS AND CONS OF SOCIAL NETWORKING SITES	26
7 REDUCING THE RISKS	27
KNOWLEDGE-BASED EMPOWERMENT AND PROACTIVE INVOLVEMENT	27
RULES	27
BASIC SAFETY TOOLS	28
INTERNET SERVICE PROVIDERS.....	28
ROUTERS	28
OPERATING SYSTEM CONTROLS	29
8 SOFTWARE PROGRAMS AND ONLINE RESOURCES .	30
SOFTWARE PROGRAMS	30
SOCIAL NETWORKING PROGRAMS	30
TIME CONTROL	31
REMOTE NOTIFICATION AND PRIVATE MONITORING	31
BSAFE ONLINE	31
ONLINE RESOURCES	31
TYPES OF RESOURCES	31
EXAMPLES OF USEFUL ONLINE RESOURCES	32
9 COMMUNICATING WITH KIDS	33
COLLABORATION	33
RULES	33
WRITTEN AND VERBAL AGREEMENTS	34
ESTABLISHING A SCHEDULE	34
PRIVACY	34
PERSONAL JOURNALS AND DIARIES	35
10 SUMMARY AND CONCLUSION	36
PRACTICAL APPLICATION.....	36
RESOURCES	36
INTERNET RAPPORT	37
MINIMIZE THE RISKS	37
CONCLUSION: THE INTERNET.....	38
RESOURCES.....	39

INTRODUCTION

Many parents are quite concerned about their children's safety on the Internet. This resource has so much to offer. Children and teens have many learning opportunities available to them through this resource. They can establish healthy friendships and build self esteem through their online activities.

Never before has there been such a vast mode of communication. The Internet has opened many doors for learning and connecting with others. Children can use this resource for educational purposes and for pure enjoyment. This tool is ideal when used in collaboration with a parent.

There are also significant problems with the Internet as well. The network is decentralized and there is no online censorship. Much of the information, movies and images that can be found on the Internet are inappropriate and potentially harmful to children.

The Internet can be used for many great things but it can also be used to harm. Parents can take control of the situation by building a solid foundation of knowledge and creating a plan of action. This document offers background information, helpful resources and strategies to help you create a healthy computer environment for your children to enjoy.

1

THE INTERNET

The Internet is a communications network that interconnects computers around the globe. This resource is quite vast and offers immediate information, resources, images and a plethora of other data. The Internet is fundamentally a communicative device that connects people with information and with one another.

Expansive device uses a compilation of IP protocol-based networks. Internet Protocol (IP) is an information-based system that is used to connect one computer to another. In a nutshell, protocols are the languages used to convey information on the Internet. There are vast resources available through this type of system and its endless possibilities are mind-boggling.

The Internet has revolutionized the way that we communicate research and interact with each other. The complex system has changed our methods of buying and selling merchandise and it has had a profound impact on how individuals connect with one another.

There is evidence of the impressive influence the Internet has on people in our very language. New terms are being introduced to the English language. Words like weblog and cyberspace offer new ways of expressing developments. Standard words like cookie, browser and domain have taken on entirely new meanings as a result of the Internet.

HISTORY OF THE INTERNET

The Internet has a fascinating, though brief, history. The concept of a communicative device that works on a global level was once considered to be science fiction. The emergence of such inventions as the telegraph and telephone made the concept of a system of social interaction seem plausible. However, few imagined how expansive the networking structure would be.

The base origin of the Internet is communication, whether a collection of data or simple social interactions. This resource is valuable in crossing many miles in a very short time. In a way, the system works to make the world smaller. People can see places and connect with others who live across the globe in an instant.

Though the basic idea of the Internet can be traced back to sending a letter across the miles, the first documented description of a network system

similar to the Internet was written by the MIT associate J.C.R. Licklider in 1962. Licklider wrote about a Galactic Network that interconnected various computers across the globe.

Robert Kahn is known as the “stepfather to the Internet.” He organized a massive demonstration of a system called the ARPANET in 1972. This demonstration was featured in the International Computer Communication Conference. This very same year, the new concept of electronic mail was also introduced.

Gradually, a global inter-network was developed and by the early 1980s, private Internet service providers. By the 1990s, the Internet was available to the general public. This revolutionary electronic communication device has had a profound impact on our daily lives.

INTRANETS AND THE WORLD WIDE WEB

Some parents can become easily confused when trying to sort through various components of the Internet. Now that we have a basic understanding of what the Internet is, we should look at what the Internet is not. There are some terms that are commonly confused in this subject that should be clarified.

An intranet is an electronic network designed to convey information and data but this structure is quite different from the Internet. An intranet is a corporate complex that uses an Internet provider network system. This network also uses browsers and Web servers.

Intranets are typically restricted to a group of employees that work for a certain company. The resources commonly contain information like vacation leave and benefit plans. Employees have quick access to the necessary information. However, the data is not housed in a globally-based system.

Many people use the terms Internet and World Wide Web interchangeably. However, these are quite different. Consider the Internet to be a decentred system of networks. Each computer is its own hub that fits into a networking infrastructure that connects countless computers together.

The World Wide Web is more of a tool than a system. The Web is a way to access the information available through the Internet. This tool uses HTTP protocol language to convey information. People can find websites, use browsers and Web documents using this resource.

There are other ways that the Internet disseminates information. For example, email can be accessed through the Internet but it is not part of the World Wide Web. Instant Messaging (IM) is another example. The World

Wide Web is a very large part of the Internet but the two are not synonymous.

NETWORKS AND THE THREE-LEVEL HIERARCHY

Very briefly, the three-level hierarchy consists of sub networks, mid-level networks and backbone networks. These systems work together, offering access to data from various venues including universities, research institutions and commercial organizations. One network connects with another in a systematic fashion. The paths are ultimately chosen by the computer operator.

It is important to remember that each computer is a host. Each host functions independently. The individual operating the computer has control over which services to use including Internet and local services. The lack of central control can be empowering for parents since they have many resources available to them.

WHERE CHILDREN ACCESS THE INTERNET

Many parents would love to know every time their child had access to the Internet. This can be very challenging in many circumstances. There are several places that children can gain access to the Internet whether on the computer or not.

Ideally, children have access to the Internet in school and in their homes. This is the perfect scenario for keeping their activities monitored in a reasonable fashion. Parents could be privy to their children's basic activities without overstepping their boundaries in many cases.

Unfortunately, children have access to the Internet in various venues. They can visit friends that have home computers and possibly less supervision. It is important to stay in touch with your child's friends and their parents to make sure that they are under reasonable supervision while on personal computers.

2

DANGERS OF THE INTERNET

There is a significant price to pay for the convenience of the Internet. Many parents are quite concerned about the various elements that their children may be exposed to while surfing the World Wide Web. Having basic knowledge of the Internet is not enough. Parents also need to empower themselves by knowing the dangers as well.

Identifying the possible threats can be an overwhelming experience for many parents but it is a necessary step in the process. Blissful disregard for potential dangers is not recommended when you have children who access the Internet on a regular basis.

It also helps to know the statistics. The stats make the prevalence of the dangers concrete. The notion that the threats are not real is very appealing but the numbers tell another story. In addition, we have to consider the unreported incidents in this relatively new phenomenon.

POSSIBLE THREATS

DATA THEFT

A glaring threat that many families face when children have access to the Internet is data theft. A thief can steal identifying information from an unsuspecting child using various techniques.

Phishing is a common example that is relatable to many adults. When someone is faced with a phishing scam, they are commonly asked for personal information. After the information is given, the thief uses the stolen data to gain access to bank accounts, credit cards and other resources.

For example, a thief may pose as a representative from your bank. You may receive an email stating that someone tried to illegally access your account and it will be closed unless you fill out an online form. The form asks for personal information including your date of birth, address and Social Security number.

While many parents can recognize a phishing scam—including winning the UK lottery—many children can not. Some thieves target children to try and extract valuable financial and personal information in order to gain access to accounts or to steal the parent's identity.

This kind of information is dangerous beyond the realm of identity theft and finances. Some individuals try to exploit and entice children using the phishing approach. Children are often targeted because they are less cautious and because they are more vulnerable.

MALICIOUS SOFTWARE

Malicious software is commonly referred to as malware. This type of software is designed to antagonize, exploit and annihilate. Many parents are probably familiar with viruses and worms that can be used to devastate a personal computer. This is a very expensive lesson that can be difficult to learn without first-hand experience.

Backdoor Trojan programs are of particular concern. These programs are designed to provide unauthorized access to the personal computer. Once the thief has entrance to the computer he may become privy to information including passwords, bank accounts and detailed personal data about the child and his family. He can also gain control of the computer's functions.

This type of software is typically downloaded through infected links. Sometimes people unwittingly download infected programs without knowing it. Problems can occur after the user clicks on advertisements or buttons that launch the infected programs.

Those who invent malware often target children. These thieves know that younger computer users like to share files with friends. They tend to send attachments in emails and they often download music, games and free software. Each of these activities needs to be approached with great caution.

INAPPROPRIATE CONTENT

Many parents are very concerned about exposure to inappropriate content. Unfortunately, the Internet is completely uncensored. Children have access to many inappropriate images, dialogs and other content when they browse the World Wide Web. In many cases, children accidentally stumble across the harmful matter.

The Internet contains a plethora of valuable information. However, this resource also provides access to violent, racist, malicious and sexual content as well. The inappropriate information, images and statements can be very

unnerving to parents, especially considering that there is no way to censor the Internet. Parents have to take a proactive approach to assuring that their children are not exposed.

Parents should begin by determining what is inappropriate for their children. There will be variations from parent to parent according to the age of the child and the parents' philosophies. Adult content is a very problematic concern because it can be accessed quite easily and often accidentally.

Many children and adults find sexual or violent material on the Internet when they are not looking for adult content. Simply following an Instant Message (IM) link can lead to inappropriate material. Browsing the Web can also mislead users to harmful sites as well.

Pop-ups are quite problematic. These advertisements often entice the computer operator to click on the image that leads to the download of malicious software. Others may lead to pornographic sites. Not only do pop-ups provide unwanted access to adult content they can also pose threats to the computer system.

SEXUAL PREDATORS

Traditionally, sexual predators and pedophiles scoured schools, stores and playgrounds for unsuspecting victims. The Internet can be used as a tool for finding young children and it can be used as a source of interaction as well. Many predators approach children online with the hopes of meeting them in real life.

Children may trust others enough to provide personal information to online strangers. This information can include details like the school the child attends, his common activities and schedule. Some children may give out their address and telephone number as well during what seems to be a harmless interaction.

Common resources for sexual predators on the Internet include Instant Messaging (IM), chat rooms and forums. One interaction can lead to another, more intimate correspondence. For example, the predator gains contact with the child in a forum or chat room then follows up by sending emails and instant messages. Gradually, the predator requests to meet the child in person.

CYBER BULLYING

Children are also faced with an unlikely threat on the Internet. Other children can be a great source of distress when they abuse Internet resources. Cyber

bullying is a significant problem that often goes unnoticed. The bully has the benefit of harassing her victim without adult intervention in many cases.

The online bullying is very difficult for children to deal with because it surpasses the schoolyard. There are no adults to supervise the abuse in many cases and children often feel completely helpless in this sad situation. Many never share their painful experience with their friends and family.

Cyber bullying includes insults, gossip and threats that are circulated through emails and Instant Messaging. The hurtful attacks can be posted in forums and in social networking sites. The child is harassed in a personal way in a very public medium.

Just as it is very difficult to control bullies in the playground, it is very difficult to deal with online bullies. In many cases, the bully stays anonymous. Parents need to monitor their child's behavior before and after she goes online. If she appears anxious or upset then she may need some help.

DRUGS AND GAMBLING

Exposure to adult content may also include drugs and gambling. Since there is little regulation available for online content, many people introduce children to harmful elements using this vehicle. If the activity goes unnoticed it can lead to significant problems in the future.

There are sites that actually sell prescription medications without a prescription. Children and teens can have illegal access to meds using the Internet. These sites simply want money. They will send medications through the mail with little more than a credit card number and an address.

Gambling sites are very popular on the Internet and they can be a great source of entertainment. However, many teens may illegally engage in gambling on these sites. Some use credit cards in order to have a chance of winning money.

Parents should carefully check their monthly credit card statements to make sure that no underage gambling is taking place on their computers. The gambling site has no real way of knowing who is operating the computer. They can not detect underage gamblers. Parents have to take a proactive stance on this issue.

3

STATISTICS

THE STATISTICS

The statistics on child abuse on the Internet is staggering; especially when you consider that every incident is not documented. There are many cases that are never reported and many children never communicate their unfortunate experiences with their parents. It is important to keep in mind that this is a relatively new phenomenon that requires a lot of attention.

Statistically, one out of every five children will be the target of an online predator or pedophile each year. This is twenty percent of the children that use the Internet. This is good reason for parents to be very concerned about this problem.

Seventy-seven percent of the targets are fourteen years of age or older. A staggering twenty-two percent are between the ages of ten and thirteen. This very young population is very vulnerable and they are often far too trusting to identify a predator in many cases.

In addition, ninety-three percent of children who are targeted online do not tell their parents about the online sexual advance. The children surveyed noted that they would not disclose this information because they were afraid of being prohibited from using the computer.

Many of the children surveyed admitted that they would give out personal information if they were promised goods or services in exchange. The data includes cell phone numbers, addresses and school location. Some are happy to provide their date of birth as well.

Common information included in profiles includes age, sex and location. (Some solicitors will use ASL to request the child's age, sex and location). Nearly sixty-five percent of teens that have online profiles post videos or photos of themselves. Girls are more likely to post images of themselves than boys.

Nearly seventy percent of teens admitted that they receive personal messages from people they do not know on a regular basis. The majority of teens who receive these messages do not tell their parents or guardians about the correspondence.

It is important to remember that these numbers do not reflect the entire computer using population among children. The above statistics are located on the ChatAlert website, one of many resources available to parents and caregivers. There are many other statistical resources to consider as well, each taking a unique perspective on online dangers for children.

TYPES OF CRIMES AGAINST CHILDREN

It is very unfortunate that modern technology can be used in crimes against children. The predator has a relatively new venue to gain access against to more children than ever before. The criminal has the benefit of anonymity in this venue. The predator faces fewer risks when approaching children online rather than face-to-face.

The face-to -face meetings are of particular concern to parents and caregivers. The gradual building of an online relationship is very dangerous because of the risk of sexual exploitation. Many predators use the Internet to find children that they intend to meet in real life.

Children can also be exploited online without ever meeting their assailant in person. Harassment and exploitative engagements can be conducted solely online. Predators may use email correspondences to gain access to pictures of children. Many conversations may seem innocent at first but eventually lead to explicit sexual correspondence.

There are many types of crimes against children that are rooted on the Internet. These include harassment, sexual exploitation, inappropriate content, illegal drug purchases, violent content and data theft. Children are at risk to be exposed to adult content. They can be provided inappropriate information ranging from hateful racist comments to how to make an explosive.

The prevalence of occurrences is nearly impossible to track. Children and teens admittedly avoid telling parents and caregivers about online solicitation and inappropriate content. Surveys and statistics only cover a small portion of the population.

The Internet is a relatively new communicative device that offers a world of information. Unfortunately, there are many negative elements that parents need to be aware of as well. Online crime against children is a new phenomenon rooted in a very old social problem. There are many new challenges that parents have to face in this realm of anonymity.

4

LEARNING THE BASICS

Parents can take a proactive approach to assuring the safety of their children by learning the basics of online interactions. The Internet can be overwhelming because it is so vast. This seemingly endless resource has so much information and it is quite complex.

Knowing the background information about the Internet presented in Chapter 1 is a great start. Parents can take control of the situation much easier if they have a solid knowledge foundation on which to build.

It also helps to know other basics of the Internet including common abbreviations and acronyms. The language of the Internet is ever changing and the more terms you know the better able you will be to communicate effectively with your kids.

Other important information includes tracking online activity and visiting your child's online profiles. There is a balance that needs to be kept in the realm of your child's privacy. Clearly communicating that the Internet is not a place to post information that is not appropriate for parents to view is a very important step.

Before laying down the ground rules, it is necessary to have a solid understanding of the types of activities that your children engage in during their time online. Constant surveillance and supervision is nothing short of intrusive but intelligent intervention is very useful when it comes to keeping kids safe online.

ABBREVIATIONS AND ACRONYMS

The current abbreviations and acronyms used in many online exchanges are enough to make your head spin. It seems as if your children are corresponding with other using code. However, these variants are actually shorthand that makes communication fast and effective.

The shorthand also makes the correspondences difficult to understand. Parents can learn some commonly used acronyms using the Internet as a

resource. It is crucial that you take some time to invest in learning the common terminology and abbreviations. This is time well spent.

A simple online search through your browser of choice can yield excellent results. Some parents prefer to bookmark pages that contain Internet terminology and abbreviations while others like to take notes on the subject. The latter will take a little more time but it will pay off in the end.

Taking a few notes is a wonderful way to learn the terms and acronyms more effectively. Bookmaking pages that you may never revisit does little good. You also can do well to see which terms and abbreviations stand out. Maybe you have seen them before or perhaps some are outstanding because they are disturbing.

Following are some commonly used acronyms that are of interest to many parents and caregivers. There are many others to consider as well but this list provides a general idea of what you can expect to find. The list does not include abbreviations and acronyms that contain strong language.

- ATTYOB
Anything That Turns You On Baby
- ASL
Age/Sex/Location
- BTWBO
Be There With Bells On
- IRL
In Real Life
- MI RL
Meet In Real Life
- PGP
Pretty Good Privacy
- POS
Parent Over Shoulder
- RFI
Request For Information
- SYT
See You Tonight
- WAUF
Where Are You From

- WDYLL
What Do You Look Like
- WYTTIWTK
What You Tell Them Is What They Know

These acronyms and abbreviations along with many others can be found on the Internet Acronyms Dictionary <http://www.gaarde.org/acronyms/>. This sampling may seem innocent enough but parents and caregivers can monitor their child's interactions a little easier.

Shorthand terms like MIRL (meet in real life) and SYT (see you tonight) are very valuable. Parents can determine whether or not the correspondence is appropriate if they know the key terms and acronyms.

TRACKING COMPUTER ACTIVITY

Fortunately, electronic passage through the Internet leaves evidence that can be traced. The interactions can be traced back from the recipient to the sender. The process can be quite confusing and many techniques are left to investigators. Nevertheless, it is comforting to know that predators can be traced back to their roots.

If there are any concerns about a possible stalking or online crimes against your child, you have the peace of mind in knowing that the authorities are able to track down suspects though the computer. Internet tracking and tracing are valuable resources for authorities in pursuit of an online criminal.

The United States Federal Bureau of Investigation has tracking programs that are designed to track down predators and criminals that use the Internet as a tool for harm or illegal activity. Programs like Carnivore are capable of scanning emails and electronic correspondences in order to find interactions that meet a certain criteria.

TRACKING EMAIL

Email messages can be tracked as well. This may be old news to many people who are privy to recent current events in politics. Email transmissions are quite simple for a computer savvy individual to track. Each correspondence leaves a traceable trail that exists between the sender and the receiver.

Investigators have access to the time and date and location of the transmission is easily unveiled. The internet address (also known as the IP) of the person sending the message can be traced through email transmissions. Anonymous emails are not quite as anonymous as the sender may think.

When a person uses an alias to convey malicious email messages his correspondences can be traced back to his personal computer. Some may try to use public computers in an effort to throw investigators off their trail. In many cases, the institution that houses the computers has information about the sender.

PARENTAL INVESTIGATION

The FBI has impressive resources but this does little good to parents and caregivers that want to take preventative measures to ensure the safety of their children when engaged in online activities. By the time the authorities have entered the investigation serious damage may have already occurred.

Parents and caregivers are best advised to take control of the situation before the need for professional investigation is necessary. Taking preventative measures is the ideal approach to keeping online criminals at bay to the best of your ability. Part of the preventative approach involves tracking tools that can be used by the general population.

TRACKING TOOLS

Computers are well equipped with internal tracking features that can be accessed with relative ease. Common tools include cookies and the browsing history. Parents can find out which websites their children visited and how often by using the browsing history stored in the Internet toolbar. Different browsers will have access to the history in different areas.

For example, FireFox offers quick access to the browsing history in the upper left hand corner of the screen. You can gain access to the browsing history through the Tool or Options button depending on your search engine of choice.

It is important to note that many savvy young computer users know how to delete the browsing history. If the history is consistently empty after your child uses the computer then she is probably clearing her searches. There are some other ways to find browsing information in addition to the search history.

COOKIES

Cookies are files that are automatically stored on your computer when you visit a website. The host computer (your home computer) loads a file or files on to the computer when the operator electronically enters various sites. There are various uses for cookies.

These computer files are actually tracking devices that are helpful in recording the username and password for returning visitors. Commercial sites use the files as a convenience for its customers. The consumer does not have to enter his password and username each time he visits the website. This allows for quick access to the site during subsequent visits.

Cookies also pose some problems as well. The files can be collected without the user knowing. The user's information is at risk for being used without permission or knowledge. It is important to clear cookies from your computer on a regular basis.

Since cookies are files, they can be transferred from one system to another. Law enforcement investigations often look into these files for information and sometimes the information is sold to subscriber mailing list. Nevertheless, illegal collection of this data can also be collected by hackers.

Parents can make a regular practice of looking at the collection of cookies on their Internet browser. Reviewing and clearing the cookies on a monthly, weekly or even daily basis is good practice. It is important to remember that you will have to reenter passwords and usernames on the websites that you visit regularly. This is a very minor inconvenience.

BEACONS AND BUGS

Other tracking devices are quite similar to cookies. While parents can browse through the cookie files to get an idea of where their child has been they can also be used by others to gain information. Beacons, otherwise known as bugs, are tricky information-gathering devices that can pose some problems.

The beacon is an image that is positioned in a webpage or in an email message. This deceptive device is not like cookies because it cannot be disabled. The image can be very difficult to detect. Some are quite small while others are transparent.

When the user clicks on the image his information is automatically sent to the computer that hosts it. The data is sent even if the user is trying to close the graphic. The images can convey the data to a commercial business

looking for leads but in some cases, hackers and online criminals may receive the information.

PARENTAL TRACKING VERSUS ONLINE TRACKING

It is quite obvious that the FBI and hackers have a distinct advantage when it comes to tracking information on the computer. Parents are quite limited in their ability to track their children's activity. Checking the browsing history and cookies does help but there are other tools that can be used to help parents keep track of their kids' online activities.

Before we delve into the various tools for protecting kids on the Internet, it is important to become familiar with the various places children meet others online. These places include physical locations of various computers as well as popular sites, forums and chat rooms.

5

PLACES CHILDREN ACCESS THE INTERNET

WHERE CHILDREN USE COMPUTERS

Networking does not always occur online. Many children and teens gather in certain places in interpersonal social networks as well. Often, real life interactions involve some access to the Internet. Parents can monitor their children relatively well at home but they may find themselves at a loss when their children are in other locations.

Communication is of the utmost importance when it comes to accessing the computer outside of the home environment. You can work very hard to create a safe place for your children to use the home computer but there is little resource available when it comes to other areas.

SCHOOL

Fortunately, the school environment is well controlled. Children that have access to computers in their schools have the benefit of outstanding filters and strictly regulated mode of operation. Some parents like the idea of modeling the home computer schedules after the school environment.

The learning institution is designed to make the most of accessing the Internet in a controlled setting. The students are given a certain amount of time on the computers. This makes the prospect of wandering aimlessly around various websites bleak for many students.

Schedules are very important. When children have a certain number of hours or minutes to conduct searches, they tend to be more productive. Scheduling a certain number of minutes for homework and a designated time for free computer time is ideal whether in school or at home.

There are some reasons that parents should not adopt every aspect of the school's approach to using the Internet. The filters are effective but they can be too restrictive. Children and teens may become very frustrated if they are

not able to access their favorite websites from home. Balance is very important.

FRIENDS' HOMES

The school environment is well controlled. The home computer is well placed and reasonably monitored. The parents have set proper schedules and there is a harmonious balance between using the Internet as a tool for learning and as a source of entertainment. This ideal situation is challenging to realize but it can be done with some effort.

Nevertheless, parents may find another hurdle that they have to cross when it comes to their children's online safety. Peers often have access to computers. Some may be in reasonably monitored environments. Others may not.

It is unfortunate that some parents do not supervise their children's online activity. Some have no idea what sites their children visit on a regular basis and many have no clue that their children have online profiles that contain personal information. They also may not know about the dangers of using the Internet without proper precautions.

This can be a very disheartening situation for parents that work very hard to keep their children safe. It is important to keep the lines of communication open with your child, his friends and other parents. A brief discussion about online safety can make all of the difference.

The parents may seem indifferent and it may seem as if your efforts to establish an agreement across the board are in vain. You may want to suggest that the child does not use his friend's computer if you feel that there is any risk of exposure to inappropriate materials or dangerous activities.

Become familiar with the types of games that your child's friends use on a regular basis. Some may not be appropriate for her age group. Asking parents and your child's friend is a very direct approach that shows your concern. You can also clearly communicate which activities your child may not engage in and which ones are acceptable.

CELL PHONES

Another path to the Internet is the cell phone. This little device has seen many changes over the years and access to the Internet and the World Wide Web are among them. It is very difficult to monitor a child's activity on the cell phone aside from one valuable resource.

The monthly cell phone bill is a great indicator of Internet activity for many accounts. You can get a very good idea of how much your child accesses the Internet by simply viewing your monthly statement in many cases. Many companies charge for these services, making the connections obvious.

Limiting your child's use of the cell phone can be beneficial. The cellular phone may be restricted to making phone calls and taking pictures and video if you are very concerned about inappropriate Internet activity.

HOT SPOTS

Children can also access the Internet if they have a friend or acquaintance meet them at a hotspot. Common places that grant wireless Internet connections include coffee shops, restaurants, airports and shopping centers. There are some benefits and drawbacks to this type of environment.

The major benefit of using hotspots is that they are in public places. It is difficult for a child or teen to access inappropriate content in many of these environments. They are less likely to explore out of a certain realm when they are in a public place.

They are also typically sharing a computer with another person in these environments. This can serve as a benefit because they are limited with time and they are apt to respect another person's property in many cases. This can also be a drawback because your child can not control what his friends and acquaintances access.

If your child or teen is taking a laptop to a hotspot, it is very important to take some precautions. The hotspot should be well established by a reputable organization. A few locations that offer free high speed Internet access may be in operation simply to gain access to your computer.

Fake hotspots may look very real and many people can be lured into using the wireless connections offered in these locations. Once the computer user hooks up to the fake hotspot, hackers are able to access his personal information in the computer. It is crucial that you know the details about any hotspots your child or teen intends to use.

6

POPULAR NETWORKING TOOLS AND SITES

Social networking is very valuable in a child's development whether the interactions are in person or online. Creating a strong network of friends and acquaintances is a wonderful way to build confidence and self esteem. The Internet can serve as a valuable social networking tool for children and teens. It can also serve as a detrimental device as well.

Parents should become familiar with the various social venues available to their children. They should know who their friends are and where they spend their free time. They should also know where they network online. Following are some examples of popular online social networking venues.

PEER-TO-PEER SYSTEMS

Technological advancements have brought many computer users to enter peer-to-peer systems on the Internet. These systems allow users to link their computers to other computers across the globe. This may seem fundamentally similar to the Internet in general but there are significant differences.

Peer-to-peer networks are designed to allow users within each network to share files. There are some benefits to this approach including free software, music and other downloads. Basically, the individuals in the network share the files and programs stored on their computers with others in the same network.

There are some serious ramifications to using this type of system in some cases. Copyright infringement is a serious matter that may be overlooked when using some peer-to-peer networking systems. It is illegal to circulate copyrighted movies, games, music and other downloads without proper consent.

Peer-to-peer systems are also vulnerable to hackers. Those who use these networks are basically making their files public. If the network is unreliable, the users may also be exposing their personal files and information located on the hard drive without knowing it. The networks are prone to worms and viruses as well.

There is no age restriction in the use of peer-to-peer services. Inappropriate material can be easily accessed by people of all ages through these systems. Children may simply want to download a movie but they may find pornographic content instead. Some users mislabel their videos and images for this very purpose.

EMAIL

Email correspondences are quite common. Children and teens have the ability to set up an account with a free email server like Hotmail or Yahoo. This venue is typically safe in many instances. However, just like anything else on the Internet, there are some risks.

Unsolicited emails from strangers are not uncommon and many kids fail to inform a trusted adult about unwanted correspondences. Emails can be found in some online profiles and through cookies in some cases. It is important to urge your child to tell you about any strange emails. In many cases they are simple advertisements but there are occasions when a predator or phishing scheme may try to contact a young computer user.

It is also important to urge your child or teen to open attachments sparingly. They should only open emails with attachments from trusted sources. Many viruses and worms can be spread through attachments in emails. In general, it is best to discourage children from opening emails with attachments at all.

An infected attachment can be innocently sent by a friend or relative. This can occur if the sender has a virus on her computer. Some viruses connect to files, especially pictures. Once the affected email is opened, the virus can spread to the recipient's computer.

CHAT ROOMS AND FORUMS

There is little surprise that chat rooms and forums make the list of popular social sites for children and teenagers. There is also little surprise that these venues are some of the most dangerous for children to use without some supervision. These social networking sites have gotten a lot of attention from the media for the many instances of predatory activities.

Chat rooms are of particular concern because children and teens can develop cyber relationships with predators. The predators often have the intention to meet the child in public. These venues are well observed on some news programs and television shows that expose the potential dangers.

Look for tell-tale signs that your child may be involved with an inappropriate online correspondence in chat rooms and forums. Common signs include long hours on the computer and the tendency to turn off the computer when others enter the room. The child may receive gifts in the mail or letters and pictures. Some may receive strange phone calls.

You may also recognize some changes in behavior as well. Some children will avoid interacting with friends and family. He may become withdrawn and disinterested in his favorite activities. She may be reluctant to talk about her online activities.

ONLINE GAMING

Online gaming may sound innocent enough. However, these activities are no longer simple games between the computer and the user. Today's online games involve countless participants that play against each other over the Internet.

In order to make this process work smoothly, many online games allow players to communicate with each other. They commonly use text messages, microphones or telephones. This may seem pretty safe but there are some similarities to chat rooms to consider.

The players are anonymous strangers who can communicate directly with your child. The discussions are not censored or monitored. Your child can easily give away personal information even if he doesn't realize that he is doing anything dangerous.

Those who use telephones to interact with players in online games are at risk of providing more information than they know. A simple phone number—whether listed or unlisted—can lead to a real name and a real address. The unknown gamer may have resources that can lead him right to your front door.

OTHER POPULAR NETWORKING VENUES

There are countless social networking sites on the Internet that allow people to create an online identity. Many children and teens are drawn to various sites that allow them to create their own pages. Among the most popular are MySpace and Facebook.

MySpace is appropriately named because this venue provides space for each individual who joins to create an online presence. This vast social networking website offers an interactive network. People can make friends online, create profiles and upload images, music and videos.

Many users take advantage of the great exposure that this resource provides. Some create personal profiles that contain some personal information including sex, age and location. Many people display pictures of themselves and others upload videos as well.

PROS AND CONS OF SOCIAL NETWORKING SITES

There are considerable benefits to using a site like MySpace or Facebook. These resources allow you to meet many different people who have similar interests. Some individuals use this type of venue to find work and create strong friendships with people they never would have met otherwise.

These sites often offer other benefits including free music and videos that can be used to make a page more interesting. Young users can learn a lot about using the computer and working with site building tools. This is also a valuable teaching tool that helps kids interact socially and learn how to use various elements in site development and design.

A glaring drawback is the possible exposure to negative elements. Anyone can contact you. Sites like this offer privacy settings that do not allow anyone to see your profile. However, many people may still be able to contact you through these venues.

7

REDUCING THE RISKS

KNOWLEDGE-BASED EMPOWERMENT AND PROACTIVE INVOLVEMENT

By reading the information in this text you have already made great strides in helping your children stay safe while accessing the Internet. The information provided so far has created a fairly solid foundation of knowledge that you can use to make sound decisions.

Having a grasp of where children access the Internet and the different types of activities that they engage in during their online time is a great resource. Once you are familiar with the threats and possible dangers you are well on your way to creating a system that works for your family.

Taking a proactive approach to Internet safety is ideal. There are ways that parents can work in collaboration with their children and teens in order to create a safe environment in the home and on the computer. Clear communication and a systematic approach are key factors in the success of your endeavor.

RULES

Just as the school's environment is well structured with rules and regulations, the home environment can be as well. There are specific rules that can help make using the computer well organized and safer. Once the rules are in force, children are better able to target their searches and enjoy their time online.

The computer's location is of the utmost importance. The computer should be situated in a place in the home that has relatively high traffic. This location should not be full of distractions but it should be easily accessible to other family members. Avoid placing the computer in a private bedroom.

Schedules can be so very valuable when it comes to keeping children safe while working online. If a child or teen has a specific amount of time allowed on the computer, she will tend to use the time wisely and effectively. This

prevents the temptation to blindly surf the World Wide Web which may lead to trouble.

Clearly communicate the importance of leaving all personal information off of the computer. This is one of the most important rules to follow. Under no circumstances should a child provide their or the family's personal information. This includes names, phone numbers, addresses and email addresses.

BASIC SAFETY TOOLS

There are various safety tools that can help parents take a proactive stance on their children's online safety. Following are common examples of helpful tools that are designed to keep predators, hackers and inappropriate content at bay.

INTERNET SERVICE PROVIDERS

Parents have choice when it comes to which Internet Service Provider (ISP) they use. Some providers offer built-in parental controls and Web filtering tools. These tools can include downloadable programs and filters.

A valuable downloadable program will offer subscribers a way to monitor and limit their children's online activity. Providers like America Online offer filters or email contacts, chat room contacts, website content and Instant Messaging (IM). Some programs block access to certain website and interactive services.

Check with your Internet Service Provider to see which parental controls are available to you. After considering the options and various tools offered by these resources you are better able to choose a provider that is right for your family.

ROUTERS

Some Internet routers can be set up to stop suspicious content from entering your computer system. Routers can also be used to assure that family members log on individually each time they use the computer. This makes accessing the Internet impossible if the child is not properly logged in and it also makes monitoring a little easier.

Routers can be challenging to configure. It may be best to find a computer-savvy friend or relative to help you. Some prefer to contact a professional for help in properly configuring their home computer's router.

OPERATING SYSTEM CONTROLS

Computer owners also have access to operating system controls to help keep kids safe while connected to the Internet. Some of these programs are designed to block suspicious content, prohibit access to some programs and games. They can also work to limit the amount of time a user spends on the Internet.

There are operating system control programs for Macintosh and Windows. Each program offers different features that can benefit parents greatly. Microsoft Windows Vista features a compatible system control program and Mac offers products like the Tiger operating system.

8

SOFTWARE PROGRAMS AND ONLINE RESOURCES

Some software programs and online resources are specifically designed to help parents keep their children safe while online. There are various types of programs and resources that you can use in order to make your home computer a safe learning and entertainment tool for your child.

SOFTWARE PROGRAMS

Various software programs are designed for different needs. To ensure that you choose the right products for your family, it is first necessary to determine what type of protection you require. Following are examples of programs that address specific needs.

SOCIAL NETWORKING PROGRAMS

Social networking including features like Instant Messaging (IM) are of particular concern to many parents. Web filters are helpful in blocking inappropriate content but they are not effective in these realms. There are programs available that address the social networking activities.

Some of the programs are offered at not cost as free downloads. An example is IMSafer. This free program alerts parents when an instant message contains questionable content including inappropriate language. It does so without disclosing the entire exchange.

Parents can monitor their child's activities on sites like MySpace and Friendster with products like BeNetSafe and SafeSpacers. BeNetSafe monitors children's activities on these networking sites and provides reports to parents. SafeSpacers is anonymous and monitors profiles and chats in MySpace including the possibility of the child disclosing too much information.

TIME CONTROL

Some programs allow children to access the Internet for a specific amount of time. When the time allotted expires, the program closes the session. This can be bothersome to some children but it can be quite beneficial in some cases. It helps to provide a warning that the Internet session will expire in a few minutes.

REMOTE NOTIFICATION AND PRIVATE MONITORING

Some programs are designed to alert parents when they are not at home. These devices send an email if a child tries to access a blocked site. Some programs offer silent monitoring. Children do not know that their activities are being monitored through these programs.

BSAFE ONLINE

Bsafe Online is a comprehensive software program that offers nearly everything parents need to monitor their children's online activities. This program is outstanding because it offers so much in one product. It is also relatively easy to use and install.

This software program offers pop-up blockers, a two-way firewall and a private data protection system. In addition, the program features activity reporting, scheduling and content filtering among other helpful tools.

ONLINE RESOURCES

Many websites are dedicated to helping parents keep their kids safe online. These sites are specifically designed to address specific concerns that parents may have. They also serve as educational tools for children and their caregivers.

These valuable resources can aid you in your effort to choose the right software programs and to help you develop a strategy for making the Internet a safe place for your child to learn and play. Following are different types of online and specific examples of great sites to consider.

TYPES OF RESOURCES

Some types of resources available to families are designed specifically for parents while others are designed for children and teens. Some of the sites

offer educational material and resources for monitoring online activity. Others offer activities for children and teens to use to help them use the Internet wisely.

You can find a lot of valuable information including step-by-step instructions on how to create a safe computer environment, establish rules and promote a cooperative approach to using the Internet. Parents are wise to invest substantial time in these sites and children can benefit for websites designed for them as well.

EXAMPLES OF USEFUL ONLINE RESOURCES

- NetSmartz is a great online resource for parents and children. This site is remarkably well organized and easily navigated. This website is outstanding because it offers information for specific groups. The information is divided into categories that are organized by the target audience. The home page offers access to information for parents, kids, educators, teens and law enforcement professionals
- Don't Believe the Type is an example of a parent-centered website that offers information about the dangers of irresponsible online use. This site offers insight into the threats, situations to avoid as well as viable suggestions for safely using the Internet.

9

COMMUNICATING WITH KIDS

COLLABORATION

One of the best approaches to keeping kids safe online is to work with them in a collaborative effort. Communication involves interaction. Begin by talking to your child about Internet safety. Follow up with questions and concerns that your child may have.

Of course, the process of communication will vary according to the child's age. Working together to form viable solutions to real problems is the ideal. The child or teen should feel that she has choice and that she has some control over the situation.

RULES

We touched upon rules in an earlier chapter. It is important to present the development of rules in a collaborative fashion with your child. Simply laying down the law with no reasoning behind the rules can work against your efforts in some cases. If children have a clear understanding of the rules and their development, they are more likely to follow through.

When you establish rules together the child has some feeling of control. He is an active participant in the decision-making process. Following are some general rules to consider when developing home computer use regulations for the family to share.

1. Never give out personal information including phone numbers, addressees, real names and locations.
2. Do not give out any passwords even to your best friends.
3. Private chat rooms are off limits.
4. Use a screen names for different sites. Change the name according to the site you are using.
5. Search through bookmarked pages first. If you need to browse the Internet, ask.
6. Always tell parents, caregivers or a trusted adult about disturbing or anonymous correspondences.

7. Do not meet anyone you encounter online in person. Ever.

The rules in your home will vary according to your child's specific needs. It is important to remember to develop these rules together rather than simply writing them down and placing them next to the computer station. These items should be discussed and explored in collaboration.

WRITTEN AND VERBAL AGREEMENTS

Parents may want to write a contract for their child to sign. This contract should include the specific rules and regulations of computer use. The child can read the document and explain what it means briefly before signing it. This can be an effective approach since it is so concrete.

Verbal agreements are not tangible. They may be easily forgotten and the child can easily fall into bad habits. Presenting a document that is created in collaboration is far more effective than spoken agreements.

ESTABLISHING A SCHEDULE

The Internet can be very addictive and extremely distracting. Using bookmarks for favorite websites is a fantastic way to ensure that the child isn't surfing the Web too much. Scheduling is another great approach to proper time management on the computer.

There are countless benefits to schedules including the development of valuable time management skills and self control. Like rules, schedules can be created in a collaborative effort. The child or teen can clearly see how much time is allotted for each particular activity.

You may be surprised by how willing a child is to work with a schedule. Some love to help create a calendar of visual timetable. Parents can always encourage their child to adhere to the schedule by offering an extra hour or two of free time every so often.

PRIVACY

Privacy is a crucial issue to many children and teenagers. There is a balance that needs to be considered, especially as the child grows older. Teenagers are caught in a frenzy of needing independence while still depending on their parents for support and guidance. Not enough supervision can be detrimental. Too much supervision can be devastating.

Encourage your child to communicate his thoughts and concerns with you. Many teens and children avoid inappropriate online activity because they are afraid of being banned from the Internet. Parents can help their children realize that truth and clear communication will not result in privileges being taken away.

PERSONAL JOURNALS AND DIARIES

Influence your child to keep private thoughts in a diary or journal. The child can choose her own book equipped with a lock and key. Some newer journals are electronic, requiring voice activation to open. This is a wonderful approach to creating a privacy balance. It also works to help children realize that very personal thoughts and ideas belong in the home, not on the Internet.

10

SUMMARY AND CONCLUSION

PRACTICAL APPLICATION

Having a sound foundation of knowledge is a great start in any effort. Putting theory into practice is far more challenging. Practical application of the things that you have learned here is a process, not an end. The results will vary and different techniques may be required in order to achieve the desired results.

Having information does little good if the knowledge is not used. Now that you know the threats, the statistics and possible solutions, you are well on your way to creating a proactive approach to keeping your kids safe online. Communication is a key factor in this approach.

Work with your child to create rules and schedules and put the agreement into writing. Encourage your child to follow through by rewarding positive behavior. This includes informing you about unsolicited correspondences from strangers or stumbling across inappropriate materials.

Your knowledge base is a powerful tool that can help you gain control over the situation. You can reinforce the rules and schedules by modeling appropriate online behavior. Create regulations that you need to follow as well including a proper schedule. This can be done in collaboration with your child as well.

RESOURCES

There are countless resources available to concerned parents. Explore various online safety tools and establish which tools are right for your specific needs. Follow up on information found in valuable online safety websites designed for parents and children.

Create a network of concerned parents who can help each other develop viable solutions to Internet-based problems. It is ideal to communicate with your child's friends and her parents on the topic as well. Other parents may have brilliant strategies and links to information that you may find helpful.

INTERNET RAPPORT

Build an Internet rapport with your child. Encourage him to tell you the new things he is learning through the World Wide Web. Praise her for creating bookmarks of her favorite sites and put those favorites into a special folder that is all her own. Many children are excited to share their online activities with their parents if their parents show a genuine interest.

Model the communication process by telling your children how you use the computer. Perhaps you spent an hour looking for the best summer recipes. You can also ask your child what he would like you to find on the Internet for him. Find new favorite sites together and bookmark them.

MINIMIZE THE RISKS

There are always risks when using the Internet. Consider that many adults fall for cons and phishing scams every day. You can minimize the risks by taking a proactive approach that includes active involvement with your child's daily routine. The Internet is a wonderful resource that requires care and attention. It is not a form of babysitting.

Consider the following in your approach:

1. Keep the computer in an open space in the home, not in a private bedroom.
2. Create rules with your child in a collaborative effort.
3. Establish consequences for breaking the rules. These must be consistently followed though if there is an infraction.
4. Reward appropriate behavior.
5. Model appropriate behavior.
6. Encourage communication as well as privacy.
7. Invest in the proper software programs for protection.
8. Explore Internet Service Provider (ISP) and browser options.
9. Make the most of online resources and encourage your child to do the same.
10. Establish a schedule.

There are many other approaches that you can take in order to ensure your child's online safety. One of the most important things you can do is to create an open line of communication. The Internet does not have to be a threat. It can be a very valuable tool if it is used properly.

CONCLUSION: THE INTERNET

The Internet is a relatively new electronic networking device that serves many great purposes. Your children have a wealth of knowledge available at their fingertips. They also have a world of inappropriate materials at their disposal as well.

Parents can help their children make the most of the Internet by actively participating in their online endeavors. Communication, preparation and understanding can work together in a very effective manner when it comes to the proper use of computers.

The world is shrinking due to today's technologies. We are able to travel to far off places and connect with people across the globe in a matter of seconds. There are countless benefits to exploring the Internet. Establishing good habits and thoughtful planning early on is an important step to making this most of this vast resource.

RESOURCES

<http://www.isoc.org/internet/history/brief.shtml>

<http://www.chatalert.com/dangers/research.php>

<http://www.unh.edu/ccrc/>

<http://www.prevent-abuse-now.com/law3a.htm>

<http://www.garde.org/acronyms/>

<http://www.netsmartz.org/netparents.htm>

<http://www.netsmartz.org/safety/statistics.htm>