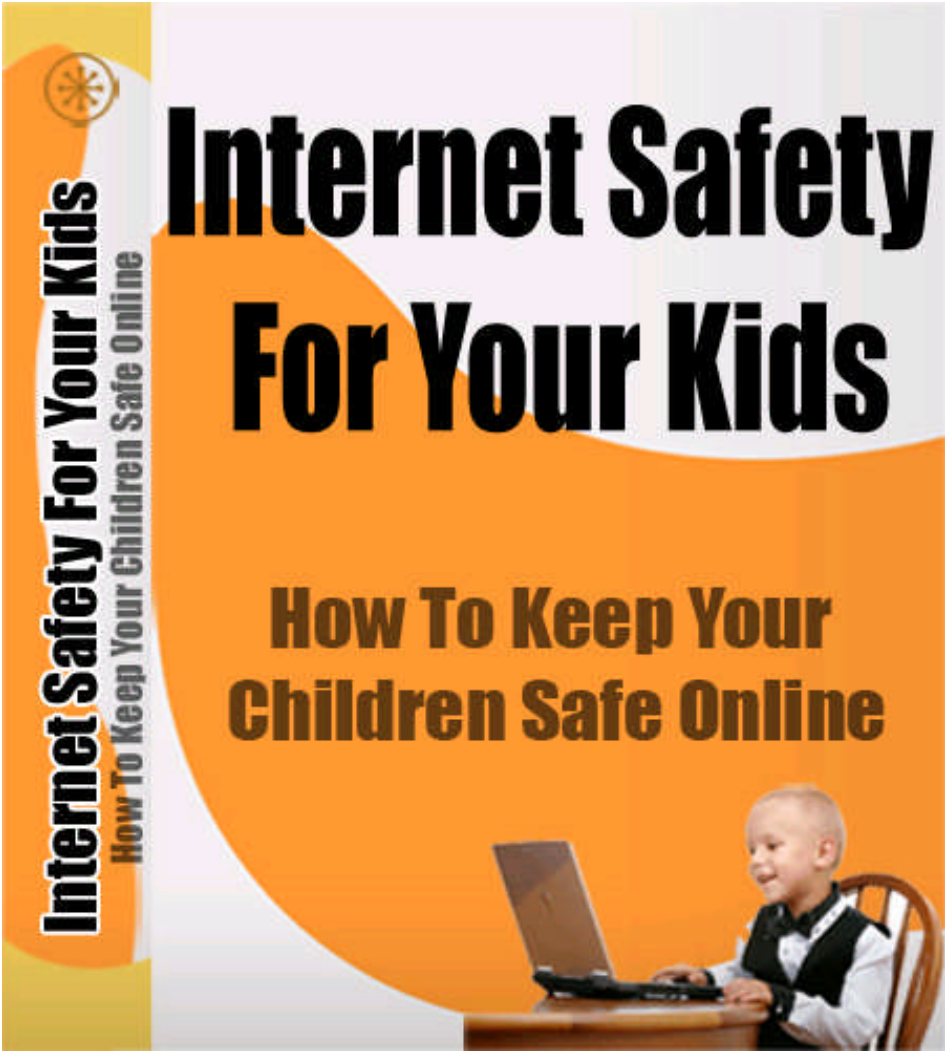


Internet Safety For Your Kids



Internet Safety For Your Kids

Brought to you by:

The Web Business Guide

DISCLAIMER: This information is provided "as is". The author, publishers and marketers of this information disclaim any loss or liability, either directly or indirectly as a consequence of applying the information presented herein, or in regard to the use and application of said information. No guarantee is given, either expressed or implied, in regard to the merchantability, accuracy, or acceptability of the information.

Internet Safety For Your Kids

Table of Contents

Caught in the Middle

What Are Some of the Dangers

Should You Violate Your Child's Privacy?

Phishing and Your Child

What Kind of eMail Is Coming to Your child?

About Firewalls and Free Software

About Abduction

What About International Abduction?

Know Who Your Kids Are Online With

Know Who You Should Contact

Chatrooms, Social Sites and Your Child

Case Studies

What Solutions Are Available

What To Teach Your Kids About the Internet

Resources

Caught in the Middle

Caught in the Middle: How the Internet Can Improve and Destroy Lives

Our access to information has never been so convenient. In ancient times, only young men were allowed to go to school and learn about philosophers and literature. When the ultra-conservative Middle Ages came along, knowledge was left in the hands of the religious, and wouldn't see a renewal until the Renaissance.

As the centuries passed, people were granted greater access to information, until our modern day scholars decided to make things easier for everyone.

From libraries stocking books in order, we moved to databases that stored information in a way that it could be stored, searched through, and retrieved. These databases and the way they were managed were brought online, where they came to the Information Superhighway. The Internet has since revolutionized the way that knowledge is accessed, and has given people from all over the world a chance to learn more and do more.

People are also now, more than ever, eager to share their expertise on specialized subjects, and help out those in need through the ease of online communication. What are some of the advantages offered by the Internet?

- Some sites offer knowledge and information for free or a minimal fee.

The online free encyclopedia Wikipedia, for instance, has allowed users to post their knowledge on certain topics, and has given users the chance to access this knowledge as they would a real encyclopedia. There are also many other sites that offer information for free, such as science sites offering modules that science teachers can use when performing experiments, or clothing sites offering online courses in fashion design.

- Not all libraries carry the books that we need, so online merchants such as Amazon and Barnes and Noble sell books, allowing more people all over the world to buy them. With the advent of the electronic book, or e-book, people can now read books on their computers without having to pick a real heavy book up.

- Knowledge is offered in different media, depending on the learning abilities of those who need information. If a person is more visual, he or she can choose to watch a video or read an online book or pamphlet on the information he or she needs. If a person learns better through listening,

however, he or she can choose to listen to audio files. This flexibility and versatility of the Internet has allowed more people to learn in the format that they want and are most comfortable with.

The beneficiaries of this technology are undoubtedly our children. They will have an easier time doing their research for school, since information is easy to retrieve online. They can buy the books they need if their local libraries don't have them. They can learn through all means possible.

These benefits, however, come with their own risks, and we as parents are caught in the middle of a war between free speech and censorship. While there are thousands of students who benefit from the knowledge offered by the Internet, there are also thousands more who become victims of predators, such as credit card thieves or worse, pedophiles. While there are thousands of students in developing countries who find their minds opened constantly by their exposure to new mindsets and cultures, there are thousands more who find themselves duped by once trustworthy people online.

If you have a child who uses the Internet constantly, then you may want to take note of these disadvantages to better monitor your child's Internet use.

- While information is easier to retrieve online, it can also encourage your child to simply cut and paste information, with little or no effort devoted to analysis. This can make your child lazy, and may even lead to your child being accused of plagiarism by perceptive teachers.
- Not all information online is true, and not all information online is edited. This has led to many schools banning the use of online sources and Wikipedia as references in important reports and assignments.
- Many online help forums are actually a venue for child predators to stalk new victims. Because children and teenagers often seek affirmation and help from people outside their family circle, they are more susceptible to such attacks.
- Pornography is rife online, and some multimedia sites may actually contain pornographic or disturbing images or footage. While your child learns from useful multimedia files, he or she may also be traumatized or wrongly indoctrinated if he or she accesses the wrong ones.

The Internet has its advantages and disadvantages, and we as parents have the right to be alarmed and vigilant. The wealth of information online has also allowed wrongdoing to proliferate, and we can often find ourselves

caught in the middle. All that we can do is protect our children, and make sure that they have access to real books and research materials, so that they don't have to rely completely on online sources for their work.

What Are Some of the Dangers?

What Are Some of the Dangers of the Internet?

The information superhighway and the Internet revolution have allowed people of all ages, races, genders, and inclinations greater access to knowledge and communication. With more information stored online, more people can read about their favorite subjects without having to run to the library, or purchase an expensive encyclopedia set. With more knowledge organized in a format that can be easy to search through, retrieve, and work with, more people can learn faster and do more research online.

This revolution in information technology and presentation comes with its own disadvantages. Not all information presented online is true or edited, and nothing can surpass power of a real encyclopedia or reference book in terms of veracity of the information presented. Not all online forums seeking to help people are populated by experts or, much less, decent Internet users. Not all websites are safe to access, and not all files that you download

from the Internet are free from malicious programs that can give hackers access to your computer.

Our children are the greatest beneficiaries of computer and online technology, and they are certainly its greatest victims. While the Internet can help your primary school student look for facts on Thailand, it may lead him or her to sites that advertise on the country's teeming sex trade.

While the World Wide Web can allow your secondary school student to do research on stem cells, it may ask for his or her credit card to purchase certain articles or books – only to turn the tables on you and allow hackers access to the credit card itself. The Internet is home to information as well as dangers, and in order to protect your children best, you will need to know the dangers.

- Because children are easily impressionable and can easily place their trust in someone who does good things for them, many ill-meaning people can prey on them and ask them to give information that they shouldn't. Such predators operate at many levels, and on many sites.

They can come to forums in the guise of someone who can counsel teenagers or help children with their homework. They can come to chat

rooms and introduce themselves as grandfathers or grandmothers who want to learn about the Internet.

Predators come in many forms, but their aim will be the same: they will use children for their own selfish ends. They can ask children important information about the children's parents, leading the way for the predator to break into the house or office and steal important, valuable items. They can ask children to meet them, leading the children to be kidnapped and sold off to the sex or slave trade.

- Child pornography, despite the efforts of international governments, has shown no signs of slowing down. More and more children are lured by child pornographers to pose for lewd pictures, participate in indecent, often disturbing acts, and ultimately destroy their fragile childhood. Like predators, pornographers will prey on children's innocence, and pose as trustworthy people.
- Purchasing items through online merchants can make shopping easier, especially for housewives who have no time to hop over to the nearest grocery store or mall for things they might need. Online transactions, however, require credit card numbers and addresses, along with other important contact information.

Not all sites are created equal. Site security is becoming more of an issue as identity thieves have stepped up in their efforts to hack into accounts, steal money, and use stolen credit cards to make their transactions. Many online merchants keep a constant vigilant watch over their sites in order to ensure that no hackers enter and steal credit card numbers.

Not all Internet sites and users, however, have the technology to recognize hackers or thieves. Children will usually be the target of such people, as the online medium offers the cloak of invisibility that thieves need to dupe their victims.

By posing as someone who works for a child's father, or an aunt needing money desperately, or even a schoolmate who has met an accident, identity thieves can get credit card numbers from children. Hackers can also access a computer and fetch important information from it, thanks to their techniques of making children believe in their trustworthiness.

The Internet is an exciting marketplace, but it is also a dangerous one. Children are among its greatest victims. The Internet revolutionizes lives, and it can also change them, sometimes for the worse.

Should You Violate Your Child's Privacy?

Computers and Kids: Should You Violate Your Child's Privacy?

The Internet is both a marketplace and a library: while thousands of companies are vying for the attention and money of consumers, thousands of informational materials are available to cater to everyone's need to learn.

The age of Web 2.0 has also turned the Internet into a soundboard for the world's whines and pains, as blogs, diaries, and e-books proliferate. As the information age comes, so does the age of uncensored free expression, where everyone and anyone can post his or her thoughts online, in any shape, manner, or form.

As the once valued prize of privacy is constantly being violated online, and as the lack of private thoughts is lauded on the very much open World Wide Web, the privacy of Internet users is becoming more and more an issue. Credit card theft runs rampant on the Internet, due to the ability of hackers to get into home computers and bank records to retrieve the information

they need. Whole websites can be destroyed by malicious software. Students lose years of information and files when their computers are damaged by viruses.

There is a privacy of a different sort at play when Internet usage is concerned. It involves the right of every human being to read, view, and listen to what they want online. This privacy is something that every website owner holds dear, hence the lack of inhibitions on the Internet. Anyone interested in reading more about the Middle Ages is given a chance to do so, thanks to various history-related websites that feature timelines, footage of reenactments, and even pictures of important historical sites. Anyone who wants to cook can do so, and well, thanks to online culinary courses, and free recipes.

At the same time, anyone who wants to read or view pornographic materials can do so on one of the millions of pornography websites available online. Anyone who wants to see footage of child prostitutes can do so through websites linked to the sex trade. Anyone who wants to steal your credit card, your children, and your life can find a link to you, hunt you down, and do what they want with you and your possessions.

All these claims may seem overblown, but with the lack of restrictions online, and lack of security of most websites, they aren't entirely unfounded. According to research, over a quarter of all families surveyed become victims of credit card fraud and identity theft because their children were preyed on by seemingly trustworthy online thieves.

Thousands of children are kidnapped each year by predators who introduce themselves as well-meaning adults in forums or chat rooms. Even more children are abused, sold to the slave or sex trades, or exploited.

So should you violate your child's right to see what he or she wants online? The answer is a resounding yes. You as the parent have the right to safeguard your child's interests, and it is certainly in your best interest to protect your child from disturbing images, lewd materials, and possible predators. It is your duty to raise your child in the best way possible, and to do everything in your power to give your child the chance to be a better member of society.

You also have the duty to monitor your child's computer activities, which is especially important if your child has his or her own computer, and his or her own unlimited access to the Internet. You may get into quarrels with your

child, so be persuasive, not defensive or combative. You must explain briefly how your intrusion is for his or her own good.

How do you check your child's computer activities? An easy way would be to check your child's history folder, which you can access through the Internet browser. Through this, you can see what files and sites your child has accessed and when. Your child, however, may constantly erase the contents of his or her history folder. If you check your child's computer regularly and find that this is the case, check the Internet options to see if your child has set the computer to never store items in the history folder. If the computer has been set to store items, but the history folder is empty, then you may have to confront your child. Incessant erasing of history folder items may be a sign that your child is accessing pornographic sites.

You may also need to check your child's email, especially his or her deleted items, which can contain items that are being hidden, out of parents' reach. If you have the time, check any recently downloaded or saved files, and see the nature of these files. All of these measures may be difficult to do if your child's computer has a password, or if certain files are hidden or hard to find, but you will certainly find a way to investigate your child's activities as a caring, helping parent.

The Internet may be a cruel world for a child to walk through, but if you have the right principles and the heart of a truly devoted parent, then you can walk through this world together. All you need is perseverance and patience, and the ability to monitor your child's activities, so that his or hers, and consequently, your privacy is protected.

Phishing and Your Child

Child Security and Phishing

Phishing is an Internet term used for a certain kind of modern crime performed over the Internet. It basically involves people masquerading as something harmless, like a bill collector or online survey taker, in an attempt to gather sensitive information and/or insert harmful programs like worms, spyware, and viruses into your computer.

More often than not, children are the biggest security breach in this case. While adults have often been victims of phishers as well, children are often in a greater area of danger because of their inexperience and lack of knowledge. As in the old days, teaching your children to defend themselves is one of the best things you can do to avoid this problem.

Here are a few things to do:

1) Explain Phishing to Your Kids - let your children know about phishing.

Explain to them that people CAN pretend to be your business associates or government representatives online, and that they should NEVER give out any information to someone they don't know.

2) Drill Your Children in Anti Phishing Procedures - aside from refusing to give information, treat this as you would the old case of what you teach your children to do when approached by strangers: that they should contact you if you're available, or play safe and run away (go offline and disconnect the Internet) if the stranger is persistent. Also remember that phishers can come in many forms, even over something as harmless seeming as an online game.

2) Install Simple Firewalls and a Computer Activity Monitor - these two programs are essential. While they may not prevent the actual act of a person getting information from your kids via phishing, they provide their own security measures as well. Firewalls insure that, in case your children accept a harmless seeming survey form, no viruses or worms get inserted into your PC. Also, in the event that a phisher manages to get information

from your kids, a system activity monitor program will allow you to trace what happened while you were gone, so that you can forward the recorded information over to your local police if you wish to have them investigate what happened.

3) Know and Teach your Children about Alternate Phishing Methods - Phishing does not simply involve people trying to access your information by contacting you and your children online. There are other, more indirect methods that they can employ, so make sure your children (and you yourself!) keep aware of the following:

Link Name Manipulation - this is a common trick used by some phishers. They take the name of a famous and trustworthy site and alter it's name slightly to appear, at a casual glance, like the original site. A common trick used is to substitute a small letter "l" for a capital "i" in the name, or to replace a capital "o" with a zero "0". Aside from these simple naming tricks, placing an extension at the end or middle of a URL, like say, `sitename.com.realname.com`, is another common way of masking a hidden site. These sites will often sport a front page that looks almost exactly like the home page of the site they're mimicking, and as soon as you enter your user name and password, the phishers will have it on file and you're in trouble.

Phone Phishing - sometimes, in an offer to "validate" themselves, phishers will offer to call the victim's home to "prove" that they exist and have a "physical office" (As if you could see that over a phone! You'd be surprised at the number of people who fall for this though). As above, remind your children that this does NOT prove anything, and they should avoid any offers of such contact. Under no circumstances are they to give the home number, and if the caller already knows it and calls but you have caller ID, have them take the number down on paper for the authorities.

4) Anti Phishing Programs - there are a few licensed anti phishing programs that interact with most major firewalls. Get the latest one. These will have the names and locations of known phishing sites, as well as the programs commonly used by phishers to build their sites. These licensed programs also update themselves from their own secure websites on a constant basis to keep up to date with any changes and new information. This added security acts like a firewall or antivirus program but is dedicated to blocking, detecting, and tracing phishers.

What Kind of eMail Is Coming to Your child?

Internet Child Security: Monitoring Your Kid's Online Safety

Teaching our children online safety is every bit as important these days as teaching them the basics of "real world" physical security. The old adages of "don't talk to strangers" and other similar sayings now have their own electronic counterparts, and you should be aware of all of the possibilities to ensure the safety of your kids when they go on the Internet. Here are the major hazards of children going online, along with a few bits of advice on how to deal with them.

Hazardous Programs/Software Online - viruses, spyware, worms, and trojans are some of the major threatening software that can be encountered online. Having security programs that detect and block incoming threats isn't always enough. Since these programs can ride piggyback disguised as or attached to harmless looking email, make sure that your children never accept email from any sources they don't know, and even to reject ones with suspicious sounding names even from sources that they DO trust, as their friends' computers might have gotten infected and the emails sent out automatically by the viruses. On a related note, teach your kids the importance of maintaining a firewall and anti virus shield. Show them how to operate them, and tell them NEVER to turn it off just because the firewall may be doing something "inconvenient" like blocking a game site.

Verbal Abuse Online - whether in chat rooms, forums, clubs, and online gaming, there are enough vicious, small minded, stupid, and harmful people that might heap verbal abuse on your children, swearing at them or making sexual advances on them, or even striking at their religious or ethnic backgrounds. Teach your children that they do NOT have to put up with this online any more than they have to in real life. They should know how to get recordings or screenshots of the instances, and take them to you. You can then ensure your child's safety by contacting the moderator of the forum, game, site, etc. in question and having them ban the offending parties.

If the abuse is excessive, you can even opt for taking legal action against the person or people involved, just as you would push a slander and abuse charge if they did it on the street. The Internet's advantage in such cases is that screenshots and official records from the sites can be used as hard evidence, unlike real-life verbal abuse cases where the evidence is usually gleaned from reliable witnesses.

Phishing – let's review this again. Another danger online is the crime of phishing. This involves people contacting you or your children claiming to be something harmless like a bill collector, law enforcer, government employee, salesman, etc and attempting to get you or your children to give them sensitive information over the Internet. This usually involves things like

credit card numbers, home phone and address, social security numbers, etc. As in real life, the best defense against this is to teach your children to never divulge any information to someone they don't personally know, and to avoid giving out extra-sensitive information (credit card!) to anyone, even those they DO know.

One type of software that helps defend against these cases is the supervisor monitoring program. These packages are usually meant for office use to monitor the times a user logged into a computer, what sites they visited, which programs were run, what was downloaded and uploaded, and even what was typed. While this will not directly avoid phishing in case your kids DO give out information inadvertently, it WILL at least allow you to find out after the fact and to take appropriate legal measures using that hard evidence against the parties involved.

Stuff You Don't Want Them Seeing - lastly there are, sadly, many sites out there that we don't want our kids seeing. Aside from the obvious pornographic sites there are also ones involving graphic displays of extremes of violence, or have teachings and ideologies we'd rather not have our kids exposed to.

To prevent this, parental lock programs and timers can be used to limit which sites your children can visit and how long they can stay on the Internet. These types of software mesh perfectly with the supervisor monitoring program (mentioned in Phishing, above) to allow you to know what your children are doing online when they think you're not looking.

About Firewalls and Free Software

Free Firewalls and Children Protection Programs

The Internet is an established part of our world, and modern education has included it in the education of our children. Unlike past generations, where the Internet was as much a source of games and amusement as a tool for adults, these days our children are immersed in it. Given that it is a part of their daily lives at school, it naturally follows that we can't keep them from their computers at home so they can do research and homework on it.

With that in mind, we have to keep a close watch on the things our kids do online so that they don't unwittingly become security risks in this day and age of computer-related crimes.

There are two types of programs that will help our home security over the Internet immensely; the first is firewalls, which keep out viruses and spyware that our kids may accidentally touch on in the course of conducting their research.

The second is child safety software, which are programs especially geared towards helping parents monitor and control their children's online time.

Here are the top three free picks for firewalls and child safety programs you can download.

Firewalls

1) Comodo Firewall - one of the top picks among both free and fee based firewalls, comodo scans all incoming Internet traffic before actually allowing it to touch any other part of your PC. It's main feature is a program behavior analyzer that detects if programs have any unusual activity that may signal a virus or worm in the program. For inert viruses it also has a trojan protocol detector that is constantly updated online.

2) Kiero Personal Firewall - this is a software that has been reported by users to offer them minimal headache in operation and use. While its protections aren't as sturdy as some other firewall programs, it offers

reasonable defense. Its main strength is its ease of use, so that you can teach your children to operate it, giving them the benefits of learning Internet security early in life.

3) Zone Alarm - this is rated as a cross between comodo and kiero. It offers more security options than Kiero and is easier to use than comodo and is the most balanced choice between ease of use and security. Depending on your preferences, it can also be taught to your children, but it's advanced settings may actually cause them to mess up your firewall, so it might be a good idea to keep the operation of this software to yourself.

Child Security

1) EZ off - this program is essentially a time management software for your computer. It will automatically turn the PC on and off at scheduled intervals, allowing you to control how much time your children spend on the net. This is best used to keep your kids from playing video games past their bedtime. The timer also features a calendar and scheduler, so that you can even keep the PC running for set intervals when you're not at home.

2) Windows Supervisor - this is an office program that can also be used at home. It's main purpose is to monitor all logs made on the computer, so

that you will be able to tell not only WHEN your children access the Internet, you'll be able to tell what activity was running when they were there, including what sites they visited, files they up or downloaded, programs executed, and even keyboard typing done.

3) StopGame - for those who want to let their children enjoy the Internet from time to time, a less-strict version of EZ off is similar to a firewall in that it lets certain, specified programs and web sites be accessed at certain times of day by the computer. If your kids are, for example, doing homework from 6pm to 8pm and you let them have game time from 8pm to 10pm, you can set this program to allow them access to certain games (that you specify) from the 8 to 10 slot. Also, taking a cue from Windows Supervisor, it will be able to monitor past activity as far as the allowed game programs listed are concerned, as well as attempts made by your kids to access other sites.

About Abduction

All About Online Abduction

The fact that the Internet is rapidly expanding backs the notion that more people are regularly using the online medium. Thus, everyday, there are tons of reports over cyber-crimes committed by online predators worldwide.

Because the Internet is an open medium for people from all walks of life, you can't always prevent your kids from getting there. When logged on the Internet, your child can be exposed to a lot of dangers. There are many predators out there that are ready to feed on innocent children within the Internet.

The Internet is a place to meet people and expand a person's social circle. However, be reminded, and also remind your kids, that not all people you may meet online are 'friend material'. Like in actual life applications, you should never easily provide trust to anybody.

Online abduction is among the most popular cyber-crimes committed by scrupulous individuals over the Internet. It isn't surprising that there have already been reports of kids getting kidnapped by people they meet over the Internet. Abductors can't abduct your child online, but there are tactics that could help them do the dirty intentions.

Because kids are just starting out in life, they have to learn things and lessons in life the hard way. It is during the childhood and puberty years of kids that you should be able to extend your protection and guidance to your kids.

Some worse case scenarios of online abduction

To learn more about how online abductions are widely committed, it would be helpful if you would be informed about how the predators do their thing. Take note that online abduction strategies are alike in many ways, so by learning the usual worse case scenarios, you can understand the process better and prepare to prevent them from occurring.

Worse case scenario 1

Your child is logged online. Because almost all his friends are raving about friendster.com, MySpace.com and several other social networking sites, it is natural that he keeps his own account. Through the site, your child can interact with his friends through the in-site interactive features like private chats, emails, bulletins and posts.

Because social networking sites are social function systems, there are features that allow people to surf the entire system to meet new people. This is where the danger sets in. There might be individuals who would befriend your child. The individual may disguise themselves as another kid the same age as your child.

The process doesn't happen over night. Cyber criminals are so patient that they are willing to spend days, weeks, months or even years establishing the friendship with your child. When your child is at ease with the person, that is when the cyber criminal attacks.

The cyber criminal can ask your kid for an eyeball, wherein they would be meeting each other personally face to face. Most online abduction cases reported are committed this way. When the kid is out to take an eyeball with his friend, it turns out the meeting is a set up and the disguising friend will then abduct the kid.

Worse case scenario 2

In chat rooms and interactive channels, your kid might meet people who are out there to socialize so they could victimize innocent people. The cyber criminals might lure your kid into doing something that could compromise his safety, as well as your safety and the safety of all on your household.

The cyber criminal can ask your kid about addresses, credit card numbers and personal identification numbers on bank accounts. Since your kid is

unsuspecting and is treating his online friend with so much trust, he would be willing to disclose the information asked by his friend.

When your child divulges your address, the cyber criminal then will be able to track and monitor your kid and abduct him when there is a chance. The abductor might kidnap your kid when nobody's home except your child, or during the middle of the night when everybody is asleep.

What to do when your kid is abducted

The best thing to do when your child has been victimized by online abduction is to report the matter to the authorities. The police will extend their help in helping you find your missing child. Also retrieve the information on the Internet about your child's friends, who can be suspected of committing the cyber crime.

Keep your cool and do not panic. Experts are advising you not to give in to the demands of the abductor. If you do, you might be contributing to the continuity of such crimes. If you don't, give your full cooperation to the authorities.

Online abduction can be prevented if you educate your child about the dangers of meeting strangers on line. Do it now!

What About International Abduction?

Using the Criminal Justice System Against International Abduction

The times are truly changing. Because almost all essential transactions can now be coursed through the Internet, even crimes are emerging into new forms to underpin the rising popularity of the online medium. Let's explore this abduction problem further to include international situations.

Thus, you hear of numerous reported cases of cyber crimes, or crimes that are perpetuated through the Internet. Take note that criminals and law offenders are equally effective when they operate online as they operate personally during normal circumstances.

Online crimes are new to almost all nations and governments and there are still not enough legislations and international treaties that would appropriately deal with such unique crimes. Thus, the online predators or

perpetrators of crimes through the Internet are freely roaming the Web to find prospective prey.

Online abduction

In the United States alone, the volume of filed online abduction cases are on the rise. The US Department of Justice has revealed that in all abduction cases in the country, about a quarter had been perpetrated through emerging online technology.

About 49% of kidnapping incidences in the United States are committed by family members, when the child is abducted either by his dad or his mom. Such cases occur especially when the parents are separated.

On the average, about 27% of abduction cases in the country involve acquaintances or new friends of the child. Take note that the police identify online chat rooms and interaction as the prime venue where kids meet new friends, that lead to abduction. The remaining 23% of kidnapping incidences are committed by total strangers.

How is online abduction committed? The process can be very simple and suspicious, but still, many kids fall for the trap. The abductor gets in touch

with the child, befriends him or her, asks for personal details like address or invites the kid for a personal meeting, or popularly termed in online lingo as an eyeball.

The abduction of course isn't committed online, but the Internet becomes the facility that makes the crime possible. Criminals purposely meet kids over the Internet for the aim of kidnapping. They either disguise themselves as a boy or a girl who is of the same age as the prospective victim.

Experts and investigators analyze that the popular social networking sites are often the sites wherein strangers and kids meet. Online criminals target these sites, register to them and log in to them so they could meet kids who would be very easy to lure and convince.

What about international abduction?

International abduction is committed when the kidnapped child is taken abroad after being abducted. The criminal takes the child offshore so the parents can't easily trace their kids' location.

Also, international abduction somehow provides protection to the abductor. For one, federal police aren't as free to roam around and flex its muscles to

find the abducted child and the kidnapper. It takes time before the parents and the police figure out that the case was an international abduction.

You might be wondering how the abductor can take the child abroad. As you see, there are many ways a criminal can take a child without proper documents. Crossing land borders can be one, as well as processing a fake or fictional identification for the child.

You might be asking, "Does it really happen?" The answer would be, "Yes, a lot!"

How to pursue international abductors using the criminal justice system

The criminal justice system is primarily instituted to protect the rights and legal privileges of US citizens. If they have been aggrieved by foreigners, there can still be justice using this system.

In the case of international abduction, you will have to file reports to the police first. After establishing that the child has been taken abroad, that is the time you will be advised to pursue the criminal through the federal criminal justice system.

The US has extradition treaties with many countries. If the criminal is staying in a country that has an extradition agreement with the US, then the criminal will be apprehended and arrested and brought to the US for prosecution.

If there is none, the criminal justice system will cooperate with the country's justice system, so the respective justice system will prosecute the offender accordingly. This can be possible especially when the law provisions violated by the criminal are the same with the provisions he violated under US legislations.

Overall, it won't be an easy fight, but it will be worth it, if you want to get your child back. To prevent such problems, watch the online behavior and habits of your children and monitor the friends they make online.

Know Who Your Kids Are Online With

Knowing Who Your Kids Are With Online

The Internet is for everyone. All people will find the online medium useful because of all the resources. There are lots of educational information, entertainment and socialization going on and circulating within the Web.

Thus, your children will be more than willing to get online. Furthermore, they could also be forced to get into the Internet, because almost all their classmates and friends do so. Homework and research projects could also be done more easily, accurately and conveniently using Internet sources.

Because kids are kids, they still lack enough experience and insight to protect themselves from opportunists. No matter how smart and aggressive they can be, they can still fall vulnerable to the traps and dangers of online crimes and offenses.

If you are a responsible parent who have kids that are regularly visiting online sites, you should be assertive and firm in instituting several online safety measures to protect your kids. The volume of crimes and offenses done to children online is constantly increasing, so you should be protective enough to make sure your child doesn't fall a victim to online predators.

Cyber crimes

There are numerous cyber crimes committed against children online nowadays. Take note that these crimes and offenses are actually regular

crimes that took the form of online technology. Example of which is online abduction that we discussed in the two previous chapters.

Kidnapping is a problem in almost all countries throughout the years. But more recently, the first reported and celebrated cases of abduction done through the Internet have been taking the limelight. That is because in the past few years, people never imagined such crimes would be possibly perpetrated.

How is it committed? The criminal befriends the kid over the Internet, asks for personal details like addresses, or invites the kid for a personal meeting. The unsuspecting child, being a natural inquisitor and adventurer, might be going out of the house for an eyeball and voila, the abductor takes the opportunity to kidnap the child.

Other forms of online crimes are the online child pornography, identity theft and online child molestation and harassment. The Internet is full of pornographic materials that children shouldn't see. If unguided, your kids might cross onto one of these sites.

When a child sees porn and violent materials over the Internet, his mind is eventually being polluted. His concept about life could be altered, and he

would be aware of the concepts that shouldn't be exposed to him until the proper time. Thus, he could be exposed very early to sex.

Tracking your child's online friends

Almost all children across the globe are told by parents and guardians not to talk to strangers. However, online predators are aware of the instructions you give your child. So, these online predators cease to be strangers and instead disguise to be online individuals who are in desperate need for friends.

Your child might encounter them and be friends with them. When the criminal thinks he has befriended your child well, he then attacks. He might organize a personal meeting, or monitor your house and take the opportunity to abduct the child when nobody's around.

Experts advise that you should be very stringent and watchful when it comes to knowing who your kids are with online. Yes, you as the guardian of the kids must know who these online friends are. You should follow up and check out the identities of the online friends your kid has.

How could that be? It may not be easy, but you can do it. Some kids find it okay if the parents directly asks information about their friends. However, some kids won't find it acceptable because they perceive it as a clear invasion of privacy.

In such cases, watch over your child's online activities by becoming a simple spy. You can check the records of the computer to check out the sites your child has visited online. You should also ask the Internet service providers about safety pins and measures to prevent your child from accidentally and intentionally getting onto porn sites.

If you want to find out about the email communications of your child with his online friends, you could volunteer to create the email account for your child. Take note of the passwords. Or you could share the same email with your child.

That way, you could monitor what is going on and know the activities and motives of your kid's online friends. You could also get into several social networking sites where your kid has a membership. Constantly check out your kid's social network profile and the friends on his list.

It would be very advisable if you would take time to do the above measures to protect your child. The Internet is a wild jungle out there. Don't let your kid wander alone.

Know Who You Should Contact

Know Who You Should Contact

Children of the pre-teen years all the way up to the teens rarely play with toys anymore – certainly much less than those of the earlier generation, thanks to the advent and rise of modern technology, most notably the Internet. Games can be found on computers and the Internet, even for kids, which are most often the substitute for actual playing with other kids. Times have indeed changed with children preferring to interact online rather than for real.

While computers and the Internet are good sources of amusement and entertainment for children, dangers lurk around every imaginable “corner” of the Internet, from the actual gaming sites to hardcore pornography sites that can pop up with one simple click of the mouse.

Social networking sites like Friendster and MySpace, known to attract those of the younger generation, are also the haven for perpetrators looking for innocent, unsuspecting victims that they can find easy to trick, such as children, who are the most vulnerable.

As a parent, you need to find the various ways possible to protect your child from the dangers of the Internet, while still allowing him/her the privilege of exploring it. However, it is understandable that at times, the child can be secretive and will lie to his/her parents. Yes, he/she is only exposing him/herself to the dangers of the Internet, but a parent can only do so much when the child lies.

If all avenues of protection have been exhausted and the child still gets into Internet trouble, as a parent, you need to know who to call.

The National Center for Missing and Exploited Children is usually the agency that handles cases like these wherein the child is exploited by unknown perpetrators on the Internet. Perhaps the perpetrator sent or allowed the child to view pornographic materials, whether photo or video. Since this is bound to have a significant amount of psychological effect, the agency mentioned will help your child deal with that fact. The hotline for the National Center for Missing and Exploited Children is 1-800-843-5678.

If the act occurred on a social networking site such as MySpace or Friendster, you may try calling the site owners and/or operators and give the username of the perpetrator if you've managed to obtain it. Although this could be somewhat of a long shot (due to the fact that it is accessible from any computer in the world, including in countries without specific laws dealing with these situations), you could still try it as the very least these social networking sites could do is to ban the user from their sites.

Of course, if any sexual act, criminal activity, and/or suspicious behavior occurred, you have to notify the local law enforcement agencies. If the police are able to catch the perpetrator, it could prevent him from victimizing other children. Also, the police are very adept with modern technology and can catch a perpetrator during any criminal activity or just prior to.

It is also important to notify your Internet Service Provider. If a perpetrator tricks your child into going to a questionable site, you can have the ISP block that particular site and also warn them to warn the other clients of the said service provider. That way, the effect of the questionable site is greatly lessened.

Aside from the social agencies, law enforcement agencies, and others that will help in this problem, it is also good to inform other parents who are experiencing or will experience the same problem of a child spending a lot of time on the Internet.

Should your child be victimized, warn the other parents, whether they are the parents of your child's schoolmates, family friends, or those in social clubs, of the dangers of the Internet and how to prevent a child from being exploited. This will go a long way into helping solve a problem that affects the whole world.

Schools should also be notified, beginning with the school your child attends. Schools can give pep talks regarding the dangers of the Internet, what to do when faced with questionable circumstances, etc. Sometimes, schools have a way of reaching the children in ways parents can't.

Knowing who to contact will definitely help solve this world-wide problem of child exploitation via the Internet.

Chatrooms, Social Sites and Your Child

Chatrooms, social sites, and your child

Due to the emergence of modern technology, which includes computers and the Internet, loads of information can be easily accessed with one simple click of the mouse. A person can know the happenings in a place like China even if he/she is located thousands of miles away – like North America or Europe. Such is the power of the Internet. Unfortunately, there are dangers associated with it as well, especially for unsuspecting children.

Children, including those going into their adolescent years, are often fascinated with the thought of meeting new people through the Internet, especially via chat rooms and social sites (e.g. Friendster, MySpace, etc.).

While there is nothing wrong with social networking using technology as a means, it can be dangerous, particularly if someone finds out about the child's age and tries to exploit him/her into revealing unnecessary information. This is why it is important for parents to take good care of their children, more so in this so-called Age of Information.

One of the most reported cases of child exploitation in chat rooms is related to sexual exploitation. A perpetrator usually spends hours in a particular chat room that he thinks will interest children, waiting patiently for an

innocent child to talk to them. Some young girls (as is often the case) are more than willing to speak with seemingly friendly individuals, often for them to confide in and just share thoughts with. Little do these young ones know that the perpetrator is actually preparing them for sexual activity.

When the innocent child and the perpetrator get better acquainted via chat and/or instant messaging, the perpetrator gets more and more confident and begins to make advances, such as an "eyeball" (an actual meeting of the once virtual chatmates). This will eventually lead to an invitation to the perpetrator's place, where the actual sexual activity occurs.

The child may find it quite difficult to let go of the virtual relationship because he/she feels that there is an actual friendship going on, when in reality, the perpetrator is actually setting him/her up. As such, the child will more often than not reveal information that is usually not revealed to strangers or people hiding behind chat room nicknames. When this happens, the perpetrator can do a lot of things, such as robbing the family of the child, sexual activity, even to the extent of kidnap for ransom, and worse, murder.

A less serious threat that can occur (but nonetheless a threat) is acquiring viruses, spyware, and unwanted files through the chat room or social sites,

which will damage your computer and in some cases, break it down totally. Computer owners will find it a great hassle to be dealing with viruses, particularly if the infection is a deep one, and more so if they aren't adept at dealing with viruses and/or spyware. Sometimes, an anti-virus program isn't enough, especially if the user is a child who doesn't know that the files he/she might receive are infected.

This threat becomes more serious when the computer is used as a means of income, meaning a person works off of his computer. Should a computer break down due to a child's ignorance in the chat room, a lot of work could be lost, which will lead to loss of income, definitely something you don't want.

Another cause for concern is that the chat rooms and social sites are often times found with adult material on it. A child could possibly have his/her life changed forever if his/her morality is questioned and lost at such a young age. Nude pictures and videos aren't uncommon within such areas of the Internet, even though there are some sites that try to eliminate these.

Social sites and chatting is fine, so long as the children are kept away from the evils that are linked with these uses of the Internet. Should a child become exposed to these dangers, there is no telling what the overall effect

in his/her life would be. One way of parents protecting their children is by checking on them from time to time, especially when they are using the Internet, a powerful yet potentially dangerous tool.

Case Studies

Actual Case Studies of Kids on the Internet

As people are quickly becoming more and more dependent on technology for their everyday needs and desires, particularly the use of computers, business developers in the software industry have constantly tried to look for ways to take advantage of the trend, for their own profits and for the growth of the information technology industry as a whole.

Some of these include sites and software that are geared towards the younger generations, like public chat rooms and social networking sites. With the number of hits these receive daily, it is no question that these are things that children and adolescents of the present look for.

While social networking sites and chat rooms promote socializing with one another (even if it is mostly text), there are dangers that are associated with such. Some of these include exploitation, extortion, pornography, sexual

advances, etc., just to name a few. Perpetrators are aware most of the time that they are dealing with children and young adults, which is why they have more confidence to do the things they do – children are far easier to trick than adults.

Actual cases of these have happened, many of them in the United States. Just recently, a female teenager in Texas sued the site MySpace, a social networking site wherein a person can meet anyone from anywhere in the world. A MySpace page can be filled with pictures, videos, and other multimedia. A fake profile of a person can be made up easily, thanks to the power of computers and technology.

The lawsuit stemmed from the fact that this female teenager was sexually assaulted by an older teenager whom she met on MySpace. This man apparently put up a fake profile in MySpace, complete with fake pictures and fake data. Through this MySpace profile, they met through the Internet; he got a hold of her phone number, met each other personally and from there, the assault took place.

Incidentally, the girl's lawsuit didn't win. In order to prevent such incidents from occurring, one should exercise extreme caution, especially in chat rooms and social networking sites such as MySpace.

The case study proves that the danger on the Internet is ever present. However, that shouldn't deter children and adults from using the Internet freely – it is just important to exercise caution when doing so, something that this young girl apparently failed to do.

In addition, the girl herself lied about her age as well, claiming that she was an 18 year old when at that time, she was actually just 13. MySpace provides the privilege of using their site only for those 14 and above. Clearly, these actions show that the young girl didn't exercise caution and was exposing herself to danger by lying about her age and flirting with other male members older than her.

Other cases also involved instant messaging chat rooms and social networking sites, such as those when perpetrators tried to steal passwords and other valuable account information from MySpace users by sending them a fake HTML code (MySpace users can insert their own HTML code into their own profiles, for the matter of customization).

However, since some users are children, they are unknowingly exposing their accounts which could possibly expose their location, phone numbers, and other valuable information that should be kept private. Most of the

children don't understand HTML code and they don't know if the effect can be positive or negative.

There are many more cases in wherein children are taken advantage of through the Internet via chat rooms or social sites. As parents, it is your duty to protect and preserve your privacy from strangers, who could use your children to get what they want. Protecting them can sometimes mean restricting their Internet time, no matter how unpopular or how unconventional that seems nowadays.

With the case of the young girl, it can be seen that parents didn't exercise much caution as well because of the fact that she was able to get by pretending to be someone she was not. The chances of the act happening the way it did could have been lessened had the parents been more careful, as well as the girl herself.

What Solutions Are Available

Internet safety solutions for kids

Thanks to the birth and subsequent growth of information technology, particularly the Internet, millions of people from all over the world have access to each other. Chat rooms, social networking sites, and various Internet forums make this connection a virtual reality. Unfortunately, there is a bad side to all the wonders that the Internet showcases. One of these negatives is that children are exposed to various dangers that are very difficult to control.

You can't blame children for wanting to use the Internet for their own satisfaction. As it is often said (which is true), children copy adults around them, especially those that they look up to as role models – including their own parents. As such, when the kids see parents or their role models on TV playing with computers and the Internet, their curiosity is quickly aroused and they want to copy what these role models do. When they get a hold of the Internet, it is very difficult for them to look back.

One solution to this problem of constant exposure to the Internet's dangers is for the parents to regulate the Internet access of their children. Microsoft Windows has various user accounts in which a child can be included. All the administrator has to do is to limit the web sites that the selected user can access, and around half of the danger is already eliminated as a result of this. All it takes is a little computer knowledge from the parent.

Another way is the Internet security feature usually found within the Internet options in Windows. If a web site is accidentally visited and it contains explicit material that isn't suitable for children, a warning is displayed. This feature can be adjusted accordingly, from high security to low, with custom settings a possibility as well.

However, these measures are only half of the overall solution to the problem. It is very easy to say that this can be avoided if you, as a parent, completely disallow your child to use computers and/or the Internet. However, you also don't want to deprive your children of the technology that is within their generation. That is why educating your children on the dangers of the Internet is very essential – you need to teach them the benefits of using the Internet while making them aware of the potential dangers and bad things that can happen.

This is perhaps the best way – training your child. Not only will this be beneficial for them, as a parent, this is beneficial for you too. You will get close to your child, spend quality time with him/her, and share your life together during these moments. Along with that, you are teaching him/her to be responsible when using the Internet. Tell them that it is all right to surf the Internet, provided that an amount of caution must be exercised.

A common problem arises when children go into Internet chat rooms and social networking sites to interact with people who also do the same. However, there are many users out there who claim to be 15 years old, when in reality, they are around 20 years or older! These people take advantage of innocent children by pretending to be their friend, asking certain personal questions, and just giving the child confidence that they have a friend they can talk to. However, in real life, they are securing information that can be used against the child and his family.

This is one reason why teaching and training a child is important. Tell your child never to give out personal information, no matter how subtle it may be. Tell your child never to give a photo of himself or of his family and friends. It may be all right to meet new friends online, but tell your child never to go out and personally meet these so-called new friends without asking you parents to accompany him.

In extreme situations, a good solution would be to call in some help, if you don't think you can handle it. It is ok to admit that there are certain things that can be difficult to do. Remember that it is for the protection of your child. An example is if you want to place Internet restriction but don't know how to. It is perfectly fine to seek help.

When it comes to protecting your children, nothing can be repeated enough.

What To Teach Your Kids About the Internet

Teaching your kids about the Internet

The Internet is something that is very powerful. It provides a whole lot of information without much of the hassle associated with looking for them in an encyclopedia. Search engines have made looking for particular data easy – it is literally typing a few words and clicking. The Internet provides news in real time, even if the events going on are a few thousand miles away from where you are.

That being said, the Internet can also be dangerous. It is used to mass produce viruses and spread them around the whole world, able to affect any nation, especially those lacking in computer security. It can be used to hack into bank accounts and robbing money away from an unsuspecting owner. It can be used for terrorist functions. It is filled with dirty material – pornography, lewd acts, cursing, and crime.

The Internet is a place that you don't want your kids to go snooping around in, due to the dangers associated with it. This is why it is very important for parents to teach their kids about the wonders and dangers of the Internet, and not just one side only. Show them the whole thing; the big picture. A child who views something not suitable for him may have his life changed forever, something that even parents can't do anything about.

By teaching your kids properly, you are ensuring not only their safety, but the whole family's safety as well. Any information a child shares over the Internet to someone who is a total stranger can endanger the whole family.

Teach your kids never to share information, even if it is just a location (e.g. Los Angeles), a phone number, or even a name. Tell them that it is for the protection of the family.

Tell your kids never to give out passwords, even if they are shared with close friends. Passwords make it much easier for perpetrators to get what they want without the risk of getting caught and you never know, a close friend might have a slip of the tongue and give out the child's password to a total stranger. By then, if you are unsuspecting, the perpetrator may have gotten away with what he wanted already.

Teach your kids never to tolerate nor entertain cursing and other foul, rude language over the Internet. It is very easy to respond in a negative way to a person over the Internet since you can't be seen and you can be anywhere in the world. However, you might not know if the person the child curses is a computer expert or not, which could endanger your computer and data.

Allow your kids to have fun while at the same time restricting them. Giving them total freedom on the Internet will only lead to danger, as they are mostly innocent and unsuspecting of those who want to prey on children.

Place security measures on the Internet browser. Place the computer in the family room instead of the child's room so that you can check in on the child from time to time, which will be for his protection.

Tell your kids never to accept any file that is sent over the Internet without consulting you first. This file can be anything – a virus, a nude photo, a gross photo, a prank program, etc. It is better to exercise caution and prevent a negative occurrence rather than try to control any damage done after the file is executed.

Tell your kids to exercise caution in chat rooms and social networking sites. Tell them that there are perpetrators out there that lurk and wait for the

unsuspecting child to come and befriend them. These people ought to be treated as strangers. It would also be better if the child would tell the parents every time he meets a new "friend".

The Internet is very dangerous. A child can't hope to combat viruses, spyware, and lewd material on his own. It is far better to prevent that from ever occurring, and often times, teaching a child is the best way to go. Tell them of the rules, decorum, and other necessities in using the Internet. More importantly, tell them to have fun without the risk of exposing themselves.

Resources

List of Kid-Friendly Resources and Other Surfing Safety Tips for Parents

The Internet, for all intents and purposes, is ultimately a good thing, and it allows access to an unlimited amount of knowledge. The vast resources of information, however, are its strength and weakness at the same time. On one hand, the Internet gives your children every chance to learn about what he wishes to know, but it also gives them the chance to gain access to the wrong type of information at the same time.

Kid-Friendly Resources for Your Kids

Use of Kid-Friendly Search Engines

Sometimes, kids end up accidentally gaining access to websites that display information they shouldn't be exposed to. Unfortunately, although the intention wasn't there initially, exposure to such websites may be more than enough to catch their interest.

You can, however, reduce or prevent accidental exposure to such sites from happening by teaching your kids to use only kid-friendly search engines.

With such search engines, they can type whatever they want and they'll still end up at a website that's designed for their age. An example of such search engines is as follows:

Yahooligans (<http://kids.yahoo.com>) – created by Internet giant Yahoo for kid users, Yahooligans does not only offer a search engine database for them to use but access to games, music, movies, sports, jokes, and other educational and recreational activities as well.

KidsClick! (<http://www.kidsclick.org>) – This search engine is managed by the University of California and is based in Berkeley. It is also described as a web search created by librarians for kids.

Kids Net (<http://kids.net.au>) – This search engine is based in Australia.

AOL NetFind – A search engine by American Online for kid users.

Searchopolis – Another kid-friendly search engine.

You can also learn about more kid-friendly search engines in websites like Kids' Search Tools, Safe Kids, and Searching with Kids.

Filtering Search Options

Another way for you to reduce or prevent accidental exposure to adult content for your children is by monitoring each and every Internet session they have and making sure that you filter the search engine options before allowing them to use it. You can do these with search engines by Lycos, Ask Jeeves, and Go Network.

Other Educational Online Resources for Kids

Homework Central – This website provides categorized information regarding a broad number of topics. It's divided into three sub-categories: Homework Central Junior - which is meant for kids in primary school, Homework Central

– which is designed for people in middle and high school, and lastly Encyclopedia Central, which is dedicated for college and adult users.

Cybersmart – This is an US based online portal that teaches kids, teachers, and other school officials various ways for children to properly explore the Internet. Free tools and resources are provided to aid teachers in teaching Internet surfing safety.

Lycos – Another well-rounded website created for parents, teachers, and kids, The Kid Zone of Lycos can be divided into four zones: the Fun and Game Zones which provides recreational outlets, the New and Cool Zone (which is self-explanatory for kids), the Homework Zone – which provides “safe” websites containing information about a wide array of topics, and lastly is a zone that provides pertinent information for teachers, parents, and guardians alike.

Purple Moon – This is a website that’s primarily designed for young girls; it has a search engine and provides links to games, online discussions and projects, and informative resources.

Families Connect – If you wish to explore the Internet together with your children, you’ll achieve your goal more easily and in a more fun-filled way

through this website. The activities and options offered here are designed to allow families to become closer and learn about the Internet together at the same time.

Black Hole Gang – This place provides people an exciting, fun, and safe way for kids to learn about science. Among others, it gives kids the opportunity to play detective and uncover the mysteries of science.

Other Surfing Safety Tips for Kids

As much as possible, don't allow your child to surf the Internet alone. Kids are still kids, after all, and accidents do happen. You can't blame them entirely if they do end up gaining access to a website that contains adult content.

Make the filtered options for search engine results permanent.

And lastly, clearly explain to your kids the dangers of breaking "surfing rules" you've put down and its possible consequences.