



# Parents/Guardians + Kids + The Internet

## **What you need to know before allowing a child to go online**

Computers and the Internet seem like a great tool for both children and parents, and indeed, that's what it is. However, those of you that **often** spend time online know that certain people use the internet's unique anonymity and open communication to try to exploit other online users, in any way that they can. This can come in the form of spam, spyware, adware, scams, virus's, and hoaxes, amongst many other problems that we see and hear about every day. The regular, everyday adult computer user is always finding new ways to solve these problems and secure themselves against future attacks, usually with a great deal of success. These users are making the Internet a very safe place to be for those who take the time to practice being safe.

Sadly, with more and more homes having personal computers, exploiters have a new target - children - who are getting online **unsupervised** more and more frequently than ever before. Alongside increased E-Crime there has also been an alarming growth of online sexual solicitations of underage children. Chat rooms and web sites, such as My Space, fill up with sexual predators **everyday, many of which are only targeting underage children.** While an adult may be well guarded from such solicitations, **children are often ripe targets, especially when unsupervised.**

Online Predators are equivalent to "Stranger Danger", only these Predators come inside your home, without you knowing. You've taught your children not to talk to strangers, not to get into a strange car, not to take candy from strangers, look both ways before crossing the street, etc. Teaching your children online safety is something new that you **must** add to that list! You'll need to start by learning some things yourself, so that you can pass on accurate information to your children.

You're probably wondering what exactly it is that you need to learn and what is it that you can do, right? This small informational packet will help get you started and teach you the basics of online safety. This, easy to understand format, will consist of the most common types of questions that parents/guardians ask, a guide to checking your computer's online history, links to online sites where security software can be purchased, as well as links to 'safe' and informational web sites. Please take the time to read and learn about Online Predators, our children's lives are at risk.

# F.A.Q's

(Frequently Asked Questions)

**Q. My child is safe because he told me he doesn't "chat" or use "blogs", is this true?**

A. No. We all want to believe that our children always tell the truth, but without checking your child's computer history, you won't know for sure. You don't have to pry and you *can* give them some privacy to a certain extent but it is important to **supervise**. Also, just because a child hasn't "chatted" online or created a "blog", doesn't mean he/she won't in the future. If friends have a "blog", chances are he/she will eventually want to create one as well. Most kids are under the impression that if they only keep their friends as 'buddies', they won't encounter any strangers, which is absolutely untrue. Predators know their way around the Internet, perhaps better than you, if they want to find your child, they **will**. Anytime a child goes online they are at risk, which is why it is important they know the basic safety of 'surfing' online.

**Q. I work a lot of hours and it is impossible to constantly monitor what my child is doing online, what am I supposed to do?**

A. You have a few options. One is to purchase software that will monitor you child's computer use for you. Some programs will even send you an email, without your child's knowledge, informing you that your child is currently surfing a site that is not appropriate for children, or will pick up key words that you can program into the software. These programs are exceptionally helpful if your child will have access to the computer often while no adults are present. You can also put a password on your computer, so that your child cannot get online while you are not home. If you are deeply concerned your child may be talking to strangers online and you haven't purchased monitoring software, you can always take a main part of the computer to work with you, such as the power cord or hard drive. The most important step you can take to keep your children safe is to **KEEP THE COMPUTER IN A FAMILY ROOM!** Do not allow children to have computers, which have access to the Internet, in their bedrooms! If the computer is centrally located, the less trouble they'll get into knowing someone may walk by at any given time.

**Q. How can a stranger hurt my child through the computer? I don't understand.**

A. Obviously someone cannot literally reach through the computer and grab your child, but they can, and do, lure children out of their homes right into their hands. They can also find a child's location depending on what type of information your child has given out online. Many predators will attempt to meet with a child, in their own home when they know a parent isn't present. It is very important you tell your children to NEVER type anything personal on the Internet. Never give out their full name, address, phone number, school name, school mascot name, team name, or put their picture on a website. They should never MEET anyone they met online without.. your permission! Predators are slick in making children believe they are talking to a kid around

the same age. Children can completely avoid this problem simply by not talking to strangers online.

**Q. How do these Predators convince generally smart kids to trust them, even though they've never met in person?**

A. Predators find children that will communicate back and forth with them. Predators become the children's "friend", sometimes even "best friend". They know the right thing to say and when to say it. They may use words to make the child feel special or loved, such as calling the child "hun" or "baby", "sweetie" or saying "Luv ya" at the end of a chat. These are not normal things that a strange adult should be saying to a child. Children can be **very** vulnerable, and if the predator types just the right thing, the child is more than likely to believe him. Predators generally won't mention anything about meeting, talking on the phone, or anything in sexual nature until they are sure they can 'trust' the child not to tell anyone about their conversations. The predator becomes the child's 'friend' and will ask the child to promise not to tell anyone about his or her new 'friend'. They'll make up any type of lie to get that child under their 'control'. Many predators will even tell a child how to delete any archived conversations, history, saved pictures, emails, etc. Most are paranoid and will do everything they can to cover their tracks, as they are well aware that what they are doing is a **felony**. It's important to tell children to immediately tell an adult if a stranger is attempting contact with them online and do not respond back to the stranger.

**Q. How does an online predator strike up a conversation with a child and what types of things are said to the child?**

A. An online predator may find your child in a chat room, through an IM (Instant Message) program, through 'blogs', bulletin boards, and personal websites. They will attempt communication through any one of those utilities.

Generally, they'll just start with a simple IM saying something such as, "Hi! How are you today?" If the child has a photo online the predator may say something like "Wow, you are absolutely beautiful! Are you a model or somethin'?"

When chatting through an IM program or chat room, the most popular question is "ASL", which means age, sex, location. If the child replies back "13 female Mt. Prospect, IL" that gives the predator a huge lead as to where the child is located!

He may change the subject around a little for a few minutes, and then ask what the child's name is. The child says "John" or even "John Doe", now the predator has the child's first name, age, city and state they live in.

More into the conversation the predator asks, "What school do you go to?" The child responds with "My Mom told me never to tell anyone the name of my school!" The predator then plays 'buddy' and says, "That's ok, you don't have to tell me. Your Mom is right, it's dangerous out

there!” Now the child feels a little more comfortable with the predator because he/she is convinced the predator is afraid of dangerous things on the Internet as well.

More into the conversation the child mentions playing basketball. The predator jumps on that and inconspicuously adds, “I play basketball too! My mascot is a cute bear! What’s yours?” The child answers the question; not realizing the predator is prying information, “Hawks”. The predator now does a Google search for Hawks mascot, Mt. Prospect, IL and finds links to schools in the area that have that mascot. School, name, age, city and state are now all known about your child within a ten-minute time frame. If your child also had a photo of himself online, the predator can now easily find your child.

While that is extremely disturbing, the chat between a predator and a child can become of a sexual nature rather quickly. Once the predator feels comfortable with the child and vice versa, the predator will start asking questions such as “Are you a virgin?” or even “Do you get your female thing yet?” Predators do not censor what they say, the chats can and usually do get **extremely graphic** and many times the predator will even send the child a nude photo of himself, or ‘perform’ a sexual act on himself in front of his web cam, while the child watches.

This is just a small glimpse of the types of conversations between a minor and a predator. Keep in mind, the predator’s main goal is to meet up with the child with sexual intentions, they will say anything to accomplish their goal.

#### **Q. What exactly can an online predator be charged with?**

**A. Indecent solicitation of a minor. The exact IL state law is as follows:**

(720 ILCS 5/116) (from Ch. 38, par. 116) Sec. 116. Indecent solicitation of a child.

**(a)** A person of the age of 17 years and upwards commits the offense of indecent solicitation of a child if the person, with the intent that the offense of aggravated criminal sexual assault, criminal sexual assault, predatory criminal sexual assault of a child, or aggravated criminal sexual abuse be committed, knowingly solicits a child or one whom he or she believes to be a child to perform an act of sexual penetration or sexual conduct as defined in Section 1212 of this Code.

**(b)** Definitions. As used in this Section: "Solicit" means to command, authorize, urge, incite, request, or advise another to perform an act by any means including, but not limited to, in person, over the phone, in writing, by computer, or by advertisement of any kind. "Child" means a person under 17 years of age.

**(c)** Sentence. Indecent solicitation of a child is:

**(1)** a Class 1 felony when the act, if done, would be predatory criminal sexual assault of a child or aggravated criminal sexual assault;

**(2)** a Class 2 felony when the act, if done, would be criminal sexual assault;

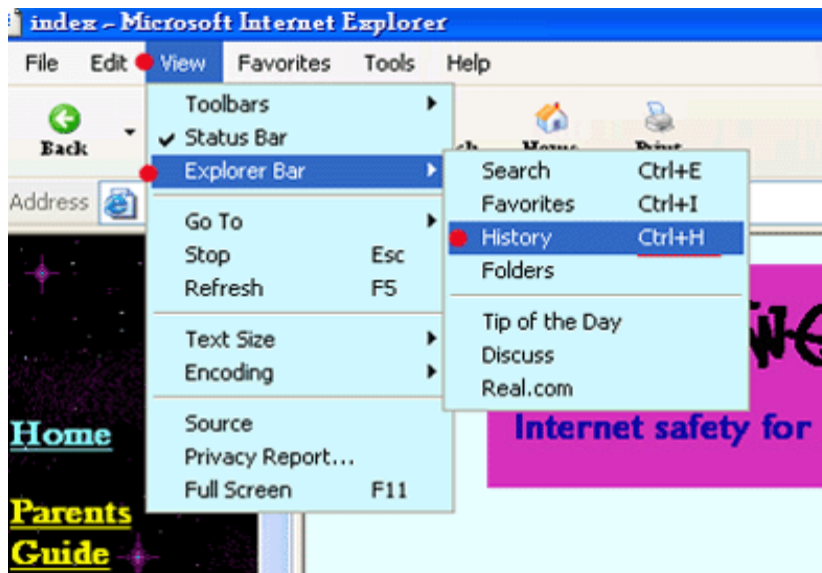
**(3)** a Class 3 felony when the act, if done, would be aggravated criminal sexual abuse.

(Source: P.A. 91□226, eff. 7□22□99.)

# Checking Online History

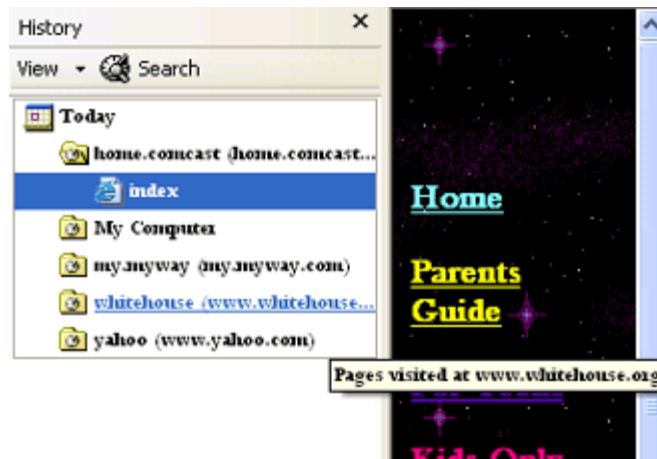
Tracking your computers history is fairly easy. Below is an example using the Internet Explorer browser.

- While Internet Explorer is open click “**View**” at the top of the toolbar.
- Next, click “**Explorer Bar**”
- Next click “**History**”



*A faster option is to hold down your “Ctrl” button and then tap the “H” button at the same time. You will get the same results as going through the above process.*

This will now open a small window to your left, showing all websites and programs that have been used. Depending upon how your computer is set to track history, you may see a few options such as “today” “yesterday” “one week ago”. You will notice that when you put your cursor over a website, it will have a line underneath it, which specifies a link. You can click on any of the websites or programs if you find the site questionable.



When looking through your browser history, pay attention for things like Yahoo! Profile pages, myspace.com, web personals, and dating sites. If your children are visiting these kinds of pages, it may indicate that they have been solicited by someone online or are attempting to meet others. Be even more concerned if you find that your child has posted their own profiles on these sites, especially dating sites, as this highly suggests they are using the internet as a medium to meet people (*making them the predatory pedophile's primary target*).

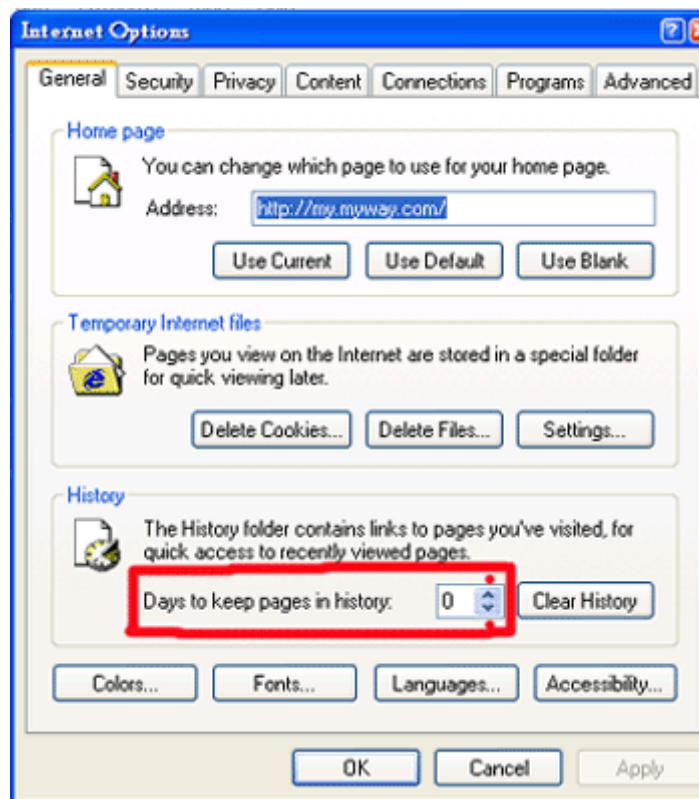
Also, watch for screen names that are of sexual nature, this may indicate your child is entering chat rooms posing as someone older. If your child does use a screen name to talk to friends, be sure to ask him/her what the screen name is and ask who is on their ‘buddy’ list. Children should not have buddies added to their list of people they don’t know!

If your screen is only showing “today”, then you need to change the amount of days to keep trace of your history. You can do that by simply by following these directions:

While Internet Explorer is open click “**Tools**”

Click “**Internet Options**”

The following window will then open.



The area circled is the amount of days history is recorded. In this example, the history is set to “0” days, which will not keep an accurate record of your computer history. Click the up and down arrows next to the “0” to change the number of days to track history. Depending on how frequent you will be able to check history, you may want to set it anywhere from 30-60 days. After you have changed the numbers click “Apply” then “OK”. Now your computer is set to track history for the new amount of days you set.

**Please be warned**, kids today are pretty smart with computers and they can delete the history, simply by clicking the “clear history” button. If you notice your child has been online and there is little or no history, chances are he/she has deleted the history. You may want to purchase special Parental software so that you can track history on your computer even if your child does use the “clear history” button. The next page will explain parental software and give you websites where you can purchase the software.

## Parental Software

Consider purchasing parental spy software if you feel comfortable with it. Such programs can capture images of your computer as it's being used, and log all keystrokes made to keep tabs on conversations. Safe surf programs and parental net blocks will prevent some sexual content from being accessed easily, and more importantly block the chat rooms where many solicitations can occur. Keep in mind that you should always abide by your own personal standards on parental privacy when weighing whether you should use such tools or not, and be prepared to address

questions by your child if confronted about the use of such tools. Also be sure to know that using such tools is not foolproof, as they can all be circumvented in one way or another. If exercising this option, make sure you are fully informed as to the functionality of the spy program before downloading/purchasing it, so you know it's proper use and are aware of how it works.

The next several pages will mention several parental software programs you can purchase along with a brief description of the product. You can also do a search online for “Parental Software” as there are many different products available today.

## Content Protect

[www.contentwatch.com](http://www.contentwatch.com)

Content Protect from Content Watch permits both remote management and remote reporting functions, and is the only product to offer these features. The remote function allows you to be anywhere in the world and be able to look at all activity logs as well as make any configuration changes. Anything you can do at home, you can also do at work or on vacation without the software. All you need is an Internet connection and password. There is also a graphical drill-down reporting of all detailed activity.

Additionally, Content Protect uses dynamic filtering; while a website might be blocked in the morning because of a violent story, once the website content changed, the site would no longer be blocked. Content Protect also permits a “warning” as well as a “blocking” function, essentially noting that something objectionable may be displayed, but permitting activity to continue, depending on filtering settings. Parents can be instantly notified via email, if attempts to objectionable material are attempted. If you as a parent want to access a blocked website, you can override the block as long as you have the password.

The program has been deemed both easy to use and easy to install. If installed on multiple computers, it keeps customized settings from one installation to the next. Few instances of over blocking (websites that should not have been blocked) and under blocking (websites that should have been blocked, but were not) were reported. One downside is that e-mail filtering is not available in Content Protect, so objectionable e-mails could still pass through the filters.

ContentProtect has been on the market for approximately a year and a half, yet is already one of the most highly regarded programs available. It is important to note, however, that its purchase must be renewed annually.

## CYBERsitter

[www.cybersitter.com](http://www.cybersitter.com)

CYBERsitter from Solid Oak Software is another excellent product. The over blocking (websites that should not have been blocked) and under blocking (websites that should have been blocked,

but were not) worked pretty well in most cases. One feature unique to CYBERSitter was that it was the only product to include a basic email-filtering option.

Additionally, CYBERSitter has the ability to scan your hard drive for objectionable material. It also will find any types of spying programs that may have been installed on your computer, either inadvertently or intentionally. CYBERSitter also had the most features out of any of the products reviewed. CYBERSitter was the only product to include a basic email-filtering feature, even though this feature wouldn't replace a typical Spam filtering product.

Setting it up can be tricky in order to get the browser to work in conjunction with the filtering. Making sure you have the correct settings with the "Default to Active Filtering Mode" turned on will make the application work smoothly. During the setup process, email notification does not work in Windows 2000 (but does in Windows XP).

CYBERSitter could consider as an improvement to have a message appear when something got blocked. When a blocked site is encountered, sometimes a blank browser appears with no text or message. Other times it displays a "Page Not Found" message. Some would argue this is a good feature, because children don't realize they are being filtered. This could be a little confusing until you get used to it. Overall, CYBERSitter is an excellent product with a few minor weaknesses. The purchase price is a one-time deal.

[NetNanny](http://www.netnanny.com)

[www.netnanny.com](http://www.netnanny.com)

Net Nanny from BioNet Systems LLC is a very good program. It is the most popular Internet filtering product in the marketplace. It has as many or more features than the other competitors. One aspect that Net Nanny stands out in is the ability to block online games, something the other competitors have not dealt with. The other is email filtering. Even though it is not an anti-Spam product, it does filter out objectionable content in an email while still allowing you to read the email without the filth.

Net Nanny states that it blocks and filters Instant Messaging, but tests did not show that this functioned. You can also view the restricted and permitted URLs and URL wildcards and add to or remove from these lists. Customization is also available for special words or phrases that you may want filtered.

The Internet blocking function that Net Nanny has implemented works differently depending on how you are surfing the web. If you type in a URL, it displays an error message. If you are using a search engine and type in an objectionable word, it just omits the results, without a block message.

Setup can be time-consuming, but is essentially simple.

Net Nanny has improved the filtering effectiveness as well as how they handle the blocking functions and warning functions. The over blocking (websites that should not have been blocked) worked extremely well, with a few exceptions. The under blocking (websites that should have been blocked, but were not) works very well with the English web sites, but non-English sites still occasionally slipped through. The purchase must be renewed annually.

## CyberPatrol

[www.cyberpatrol.com](http://www.cyberpatrol.com)

CyberPatrol from SurfControl is another good program. The profiling for individual family members could have had a few more features, but it did allow you to profile for sites and keywords. Compared to some other products, it was missing many features. Reporting of Internet activity was one important feature that was missing—in other words, if your children do something objectionable, CyberPatrol won't notify you of this. More problematic is that when a website or Instant Messenger is blocked, there is no immediate override function; instead, proxy settings have to be put into place.

Setup is simplistic, but problems have been reported regarding the need to reboot twice during setup.

The under blocking feature (websites that should have been blocked, but were not) works well in most cases. The program does allow quite a few foreign objectionable sites through its filtering mechanism. Another concern is when a website is “allowed” through, any link on the website going to any other website was allowed as well, even if it should have been blocked. The over blocking features (websites that should not have been blocked) work extremely well. This software, too, is an annual subscription price.

## Cyber Sentinel

[www.cyber-sentinel.net](http://www.cyber-sentinel.net)

Cyber Sentinel is another good product. The product has a number of options as far as setting up how you want blocked sites handled; either blocked, warned, closing of the browser, capturing a copy of the screen, or a combination of these. You need to look closely at these options to make sure the behavior of the application is what you are expecting.

There are no profiles so you don't have a choice to set up the application differently for the parents as opposed to the children. There is no real reporting function. You do have the ability to look at screen captures of various blocked sites. The screen capture function is a little cumbersome to use. Other than that, it's a fairly easy program. Installation and setup is simple.

Over blocking/Under blocking is good, but not great. It allows a number of sites through that it should have caught, especially in the foreign language websites.

Overall, a good product that is easy to use; again, the software is an annual subscription.

Again, there are many types of parental software programs available today with different features that may suit your personal needs. The programs listed above are just a few to give you an example of what exactly parental software can do for you as well as giving you a brief overview of some programs. Parental software is an extremely useful tool in helping monitor your child's online activities.

## Must see sites

The following lists a few sites where you can obtain more information about online safety and general information about using the World Wide Web.

[www.software4parents.com](http://www.software4parents.com)

[kids.getnetwise.org](http://kids.getnetwise.org)

<http://www.khalsaweb.com/internetarticles/childsafety.htm>

[http://www.icra.org/\\_en/parents/](http://www.icra.org/_en/parents/)

[http://www.safekids.com/parent\\_guidelines.htm](http://www.safekids.com/parent_guidelines.htm)

<http://www.fbi.gov/publications/pguide/pguide.htm>

<http://www.familyguidebook.com/pedophile.html>

<http://www.childseeknetwork.com/>

For additional online information please visit the original Webmomz site:

**<http://devoted.to/kids>**

This site will show information given in this packet along with additional information, a forum to ask questions, kids page, teen page, safe sites for kids to surf, and much more! The more you know the safer your child will be during his/her online experience.