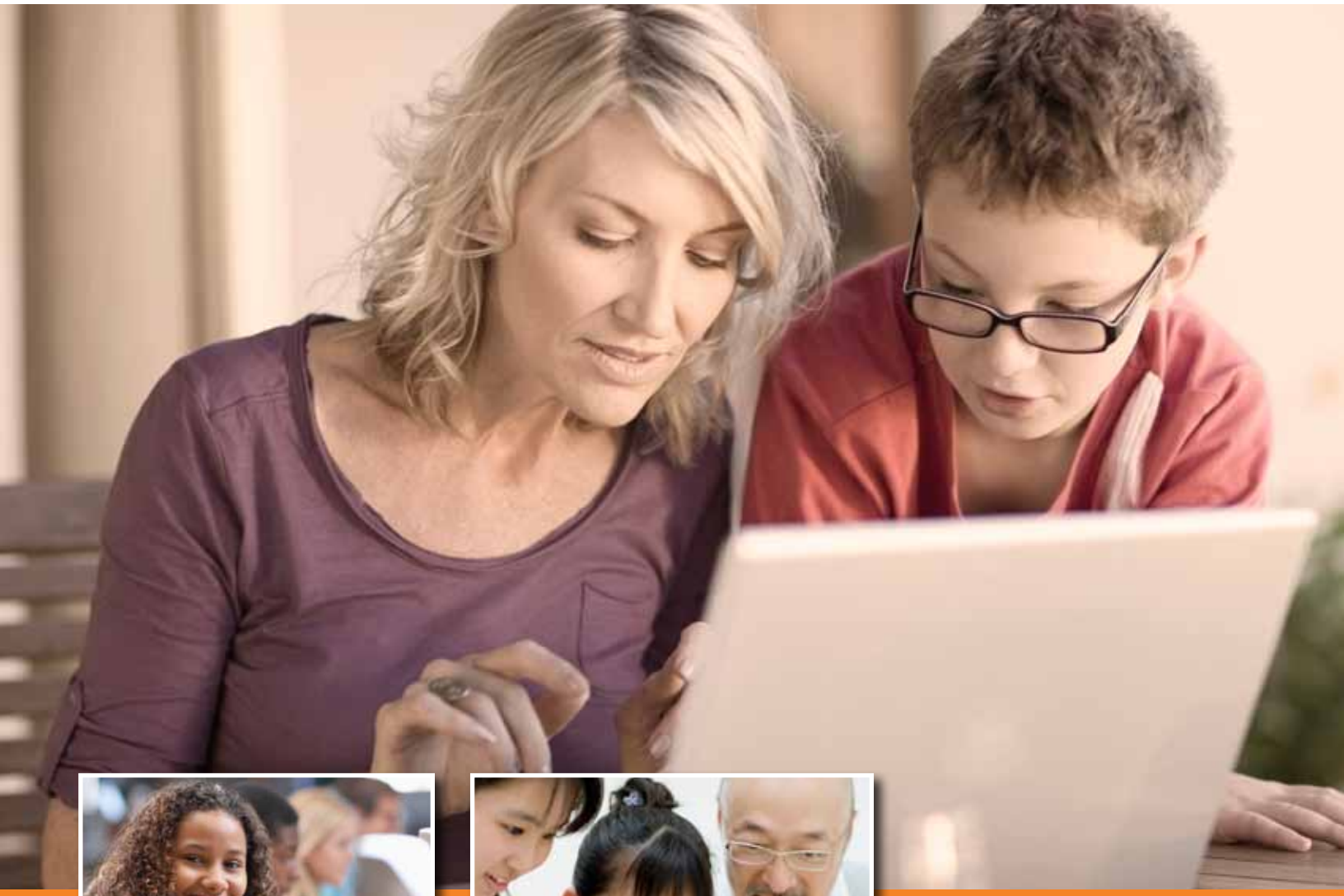
Internet Safety for Parents



Net Nanny

Introduction

The Internet is the most innovative invention of our time. If offers a wealth of information and resources in a split second. It is also a source of potentially dangerous content and images that can emotionally impact children and change the course of their future.

This document is designed to help parents keep up with the changing landscape of the online world. Every day has a new phishing technique, a new online predator, and a new cyberbully that is more savvy than the last.

Software and techniques that protected kids a few years ago are now useless, but a parent's desire to protect kids is still the same. There are countless websites and resources online to help parents become aware of new dangers; the trick is keeping up and learning the solutions that keep children safe.

In this document, there are four sections to inform you about the following issues:

- **Dangers of the Internet**
- **Circumvention**
- **Solutions**
- **Parental Controls**

Our goal is to inform you about the problems and solutions available today.

Thank you.

ContentWatch, *makers of Net Nanny*

Table of Contents

July 2012

ContentWatch Inc.
6949 High Tech Drive
Salt Lake City, Utah 84047

Section I: Dangers of the Internet

Pornography

Suffice it to say, pornography is readily available on the Internet. How big is the problem? Of all search engine requests, 25 percent are about pornographic topics.

The pornography industry is well-funded and will continue to thrive. If you consolidated all pornography companies into one entity, it would generate more money than the following companies combined: Apple, Google, Amazon, Netflix, eBay, Microsoft, Yahoo, and Earthlink.

Interestingly enough, the U.S. produces 89 percent of all pornographic web pages and they are in English.

Pornography is readily available and accidental exposure is occurring at younger and younger ages as children spend more time online. In most cases, pornography is deemed legal, with the exception of child pornography.

Pornography has undergone an evolution over the past few decades. Years ago, a pin-up girl was initially considered pornographic. Now, those images are tame compared to today's standards. In fact, you can view soft pornography on network TV.

Just as pornography has evolved, so can the mind. Studies show the mind degrades when subjected to shocking images. In essence, you can acquire a taste for images that initially would have troubled you.

Addiction

Food and sexuality affect the same reward system in the brain as drugs and alcohol.

Pornography reacts in the brain by increasing adrenaline, dopamine, and a bonding hormone (vasopressin in men and oxytocin in women).

Pornography has been found to be more addicting than drugs and alcohol.

Grooming and Cyberstalking

Child predators don't just hang out around playgrounds anymore: they pursue kids online. The process of finding and luring children online is known as "grooming" or cyberstalking.

Grooming takes place most often on social networking sites like Facebook or chat rooms. Chat rooms are commonly accessed in online games and through instant messaging (IM) accounts. Groomers pretend to be someone they are not. They know pop culture and other subjects of interest to their target. They use this information to connect with children online. Kids may engage in an online friendship with a complete stranger.

Once a relationship of trust has been established, a sexual predator will begin to test the waters by making sexual comments, suggest a face-to-face meeting, or request the child send a nude photo. If a child agrees to a meeting, he or she may not tell parents.

A victim of grooming is likely to not tell parents about what happens online as they feel responsible and guilty for the outcome.

In some cases, such online relationships have evolved into kidnapping, sexual abuse, or worse.

Cyberbullying

Cyber bulling, or bullying using online methods, is on the rise. The issue is more common among girls than boys, but both participate.

The anonymity of the Web encourages the behavior. Some states, such as California, have passed laws allowing a school to suspend a student caught cyberbullying.

Cyberbullying is a dangerous activity that can dramatically impact a child's self-esteem. It can lead to depression, self-doubt, and even suicide. As a result, angels on the playground can turn into bullies online, and the targets of this activity can be negatively impacted.

Cyberbullies may create anonymous Facebook pages or email accounts so they cannot be identified, and the lack of personal accountability can make a personal attack more extreme.

A victim of cyberbullying is likely to not tell parents as they feel ashamed for what has happened.

Signs of cyberbullying are similar to those found on the school playground: a child may become emotionally withdrawn or depressed.

Examples of cyberbullying language:

- I'm gonna kick your trash.
- I'm gonna throw you a beatin'.
- I will hurt you.
- You suck.

Web Search Gone Awry

Search engines are valuable tools that help find needed information online. However, they may not always yield the intended search results.

In fact, search results may reveal inappropriate images or sites.

Searching for things as innocent as "fast cars" can yield inappropriate images with links to inappropriate sites. What's worse, pornography companies often use words that are closely related to commonly-used innocent words just to catch a child.

Identity Theft

Identity theft occurs when an individual takes enough pertinent information to assume the identity of someone else. Because so much is shared online through social media, identity thieves have an easier job than ever.

Thieves will work for social media companies to gather as much information as possible about people. If an individual is not careful, identity thieves will be able to take out loans, credit cards, and access bank accounts.

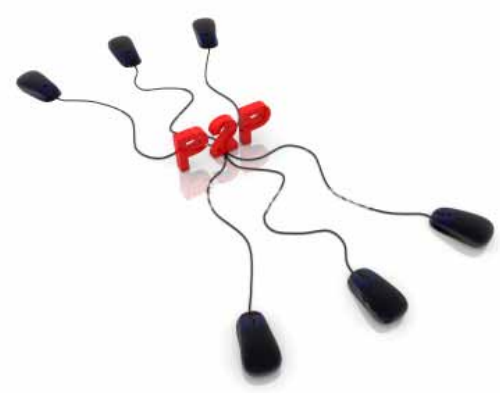
Phishing is the practice of sending fraudulent emails claiming to be a legitimate source with the goal to get the recipient to reveal personal information. A child may think they are doing a good thing by supplying their home address, phone number and birth date, but unless they are careful, they will give away their identity.

Peer-to-Peer File Sharing

Napster made peer-to-peer file sharing a craze in years past. Peer-to-peer file sharing software allows you to share the contents of your computer hard drive with anyone else on the same network. Most peer-to-peer programs are established to share music, photos, videos, movies, and more.

Children can use peer-to-peer file sharing to download content that may be infected with inappropriate content or viruses that can aid predators in finding your child's location or in hacking your identity.

The porn industry has recently made progress in halting peer-to-peer sharing of pornographic material, but this is still a very popular way to share inappropriate content.



Unless a filtering software program is equipped to block peer-to-peer sites, your child may be compromising your identity or copying inappropriate or copyrighted content without your knowledge.

Social Networking

Social networking sites can be fun and very interactive. However, they are also a showcase for inappropriate content, including pornography.

On Facebook, 47 percent of users have profanity on their page and sex-related links are shared 90 percent more than average. Oddly enough, 25 percent of households don't use privacy controls for Facebook.

At the same time, there are documented cases, for example, showing that future employment can be jeopardized based on what is posted on social networking sites.

Employers increasingly research candidates' profiles to make hiring decisions. Not knowing how your children portray themselves can be a risk to their future.

Section II: Circumvention

As every parent knows, independence becomes more and more important to children as they grow. Sometimes, teenage kids who are particularly curious will circumvent parental controls put in place.

In this section we discuss ways in which kids try to beat the system. By learning to recognize their tactics, you will have the opportunity to help keep them safe, as well as in compliance with family values.

Foreign Language Search

Unless foreign languages have been programmed into your content filter, children may be able to access whatever they like by switching to another language, like Spanish. Once this secret is discovered, language classes at school can become very popular.

Image Search

Google's image results come with a default for filtering images. This default is mid-level and will not typically reveal pornographic images. However, if the setting has been changed to turn off Safe Search filtering, then children may see pornographic images without going to a pornographic webpage.

SafeSearch

Google has a feature called "SafeSearch" which allows you to indicate how much explicit sexual content you wish to allow during a Google search.

If signed in to your account, SafeSearch can be accessed in the Search settings menu. If not signed in, to access, you have to do a Google search (on any topic) first. The Search Results screen will include a gear icon in the upper right corner of the page and it will be next to a box that shows the "Safe Search" status for your browser. You can choose to have SafeSearch on "strict," "moderate," or Off. This feature assists in establishing additional restrictions on Google searches – to ensure more appropriate results.

Proxy Web Sites

Another common way for teens to get around web filters is to use what are known as proxy web sites. A proxy web site is like a web page within a web page.

Proxy web sites are made readily available at no cost by hundreds of individuals and companies each day.

Proxies are designed with the sole purpose to allow users to surf the web without being tracked, monitored, blocked, or filtered. Proxy web pages circumvent Web filters. They are commonly used at school and home.

There are two methods to proxy web surfing: 1. proxy sites and 2. proxy servers.

Proxy sites support web access within a webpage. Browsing history reports do not capture sites visited within proxy sites, and most filters do not block proxy sites or the pages that appear in them. To see what a proxy web site looks like, search for them on Google where hundreds if not thousands will appear.

Servers

Savvy computer users are able to go to their Internet connection settings, and tell their server to go to another server outside the computer, somewhere in cyberspace. Through that external server, they can go anywhere online without being tracked, monitored, or filtered. The only thing your Internet history or parental control will see is traffic to the server, not where they actually go online.

User-generated Content

Wikis and blogs are created by average people and by others who are not so innocent. We refer to these sites as user-generated content. The most popular wiki is www.wikipedia.com.

Other sources of user-generated content are blogs, which are mainstream and are managed and sponsored by hundreds of thousands of eager web writers.

Several researchers feel that material on Wikis and blogs can be more accurate than information found in encyclopedias or other researching tools—making them valuable for education.

User-generated web sites are not normally monitored for objectionable content. And, these resources can't be monitored in real-time by most web filters. Most web filters recognize a Wiki or blog as a valuable source of information without validating the type information being shared. To truly monitor online activity, a computer or device needs a real-time web filter.

Web Access through Various Devices

Fortunately and unfortunately, the desktop is not the only means to access the Internet. Kids can go online via smart phones, tablets, gaming systems (Xbox 360, PlayStation 3, and Wii), iPods, TVs, and even Nintendo DS. Installing and/or using parental controls on all these devices will help ensure that your child is most protected.

Facebook Aliases

Parents may not know that kids can create Facebook aliases, which cannot be seen or found. An alias is simply a 'dummy' Facebook page created to which kids will steer their parents; meanwhile, the real Facebook page is only divulged to friends.

These aliases are used to keep parents out of the loop with online activity, protecting secrets that may put kids in danger.

Computer Admin Rights

Giving children access to a computer with open administrator rights is a common mistake – this will allow them to potentially uninstall web-filtering or other software. Knowing that uninstalling the software may attract attention, kids may simply deactivate the filter while online.

This will allow them to go anywhere they like, and parents will have no way of knowing what their kids have been doing. Admin Rights are set up at the operating systems level. Check your Windows or Mac operating system documentation for instructions.

IP Address

IP Addresses are used like a street address for web pages on the Internet. As an illustration, if a letter is mailed to the White House, the postmaster will know where you're sending your letter and it will arrive on the president's door. You can also mail the letter to 1600 Pennsylvania Ave NW Washington D.C., 20500-0004, which will also arrive at the president's door.

"White House" is like a web address (i.e. www.playboy.com). An IP address is like the street address, 1600 Pennsylvania Ave. The IP address for Playboy is 216.163.137.68. If you type this into your Internet address bar, you will go straight to www.playboy.com as if you had typed it out.

Using a website's IP address to bypass a web filter is an easy way to gain access to inappropriate web pages. Most web filters do not block IP addresses, which can be found simply by doing a Google search.

Pornography on YouTube

There is pornography to be found on YouTube, and few filters are able to screen the bad from the good. Even if the content is not hardcore, there are millions of videos you may not want your kids to see.

There are also filter settings built into YouTube that help screen the kinds of material your kids can watch.

Higher quality parental control solutions such as Net Nanny automatically configure these controls to the highest setting, protecting your kids from any inappropriate content.

Mashup Sites

Mashup sites are popular for people who like to have information from several sites but don't want to take the time to visit these separate sites. They are kind of like a dashboard in a car, with several sources of information on one easy-to-read screen.

Some of these sites include iGoogle and MySpace. Users are able to customize their mashup page to include headings from news sites, weather sites, online games, and other websites.

The problem is that most Internet filters are not able to discriminate between appropriate and inappropriate content on mashup sites.

Filters that do not scan page content will only look at the domain name and ignore what's actually on the page.

HTTPS

There are two kinds of web page addresses: http and https. Http sites are not secured but https sites are secured (hence the 's' in the name).

Being "secured" simply means that people would not be able to capture your private information from an https site.

Https sites secure our credit card information when making purchases online and our banking transactions. You may notice an https URL in sites like Amazon.com or when viewing your bank accounts.

The bad thing about https sites is that they encrypt pages to the point where most Internet filters will not be able to see the content of a page.

The most common pornographic sites are blacklisted, so those won't make it through most filters. However, a lesser-known porn https site may be able to sneak under the radar because of its encryption.

Section III: Solutions

There is no single solution that will keep your kids safe online. In order to maximize Internet safety, a collection of solutions is necessary.

Many solutions will be aggregated in one software program, but software and privacy protection will not be enough to keep you and yours safe. The following are important features and ways to stay safe.

Monitoring

A woman in New York using Net Nanny was able to help police capture and prosecute an online predator who stalked her daughter.

The monitoring tools captured the chat conversations between the man and her daughter and provided enough evidence in court to put the predator in jail.

Monitoring software tracks and records what users do on their computer, including online activity. Some software includes a keystroke tracker that reports on every keystroke a user my hit, making it impossible for users to cover their tracks by clearing Internet histories, chat conversations, etc.

Keystroke monitors can also be useful when capturing passwords to accounts your kids do not want you to know about.

Monitors can be purchased as a single feature or as part of a bundle with content filters. The good thing about monitors is that they report on where your children go and what your children do online, even if they are using a foreign language to bypass your Internet filter.

If a child is able to circumvent the filtering software, their behavior is still tracked so parents can know where they go. Some monitors capture instant messaging conversations. This can be especially helpful identifying cyber bullies and groomers. Some monitors can also track social networking activity.

Content Filtering

Content Filtering is the most common form of parental control on the Internet. The purpose is to block inappropriate web pages from users. Most content filtering software is based on a pre-categorized list of web sites. All web sites in the world are visited and categorized as "news," "entertainment," "pornography," "sports," and so on.

A few content filters, such as Net Nanny, use technology to analyze each web page visited based on key words, on-the-fly, to determine the category of content. Categorization is done to allow you to target your child's appropriate use of the Web.

Reporting and Alerting

As busy as life can be, there are few people who have the time or interest in reading every online conversation and looking at every page their children go to online.

Alerts typically come in the form of emails generated and sent to parents when certain conditions occur, such as when grooming (sexual predator) language is being used in a chat session.

Reports are also available to show daily, weekly, or monthly activity. Reports can be sent to an email address or viewed from a web browser.

Old Fashioned Parenting

Nothing beats good old-fashioned parenting techniques. Talking with your kids is the most important way to keep your kids safe. Being upfront with your kids about the dangers online will help them understand and appreciate the tools put in place to protect them.

It is also important to set up boundaries with your kids so they know what is and isn't appropriate in your home. Keeping your computer in a central location in the home will also help.

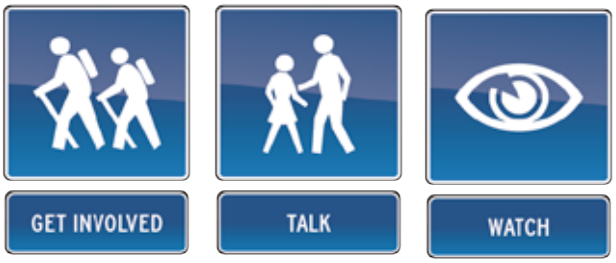
Time Limits

Another way to help protect your kids online is to set up time limit controls so that they can only access the Internet during certain times of the day and for a limited amount of time per day or week.

If kids know they have a limited amount of time to use the Internet, they will be less likely to engage in time-wasting activity. Most operating systems offer time controls, and some content filters include time controls.

Reporting an Online Predator

The adage, "It takes a village to raise a child," could never be more true than online. Sometimes it is better to report suspicious activity before things get too far.



Monitoring tools can help parents be aware of online activity, but once an online predator is identified, now what?

There is a Web Browser Pedophile Reporter Plug-in you can install on your browser. This web browser plug-in can be easily installed in all the popular web browsers on Mac and Windows computers. When installed, it places a small button at the top right of your web browser. When you're on a profile page of the individual you think is grooming your child, click the button to send the webpage to an investigator.

It also opens up an email you can put additional information in to send on to the investigator. It is simple enough to use that you could teach your child how to use it, so he or she can send an immediate report if he or she feels like grooming is occurring.

There is also The Child Predator CyberTipline. This tool, while not as easy to use as the web browser plug-in, is backed by the National Center for Missing and Exploited Children. It provides a very detailed reporting tool that forwards your tips to law enforcement.

It is important to remember that these reporting methods should only be used to report "potential" child predators. If you have any evidence that child grooming is occurring, you need to contact your local law enforcement immediately.

If they don't take any action on your report, take it to a higher level and contact your local FBI offices.

Section IV: Parental Controls

Though parental controls are important to help implement Internet safety, they can be frustrating. Whether the parental controls filter too much and block innocent sites or don't filter enough and allow some things to get through, it is important to become familiar with all the features and settings available with your solution before uninstalling.

If too many web pages get blocked, your filter may be set with very high restrictions. If too many sites get through, your filter may be set too low.

Filters will mostly categorize content on the side of caution, assuming it is better to make a mistake blocking a site rather than letting it through.

Most filters come with override settings that let you access a blocked site by putting in an administrative password. This is intended for sites that have been mistakenly blocked, to allow someone to grant permission to the user.

Before paying for a solution, use a free trial. Most Internet filters provide a free trial so you can get to know their product.

We recommend you go to reputable third-party software review sites, such as www.TopTenReviews.com to evaluate the type of parental control software you need.

How Internet Filters Work

Most Internet filters use large databases of URLs to categorize web sites. Under that scenario, web sites are pre-categorized into many categories such as entertainment, news, pornography, alcohol, gambling, blogs, wikis, health, lingerie, weapons, hate, violence, etc. These large URL databases are pre-categorized by machine and some are categorized after human review.

However, the sheer magnitude of the number of web sites on the Internet makes pre-categorization difficult. The challenge with having predefined URL lists is that web sites can change daily, web sites are created daily, blog sites or wikis can contain objectionable content, and a normally benign web site like Netflix can contain objectionable content in a rotating banner.

Net Nanny uses a unique technology called Dynamic Contextual Analysis (DCA). DCA categorizes each web site in real-time, as you type in the URL into your browser. Using text, html tags, and metadata, our rules engine determines the content of a web site using over 10,000 rules that give the DCA engine very strong categorization capabilities.

Net Nanny considers slang, acronyms, abbreviations, and modern language to determine content. DCA doesn't work on all-image web sites, but those are very few. Even all-image sites use enough text to describe or name images that we can detect the content.

Conclusion

At ContentWatch, we are proud of our flagship product, Net Nanny. Net Nanny has become an industry leader over the years, becoming a brand that works as much as a verb as a noun. At the end of this booklet, you can review a list of features developed to make your family's Internet safety as carefree as possible.

We do the heavy lifting for you, so that all you have to do is talk to your kids and be there when they need you.

Russ Warner
CEO, ContentWatch

Appendix

Net Nanny Features

- Blocks Pictures, Forums and Blogs
- Keyword Blocking
- Blocks Pornography
- Remote Management
- PC Game Blocking
- IM Alert & Analysis
- Internet Use Time Controls
- Integration with Popular Search Engines
- Filter Alerts Sent to Your Cell Phone
- Customizable “Allowed” or “Blocked” Lists
- Monitors Web Usage
- Safe Search Controls
- Social Networking Monitor
- Blocks email and IM
- Blocks Peer to Peer Sites