

Parental Control

By Govind Rammurthy – MD and CEO – MicroWorld Technologies Inc.

The Internet provides a window to our Universe, bringing its wonders to your desktop. There is unfortunately, its dark side, with harmful content that your child should not be exposed to. This white paper provides information about different types of threats your child faces every time it logs on to the Internet and suggests key features that good Parental Control software should have.

What threats await your child

The Internet is a vast repository of information - informative, helpful but sometimes harmful. When your child sees harmful content, the effect on its mind is traumatic. Given below are some probable threats that the child can be exposed to:

- **Porn:** First in the list is Porn. There are thousands of sites that offer Porn. These sites are easily accessible with just a mouse click.
- **Gambling:** There are many sites that offer online gambling.
- **Drugs:** Sites that give information on how to procure and use drugs.
- **Violence:** These sites promote racial hatred and spread inflammatory messages that incite a tender mind to turn to violence. Some sites provide information to procure or manufacture dangerous weapons.
- **Predators:** These are depraved and mentally sick people who masquerade as children and well wishers. They try to entice children by promising them goodies.

How your child falls a prey

Each day sees about 10,000 new sites coming up. Majority of them have Pornographic orientation. Harmful content can be accessed in many ways. Your child seeks some of them unwittingly and some reach your child by evil design. Given below are a few ways in which this happens:

Search Engines

Search engines allow you to enter a key word and search for related websites. The results may run into many pages. Results on the first few pages are refined to your query. Later pages display results somewhat related to your original query. These pages may carry harmful or sexual content.

For e.g.: Open google and type **toons** in the search bar. The first page displays genuine stuff. The next few pages start giving links to sexual content. Now what perverted mind thought of the idea

of creating toons with a sexual theme is beyond the scope of this white paper. But the stuff is there within easy reach of your child.

Many good and innocent words in English have been 'conferred' a Sexual status. A child searching for 'gay summer vacations' might find some very disgusting content, not related to what it wanted.

2) Special Interest Sites: Your child may be an avid gamer. Many sites offer free downloads of games. A majority of them are genuine and offer freebies, demos, software, etc. all perfectly legitimate. Demos are limited version games and offer only a few levels or options for playing. The child soon masters the demo and wants more. By word of mouth or even through the search engine it comes to know of '**Cracks**'.

Cracks are illegal copies of games and usually stored in Porn sites. While cracks are available to the determined seeker, they ask for your name and other details. Your innocent child may give out its real name and other details. These details may be picked up by perverts who entice the child with inducements.

3) Chat Rooms: While chatting is a good way to make instant friends, it is anonymous. A person who claims to be Anne, aged 8 years from New York, it might very well be Hannibal, aged 60. Such perverts strike a quick rapport with the child and will offer anything the child wants just to make physical contact.

4) Anonymizers: Kids today have become smart. They probably know more about computers than you. Anonymizers provide means to beat some of the common parental control software. These are software applications and sites that remove your systems identifying features when you access web sites. They act like gateways to Porn and other sites. Content from the accessed sites is jumbled and given to you. The normal parental control software cannot filter out such data.

5) Dialers: When pornographic sites are accessed, they try to install a dialer in your machine. If this is allowed, then the dialer uses your modem to make international calls and access 'premium' content. Presumably, people hosting the porn site share the money billed during calls with the private telephone service provider. Not only is your child subjected to more abuse, but also your phone bill is massively inflated. These dialers are sometimes hosted by hackers who use the installed dialer to thoroughly survey your machine and steal credit card numbers.

What you can do to protect your child

Your children need to be protected, whether they wish it or not. The first person to take up the responsibility is **You**. Children of impressionable age are prone to fall for alluring offers, interesting people, etc. After all nothing is more attractive than evil. You need to intrude on your child's privacy, find out what is going on, surfing habits, chat room friends, who sends e-mails and

what do they relate to, etc. Banning net use is quite barbaric and overkill. Given below are some pointers on what you can do.

Time for surfing: Set a fixed time during which the child uses the net. This should coincide with when you are around.

- **Find your Childs surfing habits:** In your IE Browser, click **History**. List of sites visited from your system is displayed. Click on the URL to find out the site contents. To find list of sites visited in previous days, click on **View** and select **By Date**. To increase the number of days, for which the details are kept, go to **Tools > Internet Options**, select **General** tab. The spin button for **Days to keep pages in history** allows you to select up to 999 days. Set the period you want, click **Apply** and **OK**.
- **Monitor the chat** activity. Find out what chat rooms the child visits and what is the talk about. Expressly warn the child not to give out telephone numbers to strangers.
- **Check e-mails** sent and received by your child. Good Content Administrator software allows you to store e-mails in a separate folder. You can browse the folder to check e-mails sent and received.
- **Spy Software** This type of software records details of all activity run on your machine. Every hour, hundreds of pictures of your computers screen are taken. The pictures reveal details of keystrokes used, chat conversations, e-mail sent and received, web sites accessed, etc. You can tell at a glance what your child has been doing on the net. But this type of software is oriented towards gathering evidence and may be useful to find what your spouse is up to. It does not prevent the child from accessing porn. To prevent access to porn and other sites you need a good Content Administration software.
- Install a good **Content Administration** software on your system. Some of the best software to protect your child are available at <http://www.mwti.net/>

Note: The author is a concerned parent and the suggestions given here are broad outlines. There are factors like child psychology, handling children's problems, etc. over which the author does not wish to give opinions. It is recommended you seek guidance from professionals in these fields.

Recommended Features of Parental Control Software

Parental Control software's come in various forms, shapes and claims. Good parental control software should allow you to perform Content Administration tasks. Put simply, you should be able to prescribe what content should be allowed and what should be blocked. This is called setting Security Policies. Recommended features for good Parental Control software are given below:

CHECK WEBSITES FOR RESTRICTED WORDS:

1) Restricted words: Software should allow you to specify restricted words and phrases like: porn, xxx, etc. and add them to the restricted words list. Access to any URL or page, that has these words, should be automatically blocked.

The software should also be intelligent enough, not to block or flag educational or medical sites. Many Content Administration software's, currently available in the market, have this crippling problem. For e.g. Sites with information about breast cancer, AIDS prevention, etc. should not be identified as porn sites.

2) List of banned sites: Software should allow you to add URLs of banned sites. Access to these sites is immediately blocked. Some notorious sites like www.hustler.com, www.playboy.com, etc. do not change their names. Such known sites need to be blocked outright.

3) Banned IP: Websites can be accessed by entering the IP (Internet Protocol) number. The software should be able to translate the IP number to its website name and block access if it contains restricted words or is on the banned list.

For e.g. www.sex-circus.com can be accessed through its IP, <http://198.63.10.71> when you use common Content Security software. Software's like [eScan](#) are able to translate the IP to its URL and block it.

4) Filter Category: The software should allow you to create category of filters for block and allow site. Sites related to the category can be listed there. For e.g. Pornography Category will have sites related to porn and all sites for this category are blocked. It should be possible to add or remove sites from block and allow category with a mouse click.

5) Log Files: The software should auto create a log of sites visited, blocked sites and reason why it was blocked.

Figure 1, shows a screen shot of [eScan](#), the top selling Anti-Virus and Content Security software that has this feature of adding restricted words.

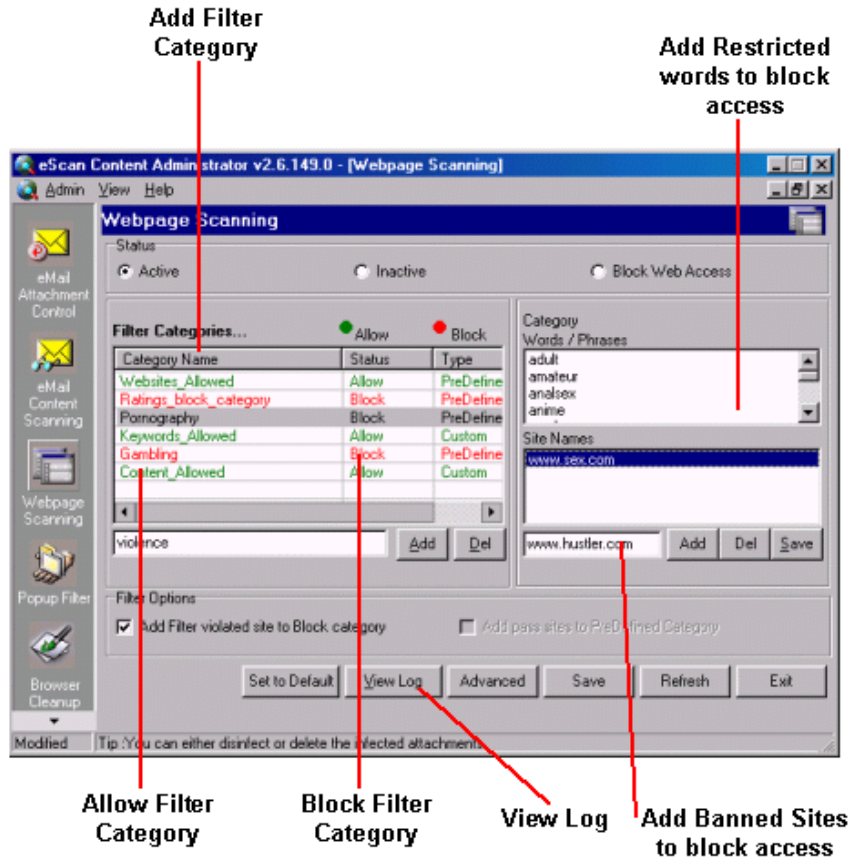


Figure 1 Features of a good PopUp Filter

ADVANCED PARENTAL CONTROL OPTIONS

The software should allow parents to enforce advanced content administration options. Figure 2, shows a screen shot of [eScan](#), the top selling Anti-Virus and Content Security software that has features of Advanced Parental Control.

Recommended features are:

1) Content Matching: After a list of restricted words is made, the software should automatically, search for such words in the accessed site. But content matching feature should be intelligent enough to differentiate between a porn site and a medical site that gives anatomical reference of a human body.

Words occurring in the following areas of the web page should be detected and denied access to:

- Site Name
- HTML Tags
- Page Title
- Page text or body
- Page description and keywords

2) **Threshold Level setting bar:** Restricted words like babe, sex, etc. can be found in legitimate sites. In Figure 1, you created a list of restricted words. In a website, if any three words from the list appear as a combination, more times than set in the threshold value, the site is blocked. The Threshold level bar allows you set the threshold value number.

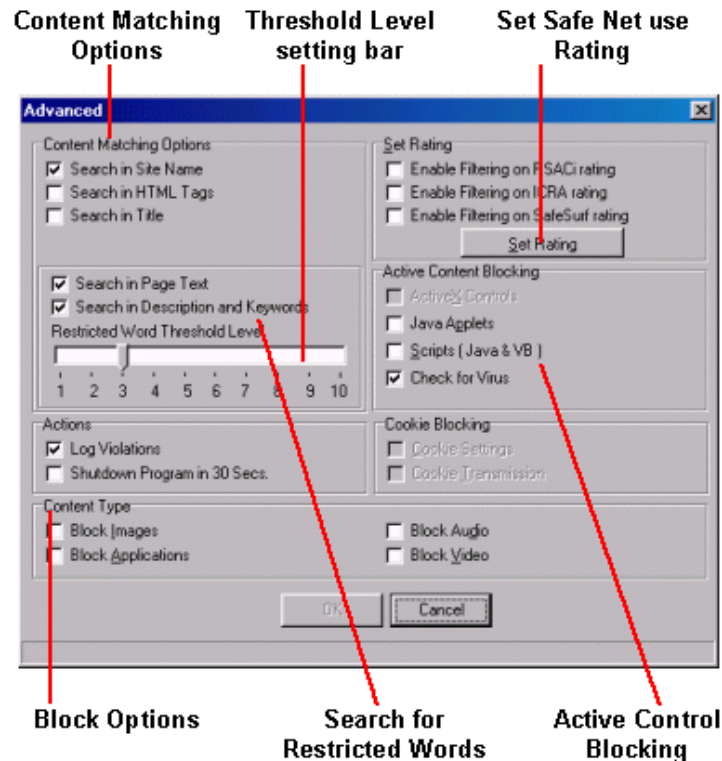


Figure 2 Content Control Options

3) **Block Options:** The software should allow you to choose options for blocking a website as given below:

- **Block Images:** Images on web pages are not displayed.
- **Block Applications:** Applications like .exe files that can run on the machine.
- **Block Audio:** Audio or sound files on websites are not played.
- **Block Video:** Movies on web sites are not allowed to run.

4) **Active Control Blocking:** Some web sites embed objects like Applets and Scripts, in your browser when you access their WebPages. The software should allow you to bar this action.

5) **Safe Net Use Rating:** For safe net surfing, organizations like RSCAi, ICRA, SafeSurf, etc. rate sites based on the language, Nudity, Sex and Violence. Your child should visit only sites rated safe for children, by these organizations.

The software should allow you to choose a rating agency and further fine tune access options for Language, Nudity, Sex and Violence.

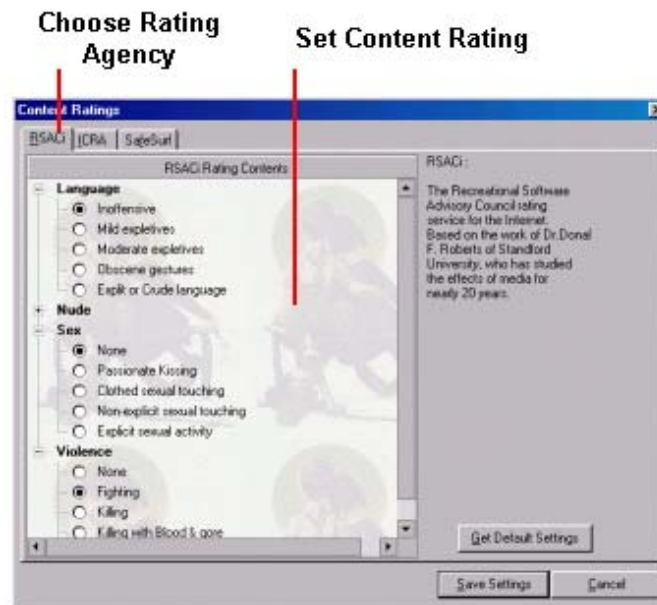


Figure 3 Set Content Rating

Good Parental Control software should be effective against Spam. Refer to the white paper on Spam for more details.

Remember that today's kids are computer savvy. They know more about computers than you. The features described in the preceding sections should be tamper proof and only people with the correct password should be able to modify them. The Parental Control software should have the feature of **password protection**. Lock the settings and assign a password that only you know. Then you can rest easy knowing that your Child is safe on the net.

About the Author

Govind Rammurthy is a hard core 'techie' with keen business acumen. He founded MicroWorld Technologies Inc. in 1995 and has been in the forefront of the fight against Viruses and other threats. He leads the team of programmers and QA who have developed world-class product suites: **eScan** and **MailScan**. These products offer the greatest control in the areas of Anti-Virus and Content-Security.

To find out how MicroWorld can help you, visit <http://www.mwti.net/>