PARENTAL SUPERVISION AND CYBER SURFING: CHILDREN'S SAFE ONLINE EXPERIENCES

Dr. Vijay Laxmi

Assistant Professor, B.K.M.College of Education, Balachaur
S.B.S.Nagar, Punjab (India)

Abstract
The Internet is an invaluable and unavoidable tool for both adults and children. Not only is it an excellent means of education, but it is also a great way for kids to have fun and socialize with their peers. Unfortunately, the Internet is also potentially dangerous for children. Sexual predators and cyber bullies are some of the common threats that face children when they are online. In addition, children are also at risk of exposure to immature materials or downloading harmful viruses to the family computer. Internet Safety for children's has become a global concern as Internet doesn't come with a user manual. According to a research by Cyberoam NetGenie, 75% parents are highly concerned about their kids' internet safety. Kids get lured to inappropriate online content and become victims of cyber attacks like cyber-stalking, child-pornography, sextortion and cyber-bullying. For kids' Internet Safety, it becomes important for parents to give a proper guideline to their kids which makes them aware about the pros and cons of Internet surfing. Parents can take steps to make their children's online experiences safe. In words of Al Salehi "Parents have to be responsible and aware of all the risks concerning the safety of the child, including the Internet. They have to guide and caution their children in such a rapidly growing world that deploys Internet. They must learn to use the internet and make a distinction between its pros and cons, not to mention knowing when to set boundaries and when to impose restrictions, as this is the need of the hour to ensure safety of the children." So this paper attempts to highlights the guidelines for parents to protect their children from antisocial behaviour as well as to make their children's online experiences safe.
Key words: *Parental Supervision, Cyber Surfing*

Introduction

The Internet is like alcohol in some sense. It accentuates what you would do anyway. If you want to be a loner, you can be more alone. If you want to connect, it makes it easier to connect. ~Esther Dyson

Online activities are an integral part of the children's lives and they probably spend many of their waking hours surfing the net. Surfing the Web has become second nature for the children. Children use the Internet to study, browses for information, socialize, or play games. These are all constructive activities and there is no doubt that the children can derive tremendous benefits from the Internet. But sometime wonderful environment can very easily become unhealthy and unsafe and even threatening for the children. The increasingly popular social networking sites, instant messaging programs, and chat rooms are just a few potentially dangerous applications that the children probably use regularly. These and others are often misused by sexual predators and cyber bullies who are lurking around the corner, just a few clicks away. Parents can't keep their children off the Internet but they can try

to make it a safer place for them, by following a few practical steps that will keep their children safe online.

Uses of the Internet

- **Surfing**
  Reading documents and visiting websites online is commonly referred to as "surfing" or "browsing". Visiting virtual museums, accessing public government documents, reading complete books and viewing short films are just a few examples of the many ways in which one can use the Internet. Be aware, however, that unmonitored computers can give the child access to material that is inappropriate.
- **Chat Rooms**
  "Chatting" online has become a favourite way for people to connect online in a group (a chat room) to share similar interests. Chatting is like talking, except that you type words rather than speak them. Typically, more than one "conversation" goes on simultaneously at a given time or chat room. There are two types of chat rooms—moderated and un-moderated. A chat room moderator enforces rules about what is acceptable to discuss in a given chat space. Experts recommend children be allowed to visit only moderated chat rooms that have been approved by parents.
- **E-mail**
  E-mail is one of the most commonly used features of computers with Internet connections. E-mail can be used effectively in a variety of ways by children—to write to family members and friends, communicate with teachers, even contact famous people and experts in various fields.
- **Instant Messaging**
  An instant message ("IM") allows two or more people to talk by typing back and forth in real time. IM programs usually appear on screen as boxes of some kind, a split screen, or small screen where the typed messages are passed back and forth. Some of these programs allow one to see what the person is writing as they are writing it.
- **Downloading/File Sharing**
  File sharing is another activity for many teens. File sharing is accomplished through easily obtainable programs that allow users to connect directly to other computers and copy (share) music files, movies, and other programs or files. This use of the Internet is a security risk because the files can be infected, and also may violate copyright protections.
- **Social Networking:** Blogging and other online diaries. Children are no longer restricted to playgrounds, sports teams or malls to meet new people. The world around them has become digital and VERY accessible. Students can set up a free e-mail address, web pages and online photo albums within minutes. Blogs (short for web logs) are like online journals and allow people to share their most intimate thoughts with a worldwide

audience. Many children have discovered that MySpace, Facebook, LiveJournal, and many other social networking sites are a great way to communicate with friends all over the globe. They are able to post messages, photos, and list all their favorite things about themselves. What children don't always understand is how public this information really is. As parents, the best way to keep your children safe is to remind them that having an online "personality" places them at potential risk. Information posted online means exposure to the entire world.

- **Gaming**
  Gaming is another option for young people—and gaming online can be very exciting. The thrill of competition, the ease of access to new games and excellent graphic effects make this activity fun for kids. But because of the ability to also chat with other players, safety issues should be discussed in the same manner as chat and IM concerns.

Cyberbullying, Harassment and Stalking

The feeling of anonymity on the web makes it a perfect playground for students to engage in cruel behavior. A 2007 study from the National Crime Prevention Council (NCPC) indicates that 43 percent of teens reported being victims of cyber-bullying. Cyber-bullying can consist of spreading lies and rumours about a person, insulting and targeting a student's sexuality or physical appearance, deceiving students into revealing personal information and then publishing it, and posting personally identifiable information or photos without the victim's consent. Technology used may include cell phones, instant message programs, chat rooms, e-mail, websites, polls and blogs.

When to Worry

There are a number of signs that may signal trouble. Parents know their child better than anyone else, so follow their instincts.

- **Screen Switching**
  If the child quickly changes screens or turns off the monitor whenever parents enter into their room, it is likely he/she is viewing something that they don't want parents to see. Be calm and ask them to move on so that you can view the screen.
- **Odd Phone Calls**
  If the child suddenly begins receiving phone calls from strange adults (or even other children) parents may have a problem. Install a caller ID program to determine where the calls are coming from and ask the child to explain them.
- **Odd Hours of the Night**
  If the child is up typing away in the wee hours of the night, he/she may be chatting online. This activity should be reserved for times and places that are supervised.
- **Sudden Influx of Cash**

If the child suddenly has more cash than can be accounted for, or shows up in unfamiliar clothing or with gifts that parents can't explain, this may be a sign of questionable activity.

- **Unusually Upset at an Internet Interruption**
  It is not normal to cry or to become overly upset when the Internet goes down for an hour or two. This type of behavior should raise a red flag and prompt frank discussions with the child.
- **Withdrawal from Family or Friends**
  If the child suddenly Withdrawal from Family or Friends this may be a sign of questionable activity. The larger the gap between the child and his /her family, the easier it is for a predator to create a relationship. So they shall have to talk to their Child.
- **Don't rely on software to do the job**
  Filtering and blocking programs can be a part of parents Internet safety plan at home, but they don't take the place of an informed and involved parent. (*cyberangels.org)*

Parental supervision/control and cyber surfing

The internet is a valuable tool for entertainment and education and children should be encouraged to use it. However, the child can also be exposed to material and behavior that they may find threatening and upsetting. Following simple guidelines can help to keep children happy and secure as they browse the internet.

1. **Place for everything:** Parents should keep the family computer in their living room or other communal area. Avoid allowing the child to keep the computer in their bedroom. Parents can then see at all times what they are viewing and this reduces the risk of them accessing material that is unsuitable.
2. **A time for everything:** agree with the child how much time they are allowed to spend online each day. This will depend on the age of the child and how much they might legitimately need the internet for study purposes. Agree on the time of day they can access the internet also and make sure that they stick to the rules agreed.
3. **Rules:** Suggested rules include limiting play time and never chatting with strangers or giving out any personal information, including the child's real name or where he or she lives. Talk to the child about the dangers of giving out personal information online. If they have a profile on any social networking site, warn them not to include any contact details that could identify them. Encourage them to set their profile to private so that no unauthorized person can view it. Parents should also advise them to use a screen name instead of their own name.Warn the child against sending pictures of themselves to strangers online. Make sure that they understand that strangers on the internet might not always be who they say they are.

4. **File Sharing:** Make sure that the child knows that downloading anything to the computer can cause serious damage. They must always get parents' permission before installing anything. Parents should always make sure that the computer is well protected with anti-virus software and / or firewalls.
5. **Think mall:** The most serious danger for children online is the risk of becoming a victim of a sexual predator. Unsupervised children may find their way into chat rooms or forums, which are proven venues that pedophiles use to lure victims. Cyber-bullying is becoming a major problem, particularly for teenagers. If parents suspect that their child has been approached online by a predator, save any and all computer and/or phone communications, and report it to the National Center for Missing & Exploited Children's CyberTipline at www.cybertipline.com. Parents can Contact the local police department if they suspect their child is in immediate danger. Encourage the child to talk about any communication they have received or viewed online that makes them feel uncomfortable or upset. Warn them not to reply to any such messages without telling parents first.
6. **Blocking and filtering**: There are various types of blocking and filtering software available, such as Net Nanny that can block access to certain types of site which might consider unsuitable. Check with Internet Service Provider (ISP) to find out if they offer any parental control options that can block the child from downloading any objectionable material.
7. **Bookmark:** Bookmark the child's favorite sites so that they can access them easily. This also reduces the danger of the child accidentally accessing unsuitable websites through misspelling words.
8. **Spend time**: Parents should spend some time on the sites their children regularly access, either with their child or alone. Parents will then be aware of the type of material available and of how other users of these sites can communicate with their child.
9. **E-mail id**: If possible, encourage the child to use parents e-mail address instead of setting up their own so that parents can monitor any communications that they are sending and receiving.
10. **Join the Game:** Ask the children to teach you how to play the game. This exercise encourages the child to be the teacher, and allows parents to identify possible safety issues while playing with their child.
11. **Be proactive:** Attend cyber safety classes and spend some time listening to and speaking with other concerned parents. The parents should familiarize them self with the services and programs their child uses.
12. **Computer savvy**: If parents are not computer savvy, enlist the help of those who are. Learn the basics of the Internet so that the children do not become complacent. Look at blogs and social networking sites to see what children are doing. To keep watch parents can create own accounts and play around with it a bit. Get on their children's friends list. Acronyms Parents Should Know are as under :

AFK / BAK	Away from keyboard/ Back at keyboard	**NIFOC**	Naked in front of computer
121	One-to-one	**WYCM?**	Will you call me?
ASL?	Age, sex, location?	**ADR**	Address
PA/ PAL/ POS/ P911	Parent alert/Parents are listening/ Parents over shoulder/ Parent alert	**TDTM**	Talk dirty to me
LMIRL	Let's meet in real life	**SorG**	Straight or gay
MorF	Male or female	**F2F**	Face to face
WRN?	What's your real name?	**WUF?**	Where are you from?
53x	Sex	**Cyber**	Cybersex, sex over the computer
WTGP	Want to go private?		

13. **Explore the Internet:** Take the time to explore the use of the computer and the Internet. They are valuable tools that can enrich the lives of every member of the family. The more parents know, the better they can protect their family. These quick tips will show them how to set up parental controls on Internet Explorer, Google Chrome, and Firefox.

- **Internet Explorer** - Internet Explorer has several areas that offer parental controls including content (restrictions on language, nudity, sex, and violence), offensive language, and listing approved or disproved websites.

To set controls:

1. Open Internet Explorer
2. Select "Tools" from the toolbar
3. Select "Internet Options"
4. Choose the "Content" tab
5. Click "Enable"
6. Adjust the slider to select the level you deem appropriate for your child
7. Save changes

- **Google Chrome** - Google has taken quite a bit of heat for not having parental controls built-in to Google Chrome. Some parents have

complained that restricted sites on Internet Explorer can be bypassed by savvy kids who use Chrome instead.

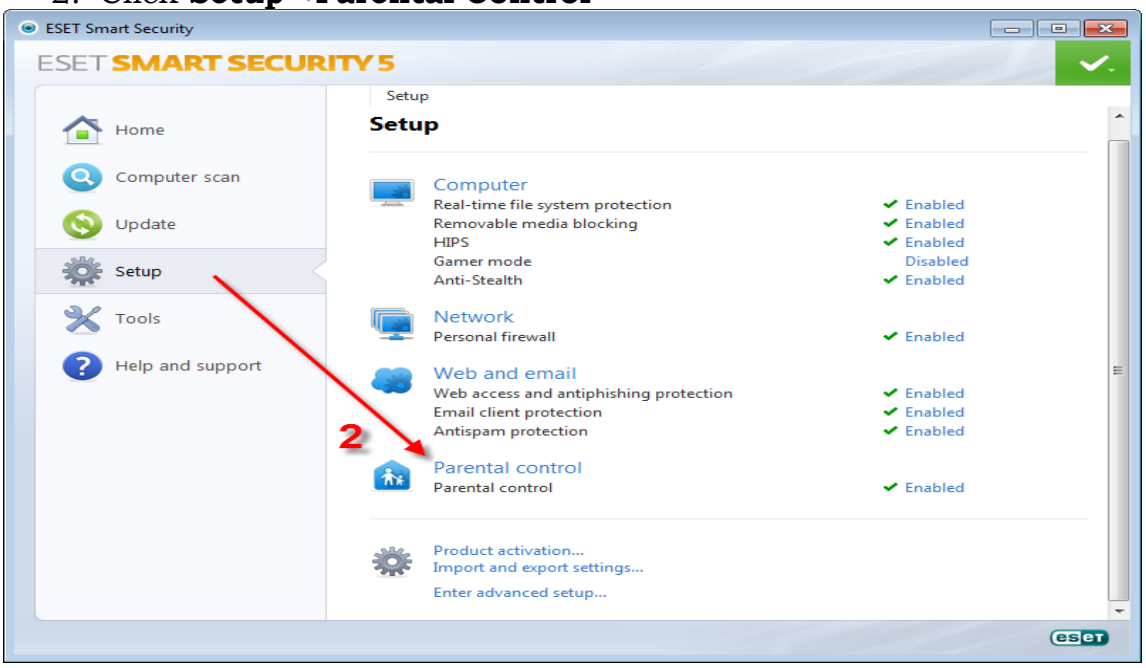
- **Firefox** - Firefox has no built-in parental controls, but they do offer an extension called "Fox Filter." Fox Filter blocks pornographic and inappropriate content for free, but other services require a fee.

14. Install parental control (content filtering) software: parents can Install parental control (content filtering) software to limit the websites the children visit, monitor their online activity, limit the amount of time the children spend online, block file sharing programs and protect them from offensive content or cyber bullies. Parents don't forget to inform the children that they have done this and explain to them that that they are not spying on them - but keeping them safe!

- **Parental control module:**

To access the Parental control module:

1. Open ESET Smart Security.
2. Click **Setup →Parental Control**



3. **Click Enabled / Disabled**

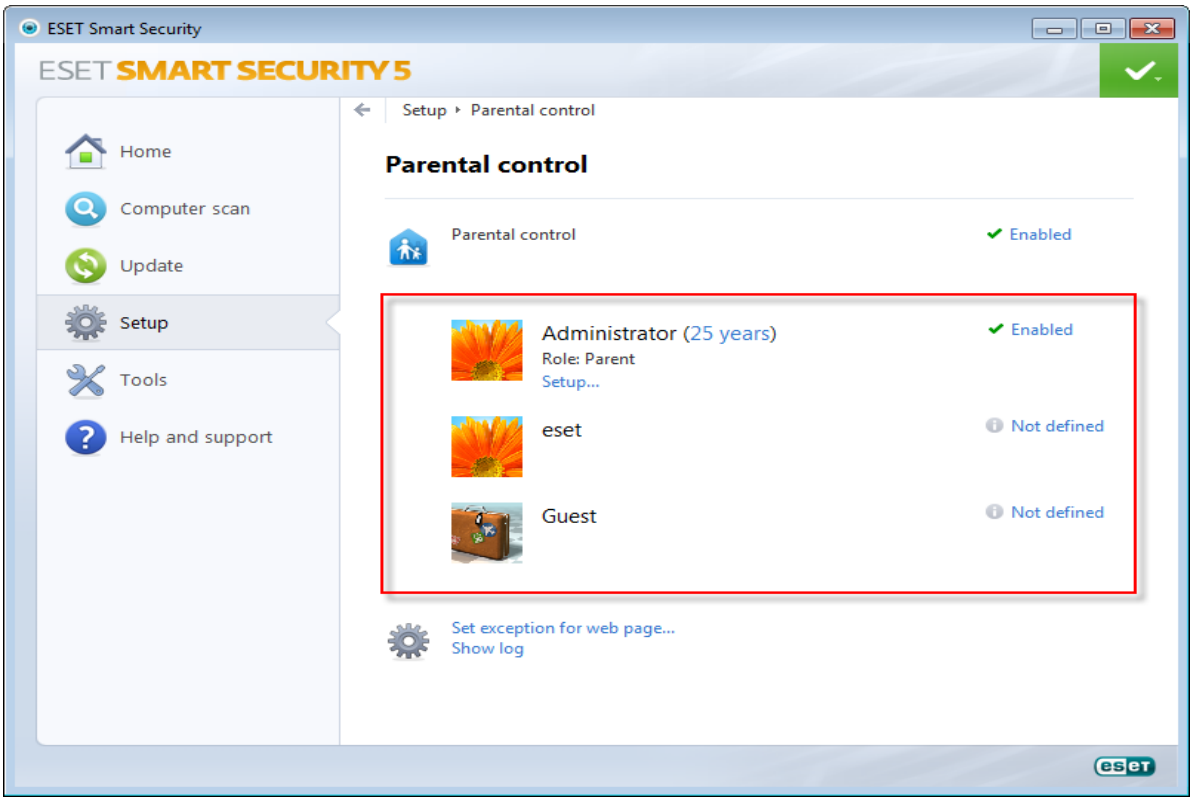
The Parental control module consists of a quick Enable / Disable feature, as well as a list of active Microsoft User Accounts. Clicking **Enabled** will temporarily disable Parental control for a specified duration. One can re-enable Parental control at any time by clicking **Disabled**. For a step-by-step guide on temporarily disabling Parental control, refer to the following Knowledge base article:

4. Product settings

Parents can also use Parental control to password protect their ESET product settings. For detailed instructions on how to password protect your settings, refer to the following Knowledgebase article:

Key Features:

User Roles: From the Parental control module, parents can control and monitor Internet access by configuring a Role for Microsoft Windows User Accounts.



- **Block Web Pages:** Another key feature of Parental control is the ability to restrict access to inappropriate content by blocking access to certain web pages.This functionality is fully customizable, allowing parents to restrict access for certain user roles.
- **Restrict access by category**: Parents can also restrict access by adding or removing items from the list of web categories for each role. If the check box next to category is selected then it is allowed. By deselecting a specific category, parents can block it for the selected account. Mousing over a category will show you a list of web pages that fall into that category.
- **Activity Logging:** See a detailed log of Parental control activity (blocked pages, the account the page was blocked for, reason, etc.) in order to better monitor Internet activity on your computer.
- **Quick selection:** Parents can quickly set up a user role by selecting a predefined configuration (Child, Parent and Teenager) or a user-created account and clicking **Copy** to copy the List of allowed categories from these accounts.

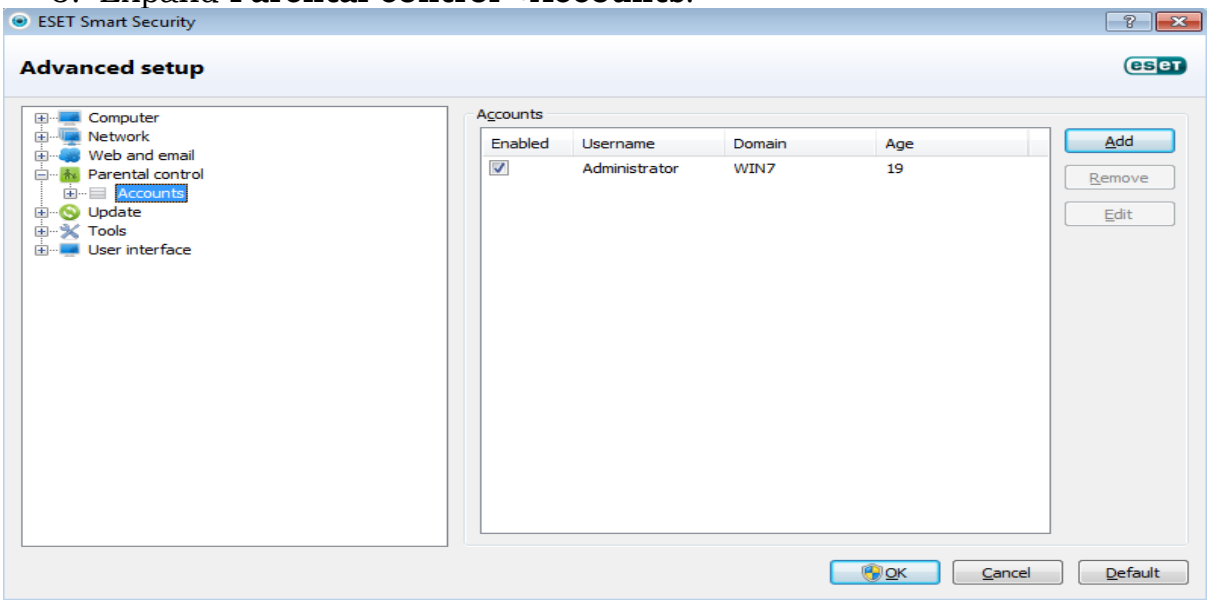
Additional Configuration

Parental control can also be modified by accessing the **Advanced setup tree**. From the Advanced Setup tree, users can:

- **Add/Edit/Remove user accounts**
- **Allow / restrict categories for user accounts**
- **Add / Edit / Remove web pages from the exceptions list**

To access Parental control configurations in the Advanced Setup tree:

1. Open ESET Smart Security.
2. Press the **F5** key on your keyboard to open the Advanced Setup window (If your settings are password protected you will be prompted to enter your password and click **OK** to enter the advanced setup tree).
3. Expand **Parental control →Accounts**.



Final words

Nowadays children spend a great deal of their childhood playing on the computer and surfing the web. Initially, parents welcomed the Internet into their homes, believing it would provide their children with access to a bottomless pit of beneficial and educational information. However, many parents soon realized that, instead of using the Internet for homework or research; for the purpose that it was originally meant for, that their kids were spending hours surfing inappropriate and undesirable websites, instant messaging with friends, playing online games, or talking to strangers in chat rooms. With children's internet use increasing and the rise of social networking sites, ensuring their child's online safety should be a priority for parents. In the same way parents put boundaries for their children in the real world, they should also do so in the virtual world. There are different types of Internet parental control software that were created to enable parents to manage and control their children Internet use. It is important for parents to understand that no matter how efficient the software is, it cannot replace educational efforts and open communication in the family. Internet parental control software can be efficient when it is combined with parental guidance for safe Web surfing and Web ethics. It is parents' responsibility to make sure that their children are informed about the benefits and dangers posed by the internet. Let them know that they can come to parents at any with any concerns they might have.

In words of **J. K. Rowling** "The internet has been a boon and a curse for teenagers".

References

Retrieved form-
http://www.nationalcac.org/prevention/internet-safety-kids.html
http://www.puresight.com/Useful-tools/tips-for-safe-internet-use.html
http://salfeld.com/software/parentalcontrol/
http://www.cyberangels.org/docs/cybersafetyguide.pdf
http://www.netgenie.net/global/learningcenter/internetsafetyforkids.html