E-ISSN: 2278 – 179X

Journal of Environmental Science, Computer Science and Engineering & Technology

Available online at www.jecet.org

Engineering & Technology

Research Article

Risks for Children in Cyberspace: A Survey

Divya Kavdia

Department of Computer. Science, CTAE, MPUAT, Udaipur (Rajasthan) India

Received: 1 March; 2012; Revised: 30 March 2012; Accepted: 30 April 2012

ABSTRACT

The internet is the valuable, essential and critical tool for children, which helps them to learn, explode and communicate with others. However, learning with internet can pose many hazards, children may become victims of harmful websites, pornography, inappropriate content, chat rooms, violence promoting sites, cyber bullying etc. The impact of these can lead to addiction of spending time on internet & can spoil the child's psychological development. With the continued growth of children interest in internet and cyber space, it is assumed that this situation will get worsen day by day. For this purpose many government acts like COPPA - Children's Online Privacy Protection Act are framed to protect children from these threats. This paper focuses on identifying risks and how to provide security to children in cyberspace. It also focuses on the awareness, concerns and attitude for child online protection. Preventive measures to be taken by parents, Teachers and others to protect children and developing tools to minimize risk are also being highlighted in this paper.

Keywords: e-Gov, Rural IT, cryptography, Digitized document, Ciphering, Digital signature.

INTRODUCTION

The Internet is now a major channel for education, creativity, opportunities and self-expression. Access to internet helps students to collaborative learning opportunities, provides new skills to obtain quality jobs, information sources, avenues of expression, connections to other Communities and many other benefits to all. It can also be a wonderful resource for kids to research school reports, communicate with teachers and other kids, and play interactive games. Kids who are old enough to punch in a few letters on the keyboard can literally access the world.

Children's access to the Internet, however, can put them in contact with inappropriate and potentially harmful material. As the number of children using the Internet increases and the age at which they begin decreases, identifying and addressing these risks becomes an important public policy objective. Some children inadvertently confront pornography, indecent material, hate sites, and sites promoting violence, while other children actively seek out inappropriate content. Dangers include grooming for sexual purposes and cyber bullying. While online, children may be victims of racism and online fraud, and can

be exposed to violent images. Additionally, through participation in chat rooms and other interactive dialogues over the Internet, children can be vulnerable to online predators. They may also become addicted to spending time online, with the risks and lost opportunities that this entails. With continued growth of Internet penetration and the Web itself, it is likely that without intervention, the situation will worsen.

That's why it's important to be aware of what kids see and hear on the Internet, who they meet, and what they share about themselves online. Just like any safety issue, it's wise to talk with your kids about your concerns, take advantage of resources to protect them, and keep a close eye on their activities. Governments, parents, caregivers, educators, business and civil society can help children to benefit from the Internet, but they also have a responsibility to protect them against risks online. Governments face many challenges when developing and implementing policies to protect children online: How to mitigate risks without reducing children's opportunities and benefits? How to prevent risks while preserving fundamental values such as freedom of speech and the right to privacy for all Internet users, including children themselves?

CHILDREN'S USE OF INTERNET

The Internet, for children and adults alike, is a hugely important communication medium. Children now use the internet to help with homework, to play games with people in other countries, to instant message their friends, use chat rooms and a whole host of other activities. [1]

Children in their teens routinely use the internet to perform tasks that their parents did at the library or using a phone, paper and pencil at their age of study. Learning computer skills is now an essential part and this can only be acquired with some practice, making it objectionable to totally restrict children internet access. Nowadays, Children's access to the internet has grown rapidly. A research was conducted by the London School of Economics [2], they founded that the following activities are performed by *Children on internet, ordered by popularity*

- Obtain information on things other than school work (94%)
- Help with school work (90%)
- Send and receive emails (72%)
- Play games online (70%)
- Send and receive instant messages (55%)
- Download music (45%)
- Look for information on careers and further education (44%)
- Look for information and shop online (40%)
- Read the news (26%)
- Chat rooms (21%)

Among the 12-19 year olds who go online on a daily basis, 21% admitted to having copied work from the internet and handing it in as their own.

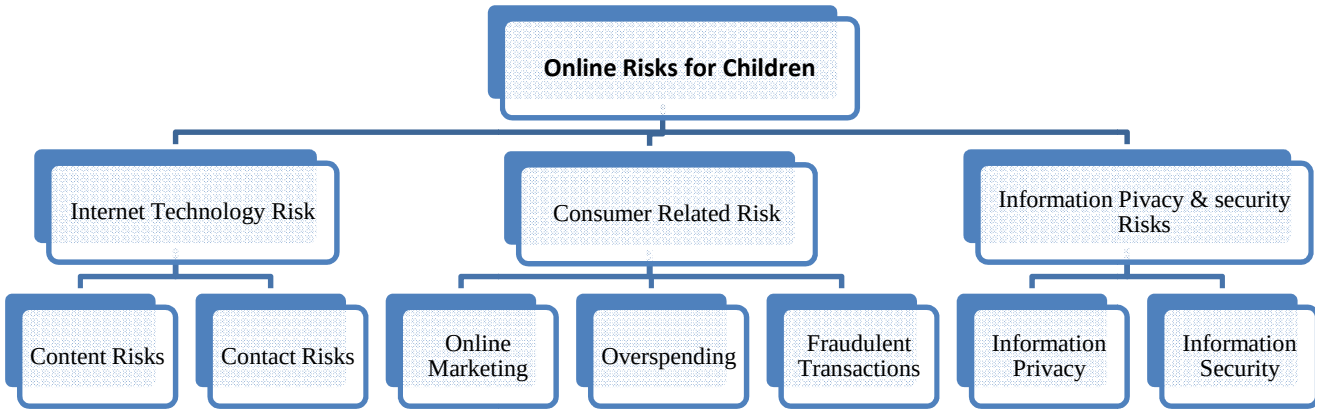
This survey concluded that, children waste their maximum time of internet access in doing irrelevant stuff like Playing games, Download music, Chat rooms and obtaining information other than school work.[3]

CATEGORIZATION OF RISKS

Risks to children online reflect the broad variety of children's use of the Internet. Several classifications of risks have been developed by the US Internet Safety Technical Task Force (ISTTF) and the US Online Safety and Technology Working Group (OSTWG), the Australian

Communications and Media Authority (ACMA), EU Kids Online, the European Youth Protection Roundtable Toolkit (YPRT) and the International Telecommunications Union (ITU) Guidelines for Policy Makers of Child Online Protection (2009a). While each of these classifications reflects the particular approach taken by above, they all distinguish between risks related to harmful content and those to harmful interactions [4].

Building on common elements of existing classifications and focusing on OECD Working Party on Information Security and Privacy (WPISP) and Committee on Consumer Policy (CCP) expertise, this report considers three broad categories of online risks for children: *i)* Internet technology risks, *i.e*. when the Internet is the medium through which the child is exposed to content or where an interaction takes place; *ii)* consumer-related risks; and *iii)* information privacy and security risks, *i.e.* risks every Internet user faces but have more negative impact on children of a particular age group. [5]



This paper emphasize on providing quantitative information on the online risk to children.

Internet technology risks: Today's children are often referred to as "digital natives" because they grow up with the Internet. As a consequence, risks pertaining specifically to children as Internet users comprise content risks (the child passively receives or is exposed to content available to all Internet users in a one-to-many relationship) and contact risks (the child is actively involved in a personalized relationship or interaction, whether bilateral or multilateral).

Content risks: Content risks comprise of main sub-categories like illegal content, age-inappropriate or harmful content and harmful advice. Potential consequences vary with the risk and other factors, such as the child's age and resilience.[6] *Illegal content, i.e.* content that it is illegal to publish, varies across jurisdiction For example, promoting bestiality, racism, hate speech and other forms of discrimination may be illegal in some countries but not in others, where it might fall under the more flexible category of "age-inappropriate content" . Content associated with sexual exploitation of children, however, is illegal in most countries, although the frequency of children's exposure to such content, while not known, is likely to be very low. *Age-inappropriate content* such as hate, violence or adult pornography, although generally not illegal, may harm children and their development. Children can accidentally stumble upon such content, can be referred to it by peers or can deliberately look for it. *Harmful advice* can result in suicide, consumption of drugs or alcohol, or the development of eating disorders. [7]

Contact risks: Contact risks occur when children interact online, for example when participating in online chats. They can be further distinguished according to whether the interaction takes place with the intention to harm the child (*e.g.* cyber grooming); children are exposed to hateful online interactions; or the child inflicts harm to himself or herself by his or her conduct (*e.g.* liability due to illegal file sharing).*Cyber grooming,* the use of the Internet by an adult to form a trusting relationship with a child with the intent of having sexual contact, is a criminal offence in several countries. [8] *Illegal interactions* can place minors or their parents at risk of criminal or civil penalties. Online piracy or sharing copyrighted material can, in some jurisdictions can lead to legal proceedings or put the household's Internet access at risk of being suspended. *Online gambling* by minors, which is illegal in most countries, is a financial threat to parents if minors have access to a credit card or other means of payment such as a mobile phone. It is also a potential source of psychological harm to the child concerned.[9]

Consumers related risk: Children face consumer risks online when they receive online marketing messages that are inappropriate for children (*e.g.* for age-restricted products such as alcohol); they are exposed to commercial messages that are not readily identified as such or that are intended only for adults.

Online advertisements for regulated or age-restricted products: to minors such as alcohol, cigarettes and prescription medicines raise concerns that such marketing downplays risky lifestyles and links children to suppliers online. The possibility for children to buy age-restricted products online does not necessarily mean that they do so.

Overspending: on online or mobile services by minors can generate *high costs* for parent. Children can subscribe to fee-based online services or spend money on online gambling if they have access to means of payment. Some popular online role-playing games require a subscription and players can incur real costs for virtual goods or advanced virtual characters.

Fraudulent transactions: occur when children enter into a distance sales contract but, having paid, do not receive adequate value for money or find themselves tied into subscriptions. Downloading of ringtones for mobile phones comes under these kinds of transactions.

Information privacy and security risks: Information privacy and security risks exist for all users. Children are a particularly susceptible group of online users, however, because they often lack the awareness and the capacity to foresee possible consequences while existing safeguards may be insufficient to protect their online privacy and security effectively.

Children bear information privacy: Risks when their personal data are collected online automatically, upon request by an information service provider, or voluntarily, when they fill their personal information in online forms.

It is important to take into account the context in which children disclose information, which can range from disclosing personal data to the entire Internet to sharing personal information with friends. Recent research tends to find that children consider offline and online contexts as part of the same reality: they use the Internet primarily to socialize with people they already know and perceive the Internet as a private space for online social activities. [10]

Information security risks: Information security poses a challenge for Internet users in general; however, children are particularly vulnerable to information security risks stemming from malicious code (malware and spyware). They are unaware of the risks and use services with a higher risk of containing malware. So far, there is only sporadic evidence of children being targeted as the weak link by online criminals. [11]

PREVENTING ACTIONS

Children may be more vulnerable from exposure to any form of electromagnetic energy, such as that generated by mobile telephones and to a degree baby monitors. This is because of their developing nervous systems, so there is a greater absorption of energy in their tissue and also a longer lifetime of

exposure. There has been some discussion regarding the safety of digital baby monitors, which use digital communication in their link between the mobile station and the base station.

Traditional child protection work: Online tools are available that control kids access to adult material and help protect them from Internet predators. There is no guarantee that these tools are capable to keep children away from 100% of the risks on the Internet. So it's important to aware kids about computer activities and educate them about online risks.

Many Internet service providers (ISPs) provide parent-control options to block certain material from coming into a computer. There are software also that helps to block access to certain sites based on a "bad site" list that your ISP creates. Filtering programs can block sites from coming in and restrict personal information from being sent online. Other programs can monitor and track online activity. [12]

Digital Enhanced Cordless Telecommunications: Philips is one example of a company that uses the Digital Enhanced Cordless Telecommunications (DECT) standard for baby monitors. The company states that this technology eliminates interference from other wireless equipment and ensures privacy. Digital technology, due to its 'pulsed' nature, appears to be more harmful at lower levels of power than the older analogue technology, which is potentially more prone to interference but creates a more 'even' output without spikes.Philips, in its documentation, states that the radiation/emission of its DECT baby monitors is not dangerous to children: "The level of electro-smog is 10,000 times lower than internationally accepted safety norms. For total peace-of-mind, we recommend placing the baby monitor at least one metre away from the baby."[13]

ELECTRO-SMOG

Electro-SMOG refers to the level of man-made Electromagnetic Energy (EME) that comes from the gadgets in our homes. Items that produce Electro-SMOG include mobile phones, microwaves, computers and televisions.

People who consider Electro-SMOG to be a problem say that constant exposure to this energy can result in headaches, irritability, sleeplessness, fatigue or even more serious health problems. Although there is little we can do to avoid this in our general environment due to mobile phone masts and so on, we can reduce the levels in our homes to a degree. The number one material that amplifies EME is metal. It therefore stands to reason that the use of metal in decorating should be kept to a minimum. Choose other materials for furniture, window coverings, appliance fronts or other surfaces. Removing computers and televisions from our children's bedrooms will reduce the level of EME. Even wooden hangers are considered preferable to metal ones.[13]

Getting Involved in Kids Online Activities: Aside from these tools, it's wise to take an active role in protecting kids from Internet predators and sexually explicit materials online. To do that:

- Become computer literate and learn how to block objectionable material.
- Keep the computer in a common area, not in individual bedrooms, where you can watch and monitor its use.
- Share an email account with children so one can monitor messages.
- Bookmark kids' favorite sites for easy access.
- Spend time online together to teach children appropriate online behavior.
- Forbid child from entering private chat rooms; block them with safety features provided by Internet service provider or with special filtering software. Be aware that posting messages to chat rooms reveals a user's email address to others.

- Monitor credit card and phone bills for unfamiliar account charges.
- Find out what, if any, online protection is offered by child's school, after-school center, friends' homes, or anyplace where kids could use a computer without your supervision.
- Take children' complaint seriously if he or she reports an uncomfortable online exchange.
- Contact local law enforcement agency if child has received child pornography via the Internet.

Many sites use "cookies," devices that track specific information about the user, such as name, email address, and shopping preferences. Cookies can be disabled. Ask your Internet service provider for more information. [14]

BASIC RULES

Set up some simple rules for kids to follow while they're using the Internet, such as:

- Follow the rules, as well as those set by your Internet service provider.
- Never trade personal photographs in the mail or scanned photographs over the Internet.
- Never reveal personal information, such as address, phone number, or school name or location. Use only a screen name. Never agree to meet anyone from a chat room in person.
- Never respond to a threatening email or message.
- Always tell a parent about any communication or conversation that was scary.[15]

Chat Room Caution: Chat rooms are virtual online rooms where chat sessions take place. They're set up according to interest or subject, such as a favorite sport or TV show. Because people can communicate with each other alone or in a group, chat rooms are among the most popular destinations on the Web — especially for kids and teens.

But chat rooms can pose hazards for kids. Some kids have met "friends" in chat rooms who were interested in exploiting them. No one knows how common chat-room predators are, but pedophiles (adults who are sexually interested in children) are known to frequent chat rooms.[16]

These predators sometimes prod their online acquaintances to exchange personal information, such as addresses and phone numbers, thus putting the kids they are chatting with — and their families — at risk.

Pedophiles often pose as teenagers in chat rooms. Because many kids have been told by parents not to give out their home phone numbers, pedophiles may encourage kids to call them; with caller ID the offenders instantly have the kids' phone numbers.

Warning Signs: Warning signs of a child being targeted by an online predator include spending long hours online, especially at night, phone calls from people you don't know, or unsolicited gifts arriving in the mail. If your child suddenly turns off the computer when you walk into the room, ask why and monitor computer time more closely. Withdrawal from family life and reluctance to discuss online activities are other signs to watch for.

Contact your local law enforcement agency if your child has received pornography via the Internet or has been the target of an online sex offender.

Technology Tools: Some common technologies used to protect children include:

Server-side filtering: Internet service providers and online server software offer filtering techniques to clients that deny access to particular content sources that have been pre-selected for blocking via automated processes, human review, and/or user options. The list of blocked URLs may or may not be disclosed and is regularly updated at the server level.[17]

Client-side filtering: This technology prohibits the browser from downloading content based on specified content sources identified by the user. Blocked sites may originate from both the software supplier and/or from the user's decision. Users maintain control over these lists with a password and may periodically download updated lists from the software's website. Some software filters out email or instant messaging.[17]

Filtering using text-based content analysis :Technology combines PC-based software and server software to conduct real time analysis of a website's content to filter out illicit content. Some software analyzes email and attachments. The user may or may not gain access to how such content is excluded.[17]

Monitoring and time-limiting technologies: This technology tracks a child's online activities and sets limits on the amount of time a child may spend online. Monitoring software often covers the Internet, email, and instant messaging activities. [17]

Age Verification System: This technology uses an independently-issued ID and controls the flow of online content by conditioning access to a web page with use of a password issued (by a third party) to an adult.Even the most sophisticated and current technology tools are not one hundred percent effective.[17]

GOVERNMENT STRATEGIES

COPPA: A federal law, the **Children's Online Privacy Protection Act** (COPPA), was created to help protect kids online. It's designed to keep anyone from obtaining a child's personal information without a parent knowing about it and agreeing to it first.

COPPA requires websites to explain their privacy policies on the site and get parental consent before collecting or using a child's personal information, such as a name, address, phone number, or Social Security number. The law also prohibits a site from requiring a child to provide more personal information than necessary to play a game or participate in a contest.

The Children's Online Privacy Protection Act generally prohibits website operators from knowingly collecting personally identifiable information from children under 13 without parental consent. It also requires site operators to collect only personal information that is "reasonably necessary" for an online activity. The law, which was enacted in 1998 and took effect in 2000, says personal information includes a full name, home or e-mail address, telephone number or Social Security number.[18]

OECD: The **Organization for Economic Co-operation and Development** (OECD) is currently preparing a report on the protection of children online. The main objectives of the work are to: enhance mutual understanding of policy approaches to the protection of children online; provide a comparative analysis of those policies; and explore how international cooperation could enhance protection of children online.

OECD held a joint meeting with the Asia-Pacific Economic Cooperation (APEC) in April 2009 on promoting a safer Internet environment for children. The OECD Working Party on Information Security and Privacy launched a project to analyze risks faced by children online and policies to protect them and, as appropriate, develop policy guidance/principles in this area. [19]

European Commission: The **European Commission** (EC) has developed a policy framework to protect children online. The EC's Safer Internet Program "aims at empowering and protecting children and young people online by awareness-raising initiatives and by fighting illegal and harmful online content and conduct." The Program adopts and funds a multi-stakeholder approach, including NGOs active in child welfare online, law enforcement bodies working in the field and researchers who collect information about online technologies and children.

APEC: The **Asia-Pacific Economic Cooperation** (APEC) has a Telecommunications and Information Working Group (APECTEL), established in 1990. It has a steering group on Security and Prosperity

(SPSG), responsible for promoting security and trust in ICT. The joint meeting with OECD was a project of the SPSG.

On 15 April 2009, APEC and the OECD held a joint symposium to exchange best practices on the protection of children online. In May 2010, APEC launched a project to build the capacity of APEC law enforcement agencies to respond effectively and offer greater protection to children from cyber-safety threats.[19]

NGOs: There are a number of **Non-Governmental Organizations** (NGOs) active in the field of COP. They include networks such as INSAFE (the European network of awareness centers) and INHOPE (the International Association of Internet Hotlines, partly funded by the EC Safer Internet Plus Program).[19]

Individual countries: A number of individual countries are actively promoting a safe Internet environment for children. The efforts of OECD member, and some non-member, countries are described in OECD (2010) and include results from a survey of policy makers presented to a joint APEC-OECD meeting held in 2009 .The ITU's Child Online Protection Initiative National Survey was run in 2009 and was directed to national governments. It collected data on the COP initiatives of many developed and developing countries. [19]

CIPA: The Children's Internet Protection Act (CIPA) is a federal law enacted by Congress to address concerns about access to offensive content over the Internet on school and library computers. CIPA imposes certain types of requirements on any school or library that receives funding for Internet access or internal connections from the E-rate program – a program that makes certain communications technology more affordable for eligible schools and libraries [20].

CONCLUSION

An increasing number of children are now using the Internet. They are starting at a younger age, using a variety of devices and spending more time online. This report focuses on online risks for children and policies to protect them as Internet users. It examines direct and indirect policy measures available to help mitigate risks for children online in order to compare existing and planned policies for the protection of children and exploring how international co-operation can enhance the protection of minors on the Internet.

This report emphasize mainly on various kinds of risks like content and contact risks, including exposure to pornography, cyber grooming and cyber bullying; consumer risks related, online marketing and fraudulent transactions and privacy and security risks, including the use of social networks without sufficient understanding of potential long-term consequences and there prevention tools like Filtering tools, Baby monitors which uses DECT, Electro-SMOG etc and other monitoring tools. These technology protection measures are most effective when teachers and educational institutions can customize technology and use it in connection with other strategies and tools. Many government Acts and Laws are also created to terminate these threats faced by children working online like COPA, CIPA and now various countries are also taking part in this area.

ACKNOWLEDGMENT

I am heartily thankful to my supervisor, Dr. Naveen Choudhary, Associate Professor & Head, CTAE, whose encouragement, guidance and support from the initial to the final level enabled me to develop an understanding of the subject. I am also grateful & offer my regards to Dr. Dharm Singh, Assistant Professor, CTAE and all of those who supported me in any respect during the completion of the paper.

REFERENCES

[1]Dina Demner "Children on the Internet "http://otal.umd.edu/uupractice/children/April (2001)

[2]John Rowlinson, “The Internet and Children: Access and Usage”, available at http://www.safekids.co.uk/ChildrenInternetAccessUsage.html (2011).

[3]Sonia Livingstone “Children’s Use of Internet: Reflections on the emerging research agenda” available at http://eprints.lse.ac.uk/415/1/NMS-use-of-internet.pdf

[4]OECD (2011), “The Protection of Children Online: Risks Faced by Children Online and Policies to Protect Them”, OECD Digital Economy Papers, No. 179, OECD Publishing. Available http://dx.doi.org/10.1787/5kgcjf71pl28-en

[5]What are the Risks for Children Online?http://kids.getnetwise.org/safetyguide/danger/

[6]National Cyber Alert Systemhttp://www.us-cert.gov/cas/tips/ST05-007.html

[7]http://kids.yahoo.com/parents/online-safety/1703/1--Teaching+Children+About+Online+Risks

[8]http://www.netsmartz.org/internetsafety

[9]Alison M. Smith ,Legislative Attorney , American Law Division “Protection of Children Online: Federal and State Laws addressing Cyberstalking, Cyberharassment, and Cyberbullying” CRS report for congress (2008).

[10]U.S. FBI Children At Risk Onlinehttp://www.surfinthespirit.com/the-web/at-risk.html

[11] OECD (2011), “The Protection of Children Online: Risks Faced by Children Online and Policies to Protect Them”, OECD Digital Economy Papers, No. 179, OECD Publishing. Available http://dx.doi.org/10.1787/5kgcjf71pl28-en

[12]Child Exploitation and Online Protection Centre (CEOP)

[13] “Digital Baby Monitors: Are they Safe?” http://www.safekids.co.uk/aredigitalbabymonitorssafe.html (2011)

[14]http://www.pctattletale.com/parenting/kids-at-risk-on-the-web.htm

[15]National Cyber Alert System

[16]National Research Council, Youth, Pornography, and the Internet, Committee to Study Tools and Strategies for Protecting Kids from Pornography and Their Applicability to Other Inappropriate Internet Content at 387 (May 2002).

[17]The Commission on Child Online Protection Act Final Report to Congress (Oct. 20, 2001).

[18] “Commission on Child Online Protection” Report to Congress (2000)

[19]International Telecommunication Union “Child Online Protection : International Telecommunication Union” Place des Nations CH-1211 Geneva, Switzerland.

[20]Federal Communications Commission- “Children's Internet Protection Act” available at http://www.fcc.gov/guides/childrens-internet-protection-act

*__Correspondence Author: Divya Kavdia ;__ Department of Computer. Science, CTAE, MPUAT, Udaipur (Rajasthan) India