ADVANCED CENTRE FOR RESEARCH, DEVELOPMENT AND TRAINING IN CYBER LAWS AND FORENSICS

CHILDREN & CYBER SAFETY - an e-book

DR. NAGARATHNA A.

JAY BHASKAR SHARMA

SPARSH SHARMA

NATIONAL LAW SCHOOL OF INDIA UNIVERSITY
BENGALURU

INTRODUCTION

According to the data, there were an estimated 4.66 billion people active on the Internet as of October 2020, that is, more than 60 percent of the global population. Internet has played a great role in shaping the way the whole world communicates. In recent years, the active digital population has constantly increased. This year however, the surge was more than ever due to the advent of COVID-19 pandemic. The world had almost come to a standstill because of the coronavirus and everything had to be shifted over to the Internet.

Employees have started working from home, meetings are being attended on video conferencing, and schools are teaching online. However, with the increased digital presence, the threat of cyber-attacks is also higher than ever. Children, among all are the most vulnerable to such attacks. Many people are under a common misconception that if children use the Internet at home, they are completely safe. This is untrue because the Internet takes children virtually to everyone and everywhere in the world. The challenges and threat to children from the cyber world vary from privacy, exposure to age inappropriate content, financial scams, and child grooming, etc. These attacks are multiplying every day and the abusers' cross-border presence is making it harder to trace and hold them accountable.

There are various mechanisms in place to ensure cyber security, but technology alone cannot protect the children.

We, as parents, guardians and teachers have a greater role to play in ensuring cyber safety of children.

The UN Convention on the Rights of the Child defines a child as being any person under the age of 18. However, an umbrella categorisation of children under 18 will not be able to demonstrate the steps to be taken to harbour the security needs. This is so because children of different age groups suffer from varied threats. A young child of less than 8-years is very unlikely to have the same problems as a 14-year old child. Therefore, we need to keep various factors in mind while designing the cyber security mechanism for children.

"Every image of child pornography is an image of a crime scene in progress"

"Behind every picture, there's pain."

- Parry Aftab

***

This e-booklet seeks to provide a brief-yet-comprehensive guide for the children, parents and teachers on cyber security.

- The book will explain the potential threats and the statutory remedies available to the people in an easy format.
- Additionally, it lays down simple steps that the parents and teachers can take to ensure the cyber security of their children/students.
- Lastly, it takes the issue of children safety to a broader level of national security and explores the way in which the same can be protected.

***

WHAT IS CYBER SECURITY FOR CHILDREN?

Technically, cyber security refers to defending computers, mobile devices and networks from malicious attacks. It takes various forms such as network, application, information, or operational security. The online protection of children through cyber security is the holistic approach to protect them from potential threats and attacks that they may suffer online.

This requires a country to have a strong cyber security mechanism, having specialised body to receive, investigate and act on the complaints. The body should have enforcement powers and technological advancement so as to protect the citizens from potential attacks. Further, there are certain basic rights and safety practices that parents and teachers should be aware of, and should also make their children aware, in order to ward off potential threats.

Parents should engage with children on their online activities, be aware of the online services used by them, help the children understand and manage their personal information, and educate them on the dangers of meeting any strangers etc.

Schools & teachers should teach cyber security to the students, raise awareness about the importance of digital footprint, ensure that learning software provided by the school is filtered and monitored and bring active steps to report any crimes that they witness to the appropriate authority.

WHY IS CYBER SAFETY IMPORTANT?

According to UNICEF estimates, 71% of the total young population in the world is on Internet. Moreover, one out of every three active users on the net is a child. We might consider cyber-attacks as trivial affair since unlike physically committed crimes, it does not leave a tangible effect on us. However, cybercrimes can severely affect one mentally, psychologically and emotionally. This makes it essential for us to learn cyber security, especially for those who are vulnerable to it the most like children and disabled.

Cyber security helps us in utilizing the Internet appropriately for learning and connecting with people. Further, it is important because it encompasses everything that pertains to protecting our personal data including sensitive data such as protected health information, bank details, intellectual property and many more.

Children may also tend to share personal photos and videos if they are unaware of the need of maintaining its privacy and confidentiality. Such may at times go into wrong hands, even leading to unwarranted acts such as crimes committed either in online or offline scenario. Hence it's a matter of concern.

WHAT ARE THE THREATS?

Cyber Grooming: Cyber grooming is a cyber-threat that is faced by children across the globe and not just restricted to India. Essentially, this is a threat in which an individual attempt to develop an emotional connection with a child, through cyber means. The individuals practice this through various cyber means like social media, online gaming websites etc. The individual pretends to be a child and this leads to the children trusting them eventually. After some period of time, when the trust between the child and the imposter gets built, the imposter gets the ability to take advantage of the child and use the child accordingly.

Cyber Bullying: Cyber bullying is another major aspect of the cyber threats faced today. Essentially, it is an act of harassing other children by the use of obscene, abusive language. This can be achieved by sending children hurtful content. However, it can result in severely hampering a child's confidence. It is imperative to understand, that if cyber bullying of a child is not identified at an early stage, it can result in far reaching consequences. Some of the consequences being negative impact on the mental, and emotional health of a child. This can therefore, severely hamper their growth.

Online Transaction Fraud: Though most of the children do not have their own bank accounts. However, they frequently use their parents' account for doing online transactions for gaming, shopping, etc. Criminals use several fraudulent tactics like calling to offer you benefits with fake identity etc. to steal money from the accounts.

Source: TotalProSource.com

Online Gaming: Online gaming, universally has now become a part of a child's daily activity. Further, online gaming is not just restricted to playing games, it has due to technological advancements and accessibility, become a way for people across places to share their thoughts while playing. It has emerged as a kind of social media in certain ways. However, there is a tendency to not be careful while connecting to people through online gaming, which can cause damage. Further, there is a risk of getting affected by spams, viruses while installing the same. This can lead to cyber bullying through the use of coarse language, infringement of children's privacy since a lot of personal information is uploaded and it can be misused, and this may also incur online transaction frauds.

Email Fraud: No work or activity today, can be imagined without communication. Communication runs today's society. Communication is done primarily through mails and therefore, has become an essential part of the society. We generally require email to engage in any online activity, whether it is gaming or social media. However, with data breaches in such companies, the email address reaches many unauthorised hands. Therefore, someone from anywhere across the country can send mails containing viruses, malwares and bugs attached to it.

LAWS TO ENSURE ONLINE SAFETY OF CHILDREN

In India, the Indian Penal Code, 1860 along with Information Technology Act, 2000 and Protection of Children from Sexual Offences Act of 2012 are the primary instruments for dealing with cybercrime in the country.

INFORMATION TECHNOLOGY ACT, 2000:

The Information Technology Act, 2000 has provisions which deal with various cybercrimes. It provides for penalty in case of unauthorized access to data and damaging of computer and data on computer through cyber-attacks including through virus. The Act also has specific provision to protect children on online platform and that is Section 67B.

According to Section 67B, child pornography includes

- publication or transmission of material in any electronic form, depicting children engaged in sexually explicit act or conduct; or
- creation of text or digital images; or
- collecting, seeking, browsing, downloading, advertising, promoting, exchanging, distributing any electronic material depicting children in obscene or indecent or sexually explicit manner; or
- cultivating, enticing or inducing children to online relationship with one or more children for and on sexually explicit act or in a manner that may offend a reasonable adult on the computer resource; or
- facilitating online abuse of children; or
- recording in any electronic form one's own abuse or that of others pertaining to sexually explicit act with children.
- Additionally adult pornography and offences of obscenity are regulated through Section 67 and 67A.

OTHER RELEVANT PROVISIONS:

Section 66E: According to this section, publication or transmission of image of a private area of a person without consent of such person is made punishable, if such images are captured under circumstances violating privacy.

Section 66C: This section deals explicitly with identity theft cybercrimes. This section prescribes punishment for any individual who fraudulently or dishonestly uses personal information like password, e-sign of other people.

Section 66D: This provision imposes punishment on a person who commits cheating by impersonating another.

Section 43A: CHLDREN'S PERSONAL AND SENSITIVE DATA – Though this provision imposes civil liability in form of 'compensation' it requires individuals and institutions handling personal data and sensitive information of people to take care of such information as against illegal use and exposure. This provision is wide enough to cover personal data and sensitive personal information of children.

INDIAN PENAL CODE, 1860

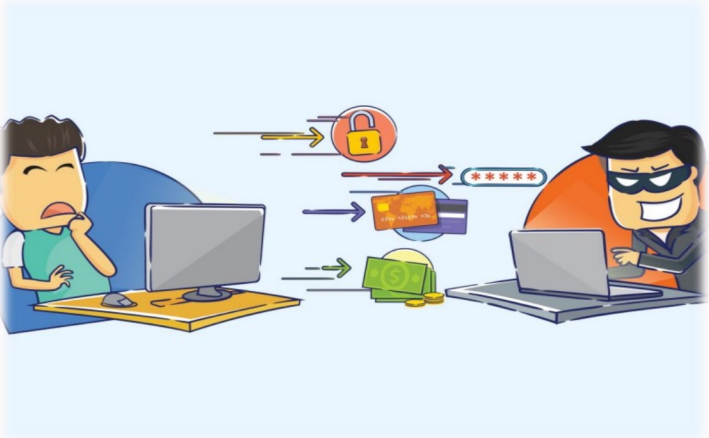
None of the provisions of IPC specifically deals with cybercrimes committed against children. However, the IT Act runs parallel to some of the provisions from IPC which penalizes certain forms of cybercrimes, including those in relation to:

financial frauds

online cheating

forgery

Images Source: *Pinterest*



obscenity

cyber stalking

sexual harassment

voyeurism

criminal intimidation

PROTECTION OF CHILDREN FROM SEXUAL OFFENCES ACT, 2012

Protection of Children from Sexual Offences Act, 2012 also provides for remedies to children in cybercrimes. According Section 2 (da), "child pornography" is defined as:

> ***"any visual depiction of sexually explicit conduct involving a child which include photograph, video, digital or computer generated image indistinguishable from an actual child, and image created, adapted, or modified, but appear to depict a child;"***

Other important provisions of the Act includes the following:

According to Section 11, if a person with sexual intent does any of the following acts, it is considered as an offence of Sexual Harassment on such child:

(i) uttering any word or making any sound or any gesture or exhibiting any object or part of body with the intention that such word or sound shall be heard, or such gesture or object or part of body shall be seen by the child; or

(ii) making a child exhibit his or her body, or any part of his body so as it is seen by such person or any other person; or

(iii) showing any object to a child in any form or media for pornographic purposes; or

(iv) repeatedly or constantly following or watching or contacting a child directly or indirectly via any electronic, digital or other means; or

(v) threatening to use , in any form of media, a real or fabricated depiction through electronic, film or digital or other mode, of any part of the child's body or the child's involvement in a sexual act; or

(vi) enticing a child for pornographic purposes or giving gratification therefor.

The above offences of Sexual harassment of a child is made punishable under Section 12.

Under Section 13, use of child for pornographic purposes is made punishable. According to this provisions, the offence is constituted if a child is used in any form of media (including programme or advertisement telecast by television channels or internet or any other electronic form or printed form, whether or not such programme or advertisement is intended for personal use or for distribution), for the purposes of sexual gratification, which includes—

(a) representation of the sexual organs of a child;

(b) usage of a child engaged in real or simulated sexual acts (with or without penetration);

(c) The indecent or obscene representation of a child.

The above offence is made punishable under Section 14.

According to Section 15, storage of pornographic material involving child is made punishable. As per this provision, a person is punishable if he—

(1) stores or possesses pornographic material in any form involving a child, but fails to delete or destroy or report the same to the designated authority, as may be prescribed, with an intention to share or transmit child pornography, is made punishable.

(2) Stores or possesses pornographic material in any form involving a child for transmitting or propagating or displaying or distributing in any manner at any time except for the purpose of reporting, as may be prescribed, or for use as evidence in court.

(3) Stores or possesses pornographic material in any form involving a child for commercial purpose.

MODES OF REGISTRATION OF COMPLAINTS

[I]

FIR with local police or Cyber Crime Police Station:

Under Section 154 of Criminal Procedure Code, 1973.

[II]

Private Criminal Complaint with Judicial Magistrate:

Under Section 200, Criminal Procedure Code, 1973.

[III]

Online Cyber Crime Reporting Portal Launched by MEA:

www.cybercrime.gov.in is the online reporting portal in which children and women can report cybercrimes against them.

Cyber-crimes related to Child pornography, Sexual abuse, Identity theft are to be reported here. Note that even anonymous complaints can be filed on this portal.

GUIDELINES FOR CHILDREN: DO'S AND DON'TS

DO NOT SHARE ANY PERSONAL INFORMATION

⇒ Do not share your personal information to any stranger or on any website or other internet links.

⇒ This personal information can be any detail about you which includes your name, phone number, Aadhaar card details, bank details, address, your parent's details, etc.

⇒ Do not share your photographs, videos and if any asks for it online, inform it to your parents or any trusted adult.

DO ASK BEFORE YOU CLICK

⇒ Do not click on any emails from any strangers, pop ups and other unfamiliar links and websites. Ask your parents or any trusted adult about it.

DO CREATE STRONG PASSWORDS AND DON'T SHARE

⇒ Do not create weak passwords and periodically change your passwords.

⇒ Ensure that you create strong passwords and don't share it with anyone except your parents.

DO SHARE ANY SUSPICIOUS ACTIVITY WITH A TRUSTED ADULT

⇒ Whenever you see a suspicious or an unusual activity on the internet, let that be known to your parents or any trusted adult before engaging on it.

DO NOT MEET SOMEONE YOU HAVE ONLY MET ONLINE

⇒ Don't do get together with anyone you have only met online.

⇒ Let your parents know about any stranger who asks you to meet.

DO REPORT INSTANCES OF BLACKMAIL AND ABUSE

⇒ Instances of blackmail, abuses occur frequently on the internet. It is essential to inform your parents or any trusted adult about the same. Hiding it and dealing with it on your own only aggravates the situation.

GUIDELINES FOR PARENTS

EDUCATE YOUR CHILDREN ON CYBER SAFETY AND SECURITY

⇒ It is imperative that parents teach their children about the dangers of cyber space. Discussions with children on various cyber dangers like Frauds, Dangerous Websites is a must. This will act as the building block in their cyber awareness.

MONITOR YOUR CHILD'S INTERNET ACTIVITY

⇒ Parents need to monitor their children's internet activity to be aware of what websites, mails they come across. This will help them in identifying any prospective cyber threats their children might be facing.

USE INTERNET FILTERS TO RESTRICT DANGEROUS / INAPPROPRIATE WEBSITES

⇒ Certain websites which could be dangerous or inappropriate can be restricted by using internet filters.

ENCOURAGE KIDS TO SHARE THEIR EXPERIENCES ON CYBER SPACE

⇒ Parents should teach their children to come to them when they see any instance of abuse or any suspicious activity on the cyber space.

TEACH YOUR CHILDREN TO JUDGE RELIABILITY OF VARIOUS CONTENTS ON THE CYBER SPACE

⇒ Parents should help their children to understand and examine various online platforms to equip them to judge the reliability of various contents on the cyber space.

CHECK PRIVACY SETTINGS OF WEBSITES YOUR CHILDREN USE

⇒ Parents should check the privacy settings of all the apps and websites their children use and should ensure that there are no implications to personal information and security.

GUIDELINES FOR TEACHERS

SENSITISATION OF TEACHERS

⇒ Sensitize and conduct training courses for teachers on issues relating to cyber safety of children.

WORKSHOPS ON CYBER SECURITY FOR CHILDREN AND PARENTS

⇒ Schools have the responsibility to educate both children and parents on cyber safety, security. This can be ensured by having workshops for the same.

SUPERVISE AND MONITOR INTERNET ACTIVITIES WITHIN THE SCHOOLS PREMISES

⇒ Schools should monitor the internet activity of students in the light of educational objectives, to ensure that there is no prospective cyber threat to all the stakeholders.

INCORPORATE PROTECTION AND DETENTION MEASURES

⇒ Schools should ensure that there is an effective firewall and the passwords created are strong enough for protection. Moreover, antivirus and operating systems should be regularly updated.

ALLOW THE STUDENTS TO USE PREDECIDED WEBSITES NECESSARY FOR EDUCATIONAL PURPOSES

⇒ Schools should preselect websites that the students can use according to the educational needs. This will ensure that the threat to open dangerous/ inappropriate popups and other unwanted websites is reduced.

HAVE AN EFFECTIVE AND ROBUST CYBER SAFETY POLICY

⇒ Schools should ensure that there is an effective policy made and followed in terms of cyber safety, security and privacy. Moreover, the policy should be clearly explained to all stakeholders in the school, which include the students, teachers, staff, etc.

CONCLUDING REMARKS

***

Child safety is an important concern.

***

It is essential to take online threats to children seriously, since if unchecked it may lead to dangers both on online and at times on offline platforms.

***

Content based crimes, if unchecked may lead to Contact based crimes.

***

Let's ensure child online safety now and always.

***