

CYBER ABUSE

AND ONLINE CHILD PROTECTION

There has been rapid increase and development in the use of information and communication technology. This has changed our day to day life in how we communicate, connect, influence people. More than ever the young generation is getting easy access to the cyber space. There are currently more than 500 million internet users in our country. It has changed the way they make friends, participate in games play, learn, shop, and explore their identities. With the increasing use of cyber space, cyber crimes are also increasing rapidly. However as much as the usage of internet and cyber media technology has spread across the nation, the awareness and knowledge about cyber safety and security measures has not increased. Cyber offences against children are spreading and diversifying as new methods are used to harass, abuse and exploit children. Children are more vulnerable to fall into the traps of cyber crimes for the time they invest in using cyber space and the kind of threats they are exposed to at their tender age. The increased use of social media, online gaming, and digital networking etc. have several harmful aspects where children might become victims of cyber crimes.

According to Indian Computer Emergency Response team, more than 53000 cases of cyber security incidents were reported in the year 2017.

Cyber Crimes are offences committed by individuals, companies or institutions by using computer, internet or mobile technologies through platforms such as social networking sites, emails, pirated softwares, websites etc.

There are different ways cyber crimes or abuse against children takes place. A few are mentioned below -

- **Cyber Harassment** - Messaging abusive or other objectionable content to the target child or creating fake profiles in social media with the intention of targeting the child.
- **Cyber Stalking** - Following someone on Internet/mobile for causing inconvenience, or harassment /extortion, or for other illegal motives.
- **Cyber Grooming** - Preparing a child, significant adults and the environment for sexual abuse and exploitation or ideological manipulation. (The new Terminology Guidelines define grooming as "the process of establishing/building a relationship with a child either in person or through the use of the Internet or other digital technologies to facilitate either online or offline sexual contact with that person").
- **Online Sexual Harassment** - Unwelcome sexual advances, request or demand for sexual favour, and other verbal or physical conduct of a sexual nature. "Sexual harassment" refers not only to sexual conduct with the explicit intention to violate the dignity of another person (i.e. purpose) but also to conduct of a sexual nature that a person experiences as offensive or intimidating.

- **Online Sexual Abuse** - Distribution of sexually explicit and violent content, sexual harassment.
- **Online Sexual Exploitation** - Production, distribution and use of child sexual abuse material (CSAM) (child pornography), "sextortion, revenge, pornography".
- **Pharming** - Installation of malicious code on a personal computer or server, misdirecting users to fake or fraudulent websites without their knowledge or consent.
- **Phishing** - The act of sending an email to a user falsely claiming to be an established legitimate enterprise in an attempt to scam the user into surrendering private information. The user is usually directed to a website and asked to update personal information (e.g. password, credit card, bank account numbers) that is misused for identity theft.
- **Sexting** - Self-production and posting of intimate pictures, sexually explicit conversations, posting/sharing of intimate pictures.
- **Email Spoofing** - Sending out email that look like genuine and from a trusted E-mail id but actually they are not.
- **Malicious Files Application** - Sending you malicious applications and files through direct messaging, gaming, emails through websites etc, in order to get access to the phone or personal data.
- **Online Commercial Fraud** - Identity theft, phishing, hacking, financial fraud.
- **Habit formation and online enticement to illegal behaviours** - Access to alcohol, cheating, plagiarism, gambling, drug trafficking, sexting and self-exposure.
- **Cyber Bullying** - Cyber bully means using internet or mobile technology to intentionally harass or bully someone by sending rude, mean, humiliating & hurtful messages, comments, images & videos to the child or others. Cyber bullying is one of the common cyber threats being faced by children in young age.



DO'S AND DON'TS

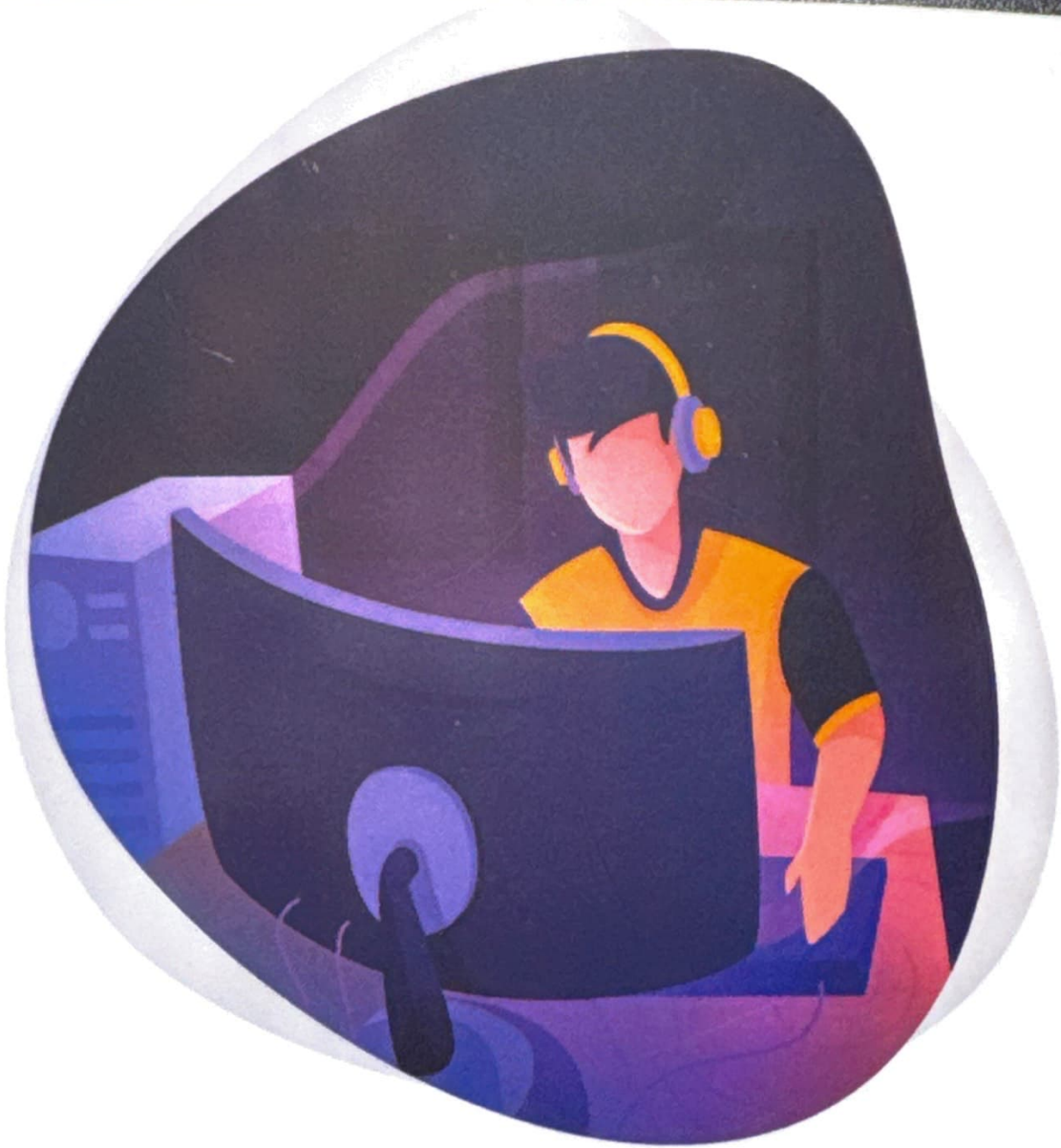
To secure yourself and children from falling into the traps of cyber crimes and abuse

- Don't accept friend requests from unknown people on social media platform
- Do not share personal information like date of birth, address and phone no. on social media and other platforms.
- Never install software and apps from non-trusted or unknown sources.
- Use good antivirus and online protection software. Keep child mode for usage of internet by the children. There is all kind of contents available for children to access online which makes them vulnerable to be exposed to harmful content.
- Check minimum age criteria in the apps and social networking sites.
- Lock down apps on phone which are not age appropriate for use by children.
- Block or report the inappropriate, aggressive, hurtful, hateful and malicious content or accounts immediately. It is better to not engage with a person who seems suspicious.
- Do not share any sexually explicit or personal, photograph, video or information through online media.
- Do not keep sexually explicit photo/video of yourself in your smartphone.
- Do not meet a person who you met just online.
- Never open a link, picture or video sent by an unknown source or person.
- Always check the URL starting with https only. The website with URL "http" encrypt your data in the website and protects it from tempering.
- Use security measures in the social networking sites and emails so that it is not hacked or compromised.
- Always use a complex password with combination of alphanumeric. Never share your password with anyone and also regularly change or update your password/ PINs etc.
- Use two or three factor log-in feature in all media like Email, Facebook, Whatsapp etc.
- Do not respond to fake emails about winning lottery, trip, awards, free gifts etc.
- Enable privacy and security settings in social networking sites like Facebooks, Instagram, Whatsapp etc. Restricting access to your posts in very important.
- If your account has been hacked, send an alert message to all your friend and contacts and report/ complain about the same to the social media provider.
- Beware about the content you spread and share in your social media. Never upload or download copyrighted content, picture or video as it is an offence.
- Educate yourself and your children about cyber crimes and online safety measures. Children also become the victims as well as the perpetrators of cyber crimes many times.
- For children, develop a habit of outdoor games as well. Excess use of online gaming and social media has many harmful effects on children. Out-door games are every important to ensure their physical, social, emotional and inter-personal wellbeing and development.



TALK TO YOUR CHILD

Communication gaps between parents and children makes children more vulnerable to cyber abuse especially child sexual abuse. Children many times fall into the traps of abusers because of manipulation and threats. This leads them to be exposed to repeated chances of abuse or extreme situations threatening their wellbeing and safety. A trusted relationship between parent and children is a key to ensure that the child is well aware about the consequences of his/her actions as well as comes to the parents first when there is any kind of threat felt by the child. Do not spy on children as it breaks the trust and intrudes their right to privacy and dignity. Having a friendly and mature relationship with children is a key to ensure that the children do not hide important aspects about their lives. More importantly educating yourself about cyber crime and online safety is vital in securing yourself and children from cyber threats.



CHILD PROTECTION SUPPORT DESK
www.childprotectionsupportdesk.org/
7414837414

CYBER CRIME REPORTING PORTAL
<https://cybercrime.gov.in/cybercitizen/home.htm>

CONTACT FOR ASSISTANCE
<https://cybercellraj.com/>
(Rajasthan)

FOR MORE INFORMATION REFER
Child Victims of Cyber Crimes Legal Toolkit - NCPCR
A handbook for Adolescents students on cyber safety,
Ministry of Home Affairs, GOI