SAFE
Internet Safety Alliance for E-Indians

unicef
for every child

विद्यया ऽमृतमश्नुते
एन सी ई आर टी
NCERT

CyberPeace
Foundation

Handbook on Digital Safety

For Children

2022

CYBER PEACE CORPS

Table of Contents

Preface

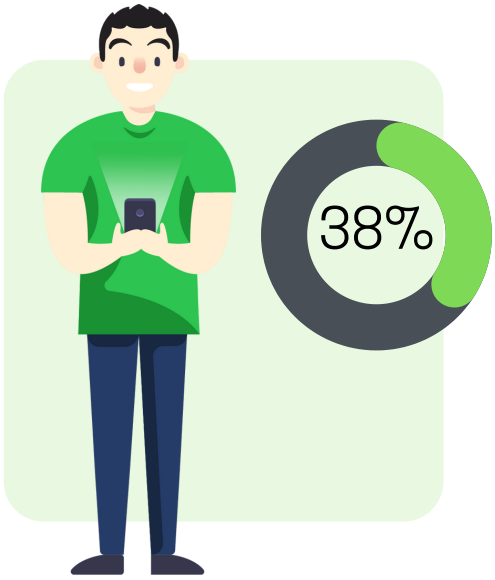
This e-handbook is a ready reckoner for children and students with access to any digital platform and is meant to provide succinct information on what they could do to prevent and, if required, address the effects of cyber abuse and seek redressal. Through this e-handbook effort has been made to explain different forms of cybercrimes that children face along with the legal provisions, prevention mechanisms, and thereafter providing tips that will help in keeping oneself safe from cyber abuse.

Introduction

Over the last two decades or so, technology has influenced human life more than perhaps any other single factor. The effects of technology have been far reaching, as it percolates into the professional life of the few but also into the personal lives of many.

According to a 2020 report, 38 percent of school-going children, i.e. those who are 15 years of age and below, are users of the internet in India. These children access the internet for information and education, social media, gaming instead of entertainment, and sports.

The onset of the pandemic further increased people's (and children's) dependence on technology and the internet, with individuals from all age groups and walks of life deciding to (and in some cases, forced to) tap into the possibilities it presented to carry on hitherto offline activities.
To anyone's dismay though, one cannot use the age-old idiom, 'So far, so good' in a sweeping manner to describe the situation. Let's consider some other facets of these developments. With the increased user base as well as the time spent online by children, came the pressing need to protect them from exposure to harmful as well as inappropriate content online.



A study conducted a few years ago found that Indian children are the most cyber-bullied in the world. Another study conducted in the National Capital Region found that one in four adolescents saw a morphed image or video of themselves and about half of these cases were never reported to the authorities. According to the National Crime Records Bureau (NCRB), there was a 400% increase in reported cyber crime cases against children in 2020 in comparison to the statistics from the previous year.

Although available data probably represents only the tip of the iceberg, what is reasonably deducible is that with increased exposure to the internet comes increased risk of becoming a victim of cybercrime, rendering children vulnerable.

The intent of this e-handbook is not to alarm children. But with the rising concerns regarding online safety of children in an increasingly digital age, there is a need to spread awareness about the various types of cyber abuse that are prevalent today and to provide information and resources to a child that can turn to for help.

What are Cyber Crimes?

Cyber crimes are defined as any criminal activity which takes place on or over the medium of computers, the internet or other technology recognised by the Information Technology Act. It includes any illegal activity where a computer or internet is either a tool, target, or both.

The conveniences brought on by the internet such as speed, anonymity and lack of borders makes financial crimes such as ransomware, fraud and money laundering, along with other crimes like cyberstalking and bullying, impersonation and identity theft and online grooming, easy to perpetuate. Cyber crimes may be carried out by individuals or groups with relatively low technical skills, or by highly organised global criminal groups.

What is Cyber/Online Abuse?

Cyber or online abuse may be defined as any online behaviour that seeks to threaten, harass, harm or humiliate a person. It refers to harassment that is carried out using the internet, mobile technologies, or other digital services. If anyone feels a sense of fear or insecurity in the online space, they are considered to have faced an incident of cyber abuse. It can happen via any device that's connected to the web, such as computers, tablets and cell phones. The abuser can be a stranger or a known person, a male or a female, an adult or an adolescent, or completely anonymous.

Why Be Concerned About Cyber/Online Abuse?

Anyone who is an internet user today is potentially at risk of becoming a victim of cyber abuse. This is especially the case with children who, while being quick to learn the use of new technologies, are equally ill-equipped both cognitively and emotionally to identify, prevent or address any abuse they may face online. The first step to combatting online abuse is by developing a shared language to identify and describe it. It is crucial that caregivers and educators who relate closely with children must acquaint themselves with these affairs so they are able to educate, protect and provide relief to the children under their care. As the internet is closely intertwined with the lives of children today, it is truly better to be safe than sorry.

Cyber Crimes: An Overview

As children are in a digitally evolving climate, exposure to and involvement in cyberspace is unavoidable. While being dependent on the internet for various activities related to study and entertainment, it is important to parallelly be aware of the risks and dangers that lurk online, especially to cyber issues that affect children disproportionately more than an average adult. In order for you to be equipped to identify, report and seek redressal for possible cyber abuse, and socialise safely on online platforms, information is pivotal.

With the pandemic, digital integration into our daily lives has only increased. In order to make use of cyberspaces effectively, one needs to be aware of both online dangers and digital etiquette. As you start spending more time in cyberspace, have online personalities and form communities online, how prepared are you to face the dangers lurking there?

- Have you ever had a conversation with your caregivers on cyber etiquette?
- Do you know the types of abuse that are Encapsulated under cybercrime?
- Do you think you will be able to identify an incident of cyber abuse, if you came across one?

Types of Cyber Abuse

Cyberstalking and Cyberbullying

Damaging or destructive writings, messages or posts, pictures or recordings, spreading false rumor or gossip tidbits, etc. targeting one person is called cyber bullying. Incessant following of someone in an unwanted manner entails stalking.

Online Grooming

Child grooming entails befriending and establishing an emotional connection with a minor, and sometimes the child's family, to lower the child's inhibitions with the objective of sexual abuse.

Phishing and Online Fraud

Phishing is a type of social engineering where an attacker sends a fraudulent message designed to trick a person into revealing sensitive information to the attacker or to deploy malicious software on the victim's infrastructure, like ransomware.

Exposure to Child Sexual Abuse Material

Circulation, creation and possession of sexually explicit pictures, videos, sound clips, literature, texts, emails, etc., especially ones featuring children.

Identity Theft and Impersonation

A crime in which an attacker uses fraud or deception to obtain personal or sensitive information from a victim and misuses it to act in the victim's name.

Hacking and Malware Attack

The act of compromising digital devices and network through unauthorised access to an account or computer system.

Legal Provisions and Redressal Mechanisms

The Information Technology (IT) Act, 2000, and the Protection of Children from Sexual Offences (POCSO) Act, 2012, were drafted to combat cybercrimes (and other offences against children in the case of POCSO Act). The IT Act is the primary legal provision that specifically deals with cyber crimes. Recent amendments to the POCSO Act addresses cyber sexual offences concerning children. Apart from these, several sections of the Indian Penal Code (IPC) address cybercrimes.

A. Legal Provisions Pertaining to Cybercrimes

Offence	Applicable Legal Provisions	Punishment
Cyber stalking	Sec 11(iv) POCSO Act, Sections 354D, 509 IPC	Up to 3 years and/or fine
Phishing	Sections 66, 66A/C/D of the IT Act, 2000	Up to 3 years and/or fine
Cyber Bullying	Sections 503, 506, 507 IPC	Up to 2 years and/or fine
Identity Theft	Sec 66C IT Act	Up to 3 years and/or fine
Violation of Privacy	Sections 66E, 72 IT Act, Sec 23 POCSO Act	Up to 3 years and/or fine
Hacking	Sections 43, 66 IT Act	Up to 3 years and/or fine
Child Pornography	Sections 11 (v) & (vi), 13/14/15 of POCSO Act, Sections 66E, 67 IT Act, Sections 292, 354A(iii)/C IPC,	Up to 3/5/7 years imprisonment and fine
Online Grooming	Sec 11(vi) POCSO, Sec 67B (c) IT Act	Up to 3/5/7 years imprisonment and fine
Online Child Trafficking	Sec 5 ITPA, Sec 366(A) IPC,	Up to 7/10/life imprisonment

Offence	Applicable Legal Provisions	Punishment
Defamation	Sections 499/500, 469 IPC	Up to 2/3 years and/or fine
Online Extortion	Sec 383/384, 385, 386, 387, 388, 389 IPC	Up to 10 years
Online Sexual Harassment	Sec 11 POCSO Act, Sections 354A, 509 IPC	Up to 3 years and/or fine
Sexting	Sections 67, 67A IT Act, Sections 11.12 POCSO Act	Up to 5/7 years and/or fine

B. How to File a Complaint?

As a child first and foremost, in case of any incident of abuse you may experience/come across online, make sure to talk about it with your parents/guardians or a teacher. It is important for you, as a minor, to have a support system that will rally around you through the process of redressal, which may be provided by trusted adults in your life. They can support you with the official processes. The information given below is purely for educational purposes. While you may, as a child, approach an authority for redressal yourself, we would recommend you take the help/support of adults you can trust.
There are several options available under law for reporting cyber related crimes. This includes online portals for reporting cybercrimes against children. These options facilitate registration of the crime. One of the easiest ways to report a cybercrime is to file a complaint at the national cybercrime portal (National Cyber Crime Reporting Portal) or to file it on NCPCR's 'POCSO E-box' web page.

Additionally, one always has the option of directly approaching a local police station or a cybercrime cell (cyber police stations). It is important to note that you can register a cybercrime FIR at the nearest local police station and that under Section 154 of the Code of Criminal Procedure (CrPC), 1973, it is mandatory for every police officer to record the information/complaint of an offence, irrespective of the jurisdiction under which the crime was committed. In case you as a child/student have been a victim of an online sexual offence, it is mandatory for your caregiver (parent/teacher/guardian) to report it under the rules of the POCSO Act. As per the law, free legal aid can be provided to you and your guardian.

There are several mechanisms to report cybercrimes. Some of the options available to you are depicted below:

Reporting Process for Children

Direct Reporting

Reporting Forum:
1. **National Cyber Crime Portal**
2. **POCSO E-Box**
3. **Childline: 1098**

Parents / Guardians / Any Trusted Adult

Teachers/School Committee
(Child Abuse Monitoring Committee/Child Safety Cell/Campus Safety Cell)

Where has the incident of abuse occured?

Outside School

In School

Reporting Forum:
1. **Local Police**
2. **E-Box**

Report incident to the school management (Child Abuse Monitoring Committee)

Make sure to collect screenshots and other evidences of the abuse

Report on the platform where online abuse has occured

Reporting Forum:
1. **e-Box**
2. **Childline: 1098**
3. **Local Police or Cyber Police**

C. POCSO e-box

The National Commission for the Protection of Child Rights (NCPCR) has launched a POCSO e-box system online. This is meant to aid you to register any case of sexual harassment of a child victim (including online abuse). You can enter details as instructed on the e-box web page: https://ncpcr.gov.in/pocso/public/

D. Childline 1098

The Ministry of Women and Child Development (MWCD) has a well-known toll-free helpline number for children. This number is to aid children in any/all cases of abuse, violence or neglect perpetrated against them. You can call this helpline to report cyber offences as well.

E. Police

All jurisdictional police stations have the power to take a complaint on cyber offences. You can directly approach a jurisdictional police station or cyber police station about a cybercrime too. In addition, the central government has also appointed a cyber cell officer for each state. You can directly approach them to report the cyber offence. https://www.cybercrime.gov.in/webform/crime_nodalgrivancelist.aspx

F. Reporting Through School Committee

According to the Handbook on Implementation of POCSO Act, 2012, for School Management and Staff, every institution is advised to constitute or designate, from an existing management committee or otherwise, a Child Abuse Monitoring Committee (CAMC) whose primary responsibility shall be to prevent child abuse and to monitor and implement the guidelines. If you are a child with knowledge of a sexual offence that has taken place against any child from the school, such offence (including online abuse) must mandatorily be reported to the CAMC. A representative of the committee after the conclusion of an immediate enquiry shall report the same to the authorities as directed under the law.

There are legal counselling centres for the victims of sexual abuse:

There are legal counselling centres for the victims of sexual abuse:

1. Aks Crisis Line: 8793088814
2. She will Survive
3. Orinam
4. Centre for Cyber Victim Counselling
5. Cyberjure Legal Consulting

G. Child Welfare Committee (CWC)

CWCs exist in each district or for a group of districts and act as the final authority for children in need of care and protection. Any child in need of care and protection may be produced before such a committee by a public servant, social worker, a public spirited citizen or by the child themselves.

H. National Commission for Protection of Child Rights (NCPCR and SCPCRs)

The NCPCR and the different State Commissions for Protection of Child Rights (SCPCRs) are statutory bodies that work towards achieving a child-rights centric approach in all laws, programmes and policies in India. One can reach out to them for all matters concerning child rights.

I. Helplines

NGO	Contact Details
CyberPeace Foundation	helpline@cyberpeace.net Ph No. 91 95700 00066
National Cyber Crime Reporting Helpline	Ph No. 1930

How to Identify, Prevent and Act?

Often, you may not want to disclose to a trusted adult about an experience of abuse that you might have undergone. There are many possible reasons for this ranging from threats by the abuser, feeling of shame & guilt, fear of not being believed, a desire to protect the abuser (if the abuser is a close relative or friend), a lack of awareness that you have been abused, you don't know whom to inform or simply for the fact that no one has asked you. However, it is important that you know how to identify abuse and that you are always alert to any signs that you may observe.

How can you identify that you are possibly facing online abuse or harassment? If you identify or are told about incidents of abuse experienced by your peers, what should be your immediate steps? What should you do if you suspect that you are being abused?

This section of the e-handbook covers aspects of how to identify abuse and protect oneself and seek redressal through appropriate mechanisms.

Early Signs of Abuse and Addiction

The higher the time spent online, the higher the chances of experiencing online abuse/harassment. Additionally, children face the risk of internet addiction that could be a result of increased time spent online, especially if it is unsupervised or unfettered. Here we have enlisted some signs that you may look out for among your friends/peers in order to identify abuse and addiction before it gets increasingly complex and difficult to deal with.

How can you identify if you are getting increasingly dependent on the internet and if you're susceptible to abuse?

Answer the following questions in "Yes/No":

1. Do you feel like you can't control your screen use?
2. Is there a loss of interest in activities other than your online interactions?
3. Does your online presence ("likes" etc.) preoccupy your thoughts?
4. Does your digital interaction interfere with other aspects of your socialisation, like your time spent with your friends, family, etc.?
5. Do you feel highly irritable, experience mood swings or anger outbursts when your screen time is curbed?
6. Do you find yourself being secretive or lying about your screen time/use?
7. Are social media chats, video games, online browsing your preferred way to make yourself feel better after a bad day?
8. Do you have regular interactions with an adult online who may be going out of their way to make you comfortable and gain your trust by sharing details of their life, getting to know about yours, sending gifts and showering you with compliments often?

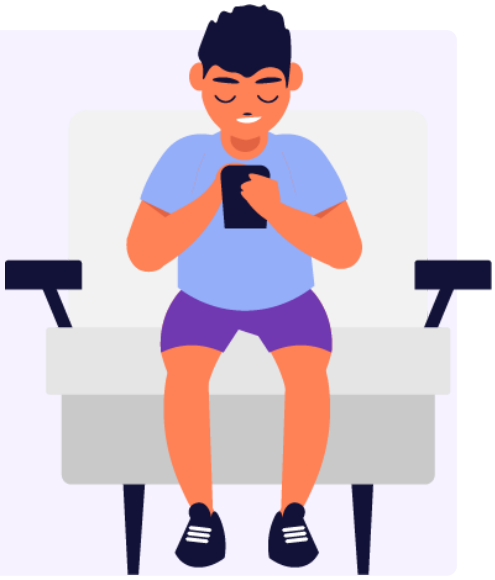
If your answer is 'Yes' to most of the above questions, then you might be beginning to form a digital addiction or you may be susceptible to online abuse.

Students'/Children's Responsibilities

As you know, there are multiple offences happening in the cyber world. By now, you may have realised that you can also be a victim and that therefore, it is important to ensure that you are cautious of your online activities. A wrong click can lead to negative consequences. Therefore, caution can definitely help you prevent many offences.

Fundamental Principles for Children

1. Follow principles of digital etiquette, be aware and responsible while using digital platforms.
2. Do not share passwords, even with your closest friends.
3. Never let your friends borrow your electronic gadgets unsupervised.
4. Never share your photos, turn on your webcam, while playing online games or during chat.
5. Do not engage in video chats with strangers.

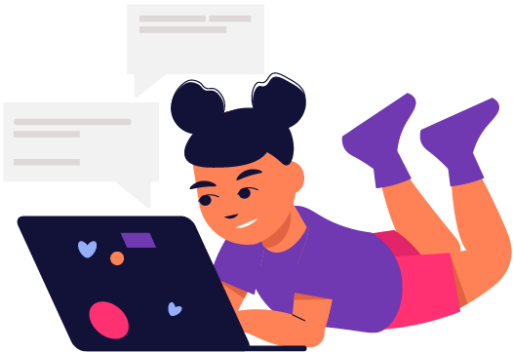


How to prevent cyber abuse: Do's and Don'ts

Given below are key principles to follow while using services in cyberspace:

Do's

- Be positive in your online interactions; always be tolerant, empathetic and respectful while using the internet.
- Pause and think before posting, commenting and sending out emails.
- Check attachments and pop-ups for viruses before clicking or downloading any file.



- Keep your browser updated and use plug-ins to prevent accidental visits to suspicious sites.
- Learn from others about how to judge the quality and reliability of information online. Always inform/take permission from trusted adults before accessing online spaces.
- Create strong passwords and frequently change them to prevent misuse.

- Read privacy settings carefully on social networking sites.
- Keep personal and private information confidential. Protect your identity and data as much as possible.
- Stay away from websites/content that are unknown/questionable.
- Use secure and legal sites to download music, movies or games. Ensure that a firewall is installed in any device you use.

- Understand digital footprints; you should only post information you wouldn't mind if your teachers, parents or a future employer saw.
- Do not meet in person with people whom you've only talked to online. People may not really be who they seem/claim to be online.

- Report immediately to the support team of a networking site if you suspect your account has been hacked.
- Learn how to block and report content that is inappropriate or makes you uncomfortable; set up high safety and privacy settings on social networks.
- Always log out of your accounts after using devices that are not your own.

- Attend any training on cyber security conducted by institutions in order to stay updated on new forms of online fraud/abuse.
- Be aware of fake news and always verify information received online before forwarding it.
- Be wary of people who come across as overly friendly online.
- Enable two-step authentication on email and social networking accounts.

Don'ts

- Do not send your mobiles, laptops etc. for repair before first clearing your data from the SIM/phone/laptop.
- Do not post anything online that you would not want there forever.
- Do not access internet services completely unsupervised or in a secretive manner.
- Do not copy things straight off the internet when doing your homework or assignments.
- Never share personal information or contact details (like address, phone number, location etc.) about yourself or anyone else on any platform.

- Never share images, videos or audio clips with personal or inappropriate content of yourself or anyone else.
- Avoid being friends with strangers on social media platforms.
- Do not feel scared or ashamed to inform trusted adults if you were abused at any point of time. Remember you are not alone.

- Do not entertain any requests from strangers or friends online that seem inappropriate or makes you uncomfortable.
- Do not respond to bullying, obscene or offensive messages, but save the evidence- do not delete the message. Share with trusted adults.
- Do not install apps or games on your devices from unknown sources.
- Never give away your account username or password to anyone.

- Do not indulge in risky behavior online e.g. sharing or writing hateful material, posting/distributing sexual images.
- Never save passwords when browsing the internet on devices that are not your own.
- Do not create fake profiles for yourself or others on any social networking site.
- Don’t use personal USBs or hard drives on public computers.

- Do not feel compelled to share intimate or personal details like one's physical or sexual experiences to anyone.
- Do not indulge in any form of give and take of sexually explicit imagery, pictures, videos etc.
- Never turn on your webcam for any unknown person. Even if the camera is off, cover the camera with a sticker.
- Do not indulge in playing online games that encourage self-harming behaviour.

Digital etiquette: What is it and why is it important for you?

Digital etiquette is about being aware of and behaving in an appropriate, responsible and ethical manner while using digital devices and technology. This includes shaping your digital reputation and being a responsible citizen of your school groups, gaming groups, and social networks. By following these principles, cyber offences such as cyber stalking, bullying etc. can be prevented to a great extent.

Being positive online

You should take an active role in building supportive online communities. Here are some things you can do to contribute to a positive online environment. As a responsible digital citizen, always review your messages and posts to be sure that they are not untruthful, negative, sarcastic or rude.

- Post positive and truthful articles
- Do not mislead others. Check facts before providing information or advice online. Misinformation leads to confusion, divisions among people and wastage of resources and time.
- Avoid posting rumours or gossip online
- Do not forward messages that promote “good luck.” Many viruses are spread via chain messages and invitations.
- Always seek permission from your friends before uploading their picture. This is a matter of privacy and is thus important that you refrain from posting pictures without the consent of the concerned person/s.

Respectfully disagree

Respectfully disagree; this should be the norm while engaging on social media. Respect the opinions of your classmates. If you feel the need to disagree, do so respectfully and acknowledge the valid points in your classmate's argument on social media posts or chats. Acknowledge that others are entitled to have their own perspective on the issue.

Avoid "digital drama"

Avoid hurtful comments, mean-spirited rumours, and embarrassing photos which are termed as digital drama. Digital drama is a common online occurrence. Such posts spread quickly and may cause immense harm to someone. Be wise and think twice of the consequences before you post any material online.

Positive response to hate/bullying

You will come across students who spew their profile with hate messages. Reacting in anger at the said situation will not solve the issue. Firstly, as a student, you must be calm and then follow safety strategies- take a break and do something you enjoy, to distract yourself. If you feel like you are being bullied, immediately report to your parents or guardian.

Be an active bystander

If your classmates are involved in bullying/stalking/posting hate messages, please do not react to it in anger. Instead, try to discuss with them the consequences of such acts and engage in constructive dialogues. If and when required, involve adults around you, like your class teacher.

General tips for all students/children: Towards safety and protection in digital spaces

How do I ensure gadget safety?

- Install and run antivirus and anti-malware software on your devices such as laptops and PCs as these programs can block malware. It is advisable to run regular scans on your device/s as that can detect malware that may have gone unnoticed.
- Keep your operating system (OS), browser, and other programs updated. The security systems in updated versions will make your device immune to various threats.
- Use two-factor authentication while using email and other websites such as banking sites. It requires two levels of verification in order to access an account and thus increases security and can reduce cases of fraud and other abuse.
- Before doing an online banking transaction, ensure that the bank has an SSL (Secure Socket Layer) certificate, check the lock sign on the address bar and HTTPS to confirm that you are visiting a secure bank website. This can help you avoid financial frauds.
- Always ensure your important files are backed-up elsewhere. Certain malware programs can delete or corrupt data on your internal drives. The two most common ways of doing this are copying your data to an external drive and using an online backup service.
- Clear cookies and other data once you finish using web browsers.

How to keep yourself safe while accessing online games?

- Read up on the nature of the game before installing the app. Make sure it is legitimate and age-appropriate for you.
- Exercise caution before making in-app purchases on gaming sites.
- Try playing the game with your parents. It would help them understand the risks involved.
- Keep a safe game name such as: SecretNinja99 or Superhero55. Avoid using first or last names or any other personal information like birth year in the username. Keep gender neutral usernames if possible. Use an avatar instead of an actual photo.
- Do not share your photo with any co-gamer or turn on your webcam during the game.

- Set complex passwords for game log-in.
- Do not talk to strangers via chat while playing games.
- Never share personal information like name, location, phone number, age, etc. to any co-gamer.
- Limit gaming hours to prevent a gaming addiction.
- Ensure that gaming does not interfere with other activities that you are involved in.

How do I make myself safe while accessing emails?

- Safeguard your email account by setting strong passwords and change them often.
- If you receive an email from a friend asking for financial help, connect with them to make sure it was sent by them.
- If you receive an email about winning a lottery, do not give personal details or click on any link provided in it.
- Do not click on a link or attachment from an unknown sender.
- If you are using a computer from a cyber cafe, never save passwords on them.
- Do not use public WiFi, especially to share personal information or for financial transactions.

Social Media Privacy Features

For children over 13 years:

To protect the privacy and security of user content, social media platforms have devised various settings and features. As users of these platforms, it is essential that we are aware of, and follow them before continuing operating our accounts. Given below are some such settings provided on popular social media sites.

WhatsApp

- Control who sees your information like Last Seen, Profile Photo, Status.
- Block contacts.
- Report contacts.
- Group Privacy Settings (lets you control who can add you to groups).
- Disable automatic photo or video downloads.
- Enable Screen Lock.
- Disable Live Location.

Facebook

- Privacy Checkup lets you control who can see what you share, your data settings, how people can find you on FB etc.
- Manage Screen Time (with tools like quiet mode and a daily time reminder).
- Block as appropriate.

Instagram

- Make an account private.
- Unfollow someone.
- Manage and filter comments.
- Mute as appropriate.
- Close Friends setting allows you to share stories with a select number of people.
- Restrict an account.
- Report posts or profiles.

Snapchat

- Choose who can contact you.
- Manage chat settings (to limit contact and how long messages last).
- Choose who can view your story.
- Turn off location sharing.
- Report, block or remove people; report inappropriate content.
- Set up two-factor authentication.
- Manage notifications to promote screen time management.

Types of Cyber Crimes: How Do I Identify the Crime?

This section details certain situations that children may come across during digital use. How can you identify the offence/crime that you or your friend might be facing or may potentially face? The section below provides information that will help you identify the issue at hand.

Phishing

Children Ask!

- What is Phishing?
- Online gaming apps keep sending offers and links for free access to game levels. Is that safe?
- My parents got me an add-on card. Can financial information be leaked through it?

CyberPeace Corps Answer!

- Phishing occurs when a fraudster sends the targeted person a spam email/message, either promising prizes or threatening an account suspension if they fail to follow the link provided to re-verify their KYC. If the targeted person falls for the trap and follows the link, their personal information could get stolen or their computer might get infected with a virus.
- For example, “A” is asked to click on a link or go to a site, to win a lottery. Instead of winning the lottery, “A” gets his identity stolen or his computers infected with viruses.
- In recent years, phishing has evolved in new directions, such as targeted spear phishing (via text message) or vishing (using voicemail).
- Smishing: Here the fraudster sends SMSes pretending to represent well-known companies, in order to trick individuals into providing personal information such as passwords and credit card details.

- Vishing: Here too, the purpose is to get innocent people to give out their personal information. The modus operandi though, is to contact people through phone calls or voice messages.
- For example, “A” pretends to be a bank employee and calls “B” asking for his account details, saying that the details are needed to update his account or to provide an updated credit card facility. If “B” falls for the trap and gives out the details, it is then used to commit financial fraud on B.
- In any of the above, a child with a financial prepaid/add-on card with no information on risks, can get impacted in any given manner.

Potential Risks With Online Gaming

Children Ask!

- I spend most of my time online playing video games or attending online classes. Should an increase in my screen time be my only concern?
- Can I be abused while playing a video game online?
- Should I avoid playing online games in order to be safe?

CyberPeace Corps Answer!

- Online gaming may seem harmless but a lot of cybercriminals find it easier to victimise a child on gaming portals as many of these applications are not secure. Some of the risks are mentioned below.

Examples of risks involved in online gaming

- Gamers on gaming apps may bully children.

- Online games contain pop-ups/ads that contain sexually explicit content
- Some people on such platforms may encourage children to cause self-harm. This could be on the pretext of the child not being able to reach a certain level in the game. This could also happen as a result of bullying by fellow gamers
- Adults might pretend to be children on these platforms and persuade them to provide personal information or ask them to meet them personally, share sexually explicit material or sext a child
- Some games show sexually explicit content
- Children can get addicted to online gaming
- Some games may require players to pay an extra amount in order to access advanced game levels. In such cases, the child might end up borrowing/stealing money, or get influenced by anyone who is willing to pay additional amounts on their behalf for the game

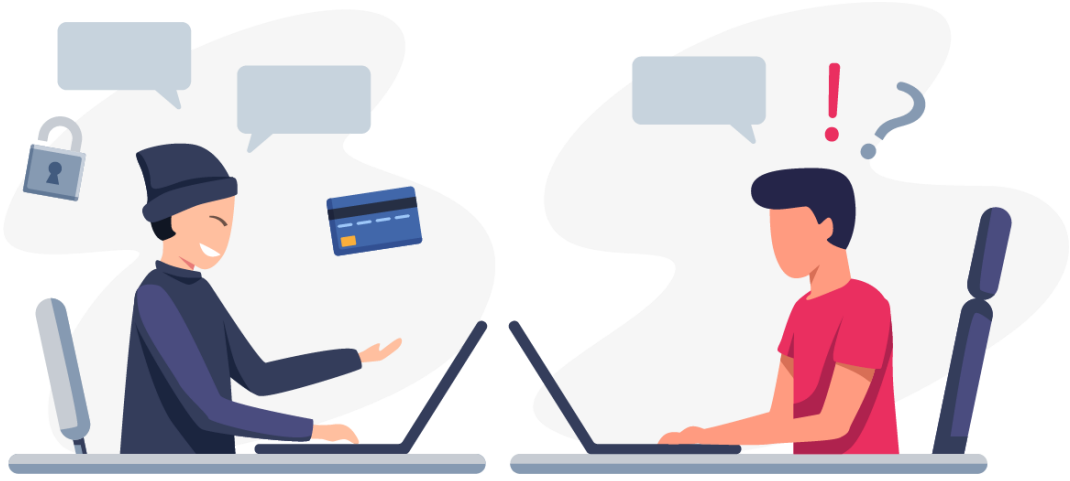
Identity Theft/Impersonation

Children Ask!

- My friend asked me for lewd pictures of myself. I have known him and his family for a long time and this seems very unlike him. How should I proceed?
- My sister was asked for her address by one of her close friends via his Instagram profile. He mentioned that his phone got rebooted so he needs the address. But his parents already have our address. How do I confirm who actually sent that message to my sister?

CyberPeace Corps Answer!

- As it sounds, identity theft involves stealing personal information to be used for fraudulent purposes. Cybercriminals attack individuals or break into corporate systems and steal sensitive information such as credit card details, personal chats, confidential information etc.
- For example, “A” may steal personal information of “B” such as debit/credit card details and engage in online transactions using it.
- Impersonation: In this, the cybercriminal steals a targeted person’s identity and commits a crime using that identity.
- For example, “A” pretends to be “B” post stealing “B’s” personal data to buy pirated games.
- Never share your personal information or pictures online, on anyone’s request, even if they claim to be a friend. Always verify their identity before sharing any information and inform your parents before doing so.



Cyber Bullying

Children Ask!

- My sister has always been into video games. However, since the last couple of weeks, she has stopped playing. She is even hesitant to go online for her classes.
- My brother used to be very proactive in uploading photos and videos of his adventures. However, he recently started avoiding the camera. Could he be facing body shaming or bullying?
- I saw a comment made by a friend of my sister's on one of her pictures posted online. In it, she called her a 'wannabe despo' and commented on her appearance. I am not comfortable with this.

CyberPeace Corps Answer!

- Cyberbullying refers to bullying that takes place over internet-enabled devices like cell phones, computers, and tablets. Cyberbullying can occur through SMS, text, apps, social media, online forums, or gaming platforms over which people can view, participate in, or share content. Cyberbullying includes sending, posting, or sharing negative, harmful, false, or mean content about someone else. It can include sharing personal or private information about someone else causing embarrassment or humiliation.

Some examples of cyberbullying are:

- Posting private or embarrassing photos of others online or sending them to others
- Starting a website that rates someone's appearance or popularity
- Verbally abusing other players in multiplayer online games
- Creating fake Facebook or Twitter accounts to ridicule someone
- Spreading gossip, secrets or rumours about another person that will damage their reputation on social media

Cyber Stalking

Children Ask!

- I am transparent about my online activities with my parents. I recently started getting blocked messages popping up on my device from multiple profiles and numbers.
- Me and my siblings are social media influencers and we upload multiple pictures and videos of our daily lives. One stranger (woman) keeps getting captured in the background of our recent videos. Could this be stalking?
- My brother used to receive lewd texts from different profiles; once he blocked all these profiles and reported them, he started getting the same messages as notes on his bicycle everyday.

CyberPeace Corps Answer!

- Cyber stalking refers to the use of the internet and other technologies to harass or stalk another person online. This online harassment, which is an extension of cyberbullying and in-person stalking, can take the form of emails, text messages, social media posts, and more, and is often methodical, deliberate, and persistent.
- For example, “A” and “B” dated each other for a while but after a while, they ended the relationship. “A” stalks “B” via her pictures on social media handles and finds out that she has been meeting a lot of people. “A” sends emails and chats asking “B” to stop meeting friends. He even threatens her saying that if she continues to meet her friends, he will commit suicide.

Child Sexual Abuse Material (CSAM)

Children Ask!

- I received spam messages and emails with sexually explicit images and video GIFs.
- My sister received a message from an unknown profile on her Instagram account. The message had a violent video attached to it which really disturbed her.
- I received a message from one of my teachers' accounts with explicit photos of the said teacher attached to it.

CyberPeace Corps Answer!

- It involves the recording of child sexual abuse in the form of photographs, video, film or an audio clip. These online platforms show violent and sexualised pictures of children. It includes nude photos, videos, graphics, or animations of a child engaged in a private act in any electronic form.

Few examples are:

- Photographs of children in minimum or no clothes
- Recording of voices of children making sexual sounds
- Recording of children getting involved in sexual acts
- Publishing of videos of children being sexually abused
- Sexting in which children are forced to send sexually explicit messages or view sexually explicit content through chat or other applications.

Online Grooming of Children

Children Ask!

- My sister is interested in anime, so she joined a Facebook group on the topic. She has been interacting with a person from the group for hours on end these days. How do I know if that is safe?
- My brother has been very resigned these days. He picks fights at home and at school. He is spending a lot of time online. His language does not feel like it is coming from him. What could be happening here?

CyberPeace Corps Answer!

- This is when a perpetrator builds an emotional bond with children through social media or messaging platforms with an objective of gaining their trust in order to eventually sexually abuse/exploit them. Online groomers mostly target teenagers as they are curious about engaging in online chat, which can be a medium of risk to online grooming. These offenders can use gaming websites, social media, email, chatrooms, instant messaging etc. to identify and groom children
- For example, “A” pretends to be a younger person having common interests as that of “B” and starts to chat with “B”. Initially “A” initiates friendly conversation like giving compliments, gifts etc. and then moves on to sending obscene messages, photographs or videos to “B.”

Cyber Trafficking

Children Ask!

- A student from my school ran away from home after an argument with her parents. She left a letter where she mentioned having fallen in love with someone she met over an internet site and that she was going to live with him. What can we do as her peers to preempt such a situation?
- I have been shooting videos and posting them online. Recently I started meeting different people who say that they like my videos and would like to cast me in television roles.

CyberPeace Corps Answer!

- Traffickers use online chat-rooms or social media to recruit potential child victims for commercial exploitation. They use online platforms to gain access to and trust of the child and then use the child or the child's images/videos for commercial sexual exploitation and other forms of abuse. These range from forced sexual exploitation, pornography, mail-order brides and forced labour.
- For example, "A" is a trafficker pretending to be a child. "B", a child, enters into a relationship with "A" via chat. "A" then asks "B" to meet him and "B" decides to go ahead with the meeting. "A" then lures "B", and sells "B" to an agent for commercial sexual exploitation.

Revenge Pornography

Children Ask!

- I, under the influence of an older friend, shared a sexually explicit picture of mine with a friend. Later, we had an argument over our marks in school, and now that older boy is threatening to upload my sexually explicit picture online.

CyberPeace Corps Answer!

- Revenge pornography happens when a person's private or sexually explicit picture gets circulated by the offender who was in relationship with that person. Revenge porn is a growing concern among teens nowadays. Some teenage students, who have been in a relationship, find their explicit photographs circulated on social media platforms or their names tagged on such types of pictures. This is done mainly as revenge because the victim ended the relationship.
- For example, "A" and "B" are teens who enter into a relationship. "A" lures "B" to send nude pictures. After a while, "B" decides to break up with "A", resulting in the latter feeling offended and taking revenge by posting "A's" pictures on social media.

Stalkerware

Children Ask!

- I had a fight with my girlfriend. During the argument she made a reference to an online conversation that I had a few days before with a friend, about which I had not made any mention to her or anyone else. How did she get to know of my private conversation?

CyberPeace Corps Answer!

- Software programmes created especially to track people while remaining hidden from view are referred to as stalkerware. These programmes are often used to track down and spy on individuals. It operates by running in stealth mode in the background of a device such as a smartphone. It also masks itself as another app like a camera, calculator, recorder, etc.
- For example, “A” and “B” are teens who enter into a relationship. “A” downloads an app on his girlfriend “B’s” phone without her knowledge to track her online activities and interactions.

Ransomware

Children Ask!

- I was looking for a key to an online game on a low-security website during which a pop-up ad came up, which I closed. But soon after, my cursor started moving on its own and different windows started opening on my system.

CyberPeace Corps Answer!

- A form of virus known as ransomware prohibits or restricts users' access to their systems, either by locking the system's screen or by encrypting the users' files, in exchange for a ransom. Modern ransomware variants, commonly known as crypto-ransomware, encrypt particular file types on compromised systems and demand that users pay a ransom using specific internet payment methods in order to receive a decryption key. This is usually used to get remote access to the systems through malicious websites, infected emails and unknown attachment downloads and public WiFis.
- For example, “A” received an email from “B” with a video attachment. “B” opens the video and is then locked out of her system. Her email, social media accounts, etc. start operating from her system without any action on “B’s” part. She receives a message on her screen asking her to pay 1000 bitcoins in order to put an end to these activities.

Malware Attack

Children Ask!

- We were awaiting an admissions response from a school application. I received an email from a similar email ID as that of the school. When I opened it, my system started acting strangely and various windows started opening on their own. Was it just a one-off incident or did I face a cyber crime?
- My webcam has been turning on without any intervention on my part. What could be causing this?
- I am logged out of all my apps yet there have been unusual activities in my accounts. My cards and phones are all secure. So what could this be?

CyberPeace Corps Answer!

- Malware attack, more popularly known as a virus attack, is when a fraudster uses code or software, with criminal intentions. These fraudsters use malware to attack a targeted person's system, to acquire sensitive information or even threaten the targeted person for money. Some of the different malware they may use include Trojans, viruses, worms, ransomware, and spyware.
- For example, "A" sends an email to "B" which contains malware. "B" opens the email and this causes his entire system to crash. The fraudster then accesses information from the compromised phone/laptop.

References

- https://www.cbse.gov.in/cbsenew/documents/Cyber%20Safety.pdf
- https://www.mha.gov.in/document/downloads/cyber-safety-handbook
- http://cbseacademic.nic.in/web_material/Manuals/Cyber_Safety_Manual.pdf
- https://ciet.nic.in/upload/Safetolearn_English.pdf
- https://www.cbse.gov.in/cbsenew/documents/Cyber%20Safety.pdf

Follow us for more security Tips

/Cyberpeacecorps

CyberPeaceTV