



**CyberPeace** | Foundation

# Cybercrimes And Redressals

Anindita Mishra  
CyberPeace Foundation



# Defining Digital Space

---

Understanding of this space  
and the working of Internet



# Digital Space and the Internet

- Digital space is where we connect using internet-enabled devices.
- It includes basically anything displayed on the screen of your device, including websites, movies, apps, gaming sites, etc.
- We connect in the digital space using the internet.
- Simply speaking, the Internet moves data from client to servers or client to client, via routers. It creates packets using a set of data being sent, sending each data in separate packets that gets reassembled at destination point. This enables thousands of people to use the Internet simultaneously.
- Servers are computers that store information. They can be either web servers, mail servers or file servers.

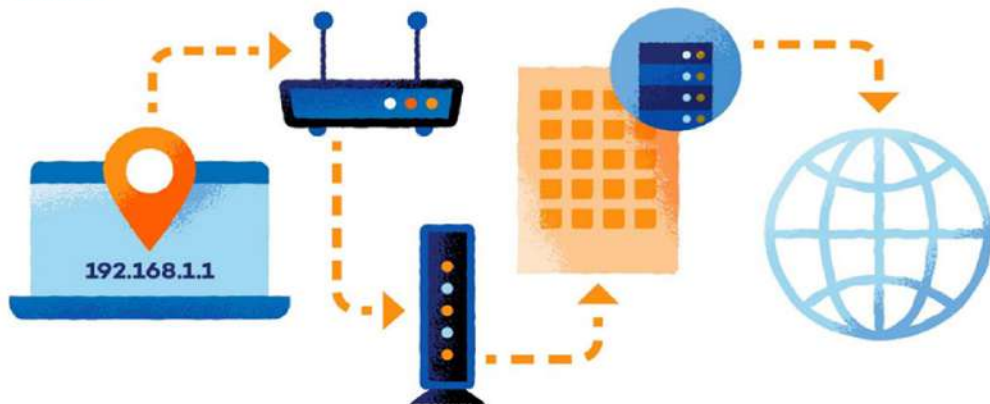


# Digital Communication Simplified



**CyberPeace** Foundation





# https://www.example.com



Protocol

Sub-domain

Domain name

Top level  
domain (TLD)

# Why Children are Vulnerable

- Children are digital orphans- born in the digital world but without the right digital skills set or education.
- They are very active in the digital space and are influenced by what they experience online; including social media, gaming and entertainment apps, micro-blogging sites, news channels, personal vlogs and You-Tube channels.
- They are curious, adventurous, risk-takers, and heavily influenced by peer pressure.
- They pick up digital literacy skills fast but lack foresight and experience.
- They can thus be brainwashed, manipulated, groomed, bullied and/or deceived.
- It is important to educate and encourage children to learn all about digital citizenship from childhood so that they grow up to responsible digital users.



# What Digital Skills Do Children Need?

- 1. Ability to sift truth from fake.
- 2. Have correct knowledge of proper communication skills.
- 3. Practice digital safety, security, and privacy.
- 4. Respect the right and dignity of all users and not abuse technology.
- 5. Understand individual responsibility and accountability.





# Cybercrimes And Its Types



# Cyber Crime

- “Cyber-crimes” are offences relating to computers, information technology, internet.
- A cybercriminal may use a device to access a user’s personal information, government information, or disable a device.



# The Threats

## Threats to Individual

- Harassment
- Revenge Pornography
- Sextortion
- Cyber Obscenity
- Cyber Stalking
- Voyeurism
- Grooming

## Financial and Other Threats

- Phishing
- Financial Frauds
- Fake Apps
- OTP Frauds
- Impersonation
- Trolling
- Cyber Bullying
- Fake news



# Sextortion

- Sextortion is a type of blackmail that happens when someone threatens to share or publish private, sensitive material unless you send them sexually explicit images, perform sexual favors, or give them money

# Cyber Obscenity

- Cyber obscenity is the trading of sexually expressive materials within cyberspace. Legally cyber obscenity is also termed 'pornography'.
- Cyber obscenity is the acts which publish transmit cause to be published "any material", video files, audio files, text files, images, animations, and even CDs, Web sites, Computer, Cell phones, etc.





# Cyber Bullying

- Bullying that occurs over digital devices such as cell phones, laptops, and tablets is known as cyberbullying.
- Cyberbullying can happen online on all social media forums, including audio/video communication forums and gaming sites, where people can view, participate in, or share content.
- Sending, uploading, or spreading unpleasant, harmful, misleading, or nasty content about someone else is considered cyberbullying.
- It can lead to embarrassment or humiliation caused by sharing intimate or private information about another individual.
- Cyberbullying can sometimes cross the line into illegal or criminal action.

# False Information

- Misinformation is incorrect or misleading information presented as fact, mostly unintentionally.
- Disinformation is a subset of misinformation, that which is deliberately deceptive.
- Mal-information is information based on reality but used to inflict harm on a person, organization or nation
- Rumors are information not attributed to any source, and so are unreliable and often unverified, but can turn out to be either true or false.





# Cyber Stalking

Cyberstalking is online harassment that involves the use of the internet and electronics. It is a punishable offence under section 354 D of IPC.

There are several forms of cyberstalking, including:

- Harassing the victim
- Embarrassing and humiliating the victim
- Exerting financial control by emptying the victim's bank accounts, or by ruining his credit
- Isolating the victim by harassing his family, friends, and employer
- Frightening the victim by using scare tactics and threats



# Voyeurism

Voyeurism is the sexual interest in or practice of watching other people engaged in intimate behaviors, such as undressing, sexual activity, or other actions usually considered to be of a private nature.



# Gaming Betting Risky Challenges

- What starts as an interesting pastime, may turn into an addiction.
- Children spend hours playing games at the cost of sleep, food, academics, friends, and sports.
- They are lured by false advertisements to betting sites.
- When parents penalize them, they get violent, to the point of aggression towards parents or self.
- Such children need urgent counselling and therapy.



Upto 40% off\* on premium plans

Subscribe Now

Home / News / India / Law enforcement agencies probing alleged killing under ...

## Law enforcement agencies probing alleged killing under PUBG addiction: MoS



Union minister of state for electronics and information technology Rajeev Chandrasekhar. (PTI)

Home > Tech > News > SHOCKING: PUBG addiction makes Lucknow boy commit this heinous crime

## SHOCKING: PUBG addiction makes Lucknow boy commit this heinous crime

A 16-year-old Lucknow boy murdered his mother after she scolded him for playing online games like PUBG.



CyberPeace Foundation

## 'Online gaming addiction is turning children violent'

TNN / Updated: Jun 10, 2022, 12:26 IST

77 PTS

SHARE

### ARTICLES



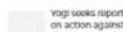
'Online gaming addiction is turning children violent'



Fast-track your journey to being a responsible leader with IT Bombay..



Sadhguru pushes for betmodel to wavenoid in Uttar Pradesh



Yogi seeks report on action against illegal parking lots



Representative image

## Hyderabad: Student squanders Rs 36 lakh on online gaming app

TNN / Updated: Jun 5, 2022, 09:02 IST

77 PTS

SHARE

AA

### ARTICLES



Hyderabad: Student squanders Rs 36 lakh on online...



Jammers installed at AIS exam halls



NEWS / CITY NEWS / LUCKNOW NEWS / 17-year-old kills mom over online game

## 17-year-old kills mom over online game in Lucknow

Pathikrit Chakraborty / TNN / Updated: Jun 9, 2022, 07:32 IST

77 PTS

SHARE

AA

## Kanpur student fakes own kidnapping, demands ransom from family after losing money in online game

A college student staged his own kidnapping after losing money for his fees in an online game in Kanpur. He demanded a ransom of Rs 1 lakh from his family.



Sunil Singh  
Kanpur  
June 20, 2022, 15:01 IST



Others the relatives informed the police about the kidnapping of their son. (Shikhar) the police found him within 24 hours. (Pia Photo)

## Indore man ends life after losing Rs 17,000 in online ludo game

A 23-year-old man allegedly ended his life by hanging himself at his brother-in-law's house in Chaulihary Park area in Indore's Asol Nagar after he lost Rs 17,000 in an online ludo game.



Shantanu Kumar Sharma  
Indore  
June 7, 2022, 12:00 IST



The deceased lost Rs 17,000 in an online ludo game. (Shikhar Representative)



## Impersonated and Fake Profile

- To copy the behavior etc. of or pretend to be (another person), sometimes in order to deceive.





## Cyberpredators

- They demand emotional attachment.
- They isolate you from your network and make you believe they're the only one you can trust.







# Inappropriate Content

- Visual depictions that are obscene, child pornography, or material that is harmful to minors.



# Stay Safe from Cybercrimes

- Use Paid Security Tools
- Sounds tempting? Nothing Comes For Free Online
- Share With Care – never give out personal information, including photos
- STOP. THINK. CLICK.
- Read T&Cs, manage cookies, check permissions asked for
- Follow Rules Online- Even If No Visible Digital Policing Going On
- Set Up Strong Passwords, activate 2FA
- Choose Friends Wisely
- Logout Of All Accounts
- Be Responsible, Realistic, and Resilient
- Practice Digital Balance



# Parents as Enablers

- Extend real life values to the digital world
- Help build your child's confidence
- Encourage them to practice inclusivity, respect, empathy, critical thinking
- Teach them to be responsible and resilient
- Set screentime limits
- Be a role model – limit your own screen time



# Teachers as Enablers

- Talk to children about digital balance, disciplined use
- Take every opportunity to discuss latest cybercrimes, solutions
- Create awareness about current issues like fakes, impersonation, scams, addiction, cyberbullying, scams and grooming
- Set up Cyber Warrior Corps in schools, mentored by a teacher/counsellor
- Emphasize on asking for permission -before tagging pics, copying from online sources, sharing info
- Empower them with the right tools and knowledge on cybersafety, including reporting mechanism



# IT ACT 2000



- Sec 66 B – Theft-Stolen Computer Resource/Device – 3 years Imprisonment with Rs. 1 Lac Fine or both.
- Sec 66 C – Hacking- Password/Electronic Sign/Unique Identity, 3 years Imprisonment with Rs. 1 Lac Fine or both.
- Sec 66 D – Cheating by personation with Computer Resource, 3 years Imprisonment with Rs. 1 Lac Fine or both.
- Sec 66E – Capture/Publish/Transmit- Private Parts Pictures of Body-Without consent- 3 years Imprisonment with Rs. 2 Lac Fine or both.
- Sec 66F – Cyber Terrorism – Life Imprisonment .
- Sec 67 – Publishing or transmitting obscene material in electronic form – 3 years and with fine which may extend to five lakh rupees.
- Sec 67 A – Punishment for publishing or transmitting of material containing sexually explicit act, etc. in electronic form – five years and with fine which may extend to ten lakh rupees.
- Sec 67 B – Punishment for publishing or transmitting of material depicting children in sexually explicit act, etc. in electronic form five years and with a fine which may extend to ten lakh rupees.





## POCSO

### (Protection of Children Against Sexual Offences Act, 2012)

It is a comprehensive law to protect the children from the following offences:

- Sexual assault
- Sexual harassment
- Pornography

It safeguard the interests of the child at every stage of the judicial process by incorporating child-friendly mechanisms for reporting, recording of evidence, investigation and speedy trial of offences through designated special courts.



# Juvenile Justice Act (JJA)

- The JJ Act 2015, sets out that children breaking laws or in need of care, nutrition, shelter, and protection, are to be treated by adopting a child-friendly approach in the adjudication and disposal of matters in the best interest of children and for their rehabilitation through processes provided, and institutions and bodies established, hereinunder and for matters connected therewith or incidental thereto
- The Act pertains to provisions for juveniles (minors) who are found to be in conflict with Indian laws
- Additionally, it sets out provisions for children in need of care and protection.
- The Juvenile Justice (Care and Protection of Children) Amendment Bill, 2018 had been introduced in the Lok Sabha. Its aim is towards the amendment of the Juvenile Justice (Care and Protection of Children) Act, 2015.



# Reporting Mechanisms



# National Cybercrime Reporting Portal

To report any Cybercrime incidence, kindly visit this website:

[https://cybercrime.gov.in/Webform/Crime\\_AuthoLogin.aspx?rnt=1](https://cybercrime.gov.in/Webform/Crime_AuthoLogin.aspx?rnt=1)



Scan QR Code to know more



**CyberPeace** Foundation

भारत सरकार गृह विभाग  
GOVERNMENT OF INDIA MINISTRY OF HOME AFFAIRS

राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल  
National Cyber Crime Reporting Portal

Language

75  
आज़ादी का  
अमृत महोत्सव

IC  
National Cyber Crime Reporting Portal

**Citizen Login**

SELECT STATE: \*

LOGIN ID: \*

MOBILE NO: \*

OTP: \*

[Click Here for New User](#)

[Forgot Login Id](#)

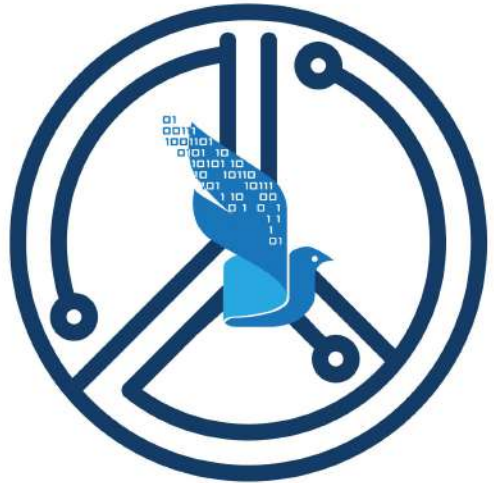
# Where to Report

- National Cybercrime Reporting Portal - <https://cybercrime.gov.in/>
- NCW Helpline - 7827170170 | <http://ncwapps.nic.in/>
- Women Safety Helpline - 112
- For reporting Financial frauds dial - 1930
- Cyber Fraud Helpline - 155260
- CyberPeace Helpline - 9570000066
- Women's helpline numbers to call are 1090, 1091, and 181.
- You can report any inappropriate content on the platform as well



# Find Us Online

- [twitter.com/cyberpeacecorps](https://twitter.com/cyberpeacecorps)
- [facebook.com/cyberpeacecorps](https://facebook.com/cyberpeacecorps)
- [in.linkedin.com/company/cyberpeacecorps](https://in.linkedin.com/company/cyberpeacecorps)
- [instagram.com/cyberpeacecorps](https://instagram.com/cyberpeacecorps)



**CyberPeace**  
— Corps —



# Find Us Online

- [twitter.com/cyberpeacengo](https://twitter.com/cyberpeacengo)
- [facebook.com/cyberpeacefoundation](https://facebook.com/cyberpeacefoundation)
- [instagram.com/cyberpeacefoundation](https://instagram.com/cyberpeacefoundation)
- [in.linkedin.com/company/cyberpeacefoundation](https://in.linkedin.com/company/cyberpeacefoundation)



**CyberPeace**  
— Foundation —



CyberPeace  
Foundation

# THANK YOU