



Rising Online Child Abuse

For Prelims: [Artificial Intelligence](#), [National Cyber Security Policy](#), [Cyber Surakshit Bharat Initiative](#)

For Mains: Impact of cyberbullying and online sexual exploitation on children, Issues Related to Children

[Source: HT](#)

Why in News?

A study published in **The Lancet**, based on a comprehensive analysis of **123 studies** from various regions, has highlighted the **growing concern of online sexual abuse** faced by children worldwide.

What are the Key Findings of the Study on Online Child Abuse?

- **Prevalence of Abuse:** It highlights that **one in 12 children globally** (approximately **8.3%**) has **experienced online sexual abuse** in the last decade.
- **Types of Exploitation:** The study identified several subtypes of online sexual abuse, including **online solicitation** involving sexual inquiries/conversations (12.5%), **non-consensual image sharing** (12.6%), **online sexual exploitation** (4.7%), and **sexual extortion** (3.5%).
- **Gender Dynamics:** There is **no significant difference in online abuse rates between boys and girls**, challenging earlier beliefs that girls are more vulnerable.
 - This suggests **changing online environments and behaviors**, with **increasing risks for boys**.
- **Mental Health Implications:** The report links online sexual exploitation to **severe mental and physical health consequences** for victims, including **lower life expectancy** and reduced employment prospects.

What are the Reasons for Rising Online Child Abuse?

- **Increased Internet Access:** **Widespread internet access** has significantly **increased children's online presence (1/3 of internet users)** rendering them vulnerable to exploitation, especially in unsupervised social media and gaming.
- **Pandemic-Related Factors:** Increased online activity during [Covid-19 pandemic](#) enabled **offenders to exploit children**, leading to a surge in abuse cases, including a **threefold rise in sextortion since March 2020**.
- **Advancements in Technology:** The large number of **artificial intelligence (AI)** tools and **digital platforms** has made it easier for offenders to create and distribute **child sexual abuse material (CSAM)** that is difficult to **detect and trace**.
- **Lack of Digital Literacy:** **Limited awareness of online safety** makes users vulnerable; only **38% of Indian households are digitally literate**.
- **Inadequate Monitoring and Enforcement:** Law enforcement and technology companies face

challenges in keeping up with **rapidly evolving online platforms**, leaving **gaps in monitoring and enforcement**.

India's Initiatives Related to Online Child Abuse

- **Legislative and Policy Measures:**
 - [Protection of Children from Sexual Offences \(POCSO\) Act, 2012](#) provides a **legal framework** to combat child sexual abuse, including **online exploitation**.
 - [Information Technology \(IT\) Act, 2000](#) contains provisions related to **cybercrimes against children**.
 - [Juvenile Justice \(Care and Protection of Children\) Act, 2015](#) addresses **child protection issues, including online abuse**.
- **Institutional Mechanisms:**
 - [National Cyber Crime Reporting Portal](#): Enables reporting of **online child abuse cases**.
 - [Indian Cyber Crime Coordination Centre \(I4C\)](#) strengthens law enforcement efforts against **cybercrimes, including child exploitation**.

What Measures Can Be Taken to Prevent Online Child Abuse?

- **Strong Legislation and Enforcement:**
 - **Stronger Legislation:** Implement **stricter legal frameworks** with enhanced penalties for offenders.
 - **International Cooperation:** Strengthen **collaboration with agencies** like **INTERPOL and FBI** to dismantle **cross-border abuse networks**.
 - **Robust Reporting Systems:** Improve **real-time reporting and monitoring tools** for social-media platforms, **establish confidential helplines**, and encourage social networks to report emerging ways to share abuse material.
- **Public Awareness and Education:** Promote **digital literacy and online safety** through **awareness campaigns** for children, parents, and educators.
 - Enhance **online safety through dedicated kids' sections**, features like **"safe search"** on social media and browsing platforms, [Artificial Intelligence \(AI\)](#)-based content filtering, and **parental controls**.
- **Collaboration with Tech Industry:** Encourage tech companies to **adopt stricter content moderation, better age-verification**, and develop **ethical AI tools** to prevent CSAM creation on dark web platforms.
- **Need for Further Research:** Invest in **extensive research and data collection**, especially in underrepresented regions around the world, to develop **evidence-based policies** and **strengthen child protection frameworks**.

Drishti Mains Question:

Discuss the state of cybercrime in India and its impact on children. Suggest measures to mitigate these threats.

UPSC Civil Services Examination, Previous Year Question (PYQ)

Prelims

Q.1 In India, under cyber insurance for individuals, which of the following benefits are generally covered, in addition to payment for the loss of funds and other benefits? (2020)

1. Cost of restoration of the computer system in case of malware disrupting access to one's computer

2. Cost of a new computer if some miscreant wilfully damages it, if proved so
3. Cost of hiring a specialised consultant to minimise the loss in case of cyber extortion
4. Cost of defence in the Court of Law if any third party files a suit

Select the correct answer using the code given below:

- (a) 1, 2 and 4 only
- (b) 1, 3 and 4 only
- (c) 2 and 3 only
- (d) 1, 2, 3 and 4

Ans: (b)

Q.2 In India, it is legally mandatory for which of the following to report on cyber security incidents? (2017)

1. Service providers
2. Data centres
3. Body corporate

Select the correct answer using the code given below:

- (a) 1 only
- (b) 1 and 2 only
- (c) 3 only
- (d) 1, 2 and 3

Ans: (d)

Mains

Q. What are the different elements of cyber security ? Keeping in view the challenges in cyber security, examine the extent to which India has successfully developed a comprehensive National Cyber Security Strategy. **(2022)**