गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS
सत्यमेव जयते

Indian Cyber Crime Coordination Centre

ऑनलाइन अपराध और शोषण से बच्चों की सुरक्षा

बच्चा कौन है, ऑनलाइन अपराधी किस तरह काम करते हैं,
कानून आपसे क्या अपेक्षा करता है, और शक होते ही आपको क्या करना है।

1098
चाइल्ड हेल्पलाइन

1930
साइबर वित्तीय अपराध

112
आपातकालीन सेवा

cybercrime.gov.in
ऑनलाइन शिकायत करें

1 बच्चा कौन है?

भारत में बच्चे की कानूनी परिभाषा, और 18 का अंक आगे सब कुछ क्यों तय करता है।

2 डिजिटल सच्चाई

बच्चे ऑनलाइन असल में कहाँ समय बिताते हैं और उन तक पहुँचना क्यों आसान है।

3 अपराधी कैसे काम करते हैं

ग्रूमिंग, सेक्सटॉर्शन, CSEAM, बुलिंग, गेमिंग, डीपफेक, तस्करी।

4 चेतावनी के संकेत

बच्चे के व्यवहार और उसके डिवाइस में क्या बदलता है - और वे चुप क्यों रहते हैं।

5 कानून और शिकायत

POCSO, आईटी एक्ट, BNS, JJ एक्ट, DPDP - और रिपोर्ट करने का आपका कानूनी कर्तव्य।

6 रोकथाम और प्रश्नोत्तर

माता-पिता, विद्यार्थियों, स्कूलों और पूरे समुदाय के लिए व्यावहारिक कदम।

भाग 1

बच्चा कौन है?

बच्चों की रक्षा से पहले यह स्पष्ट होना ज़रूरी है कि कानून किसकी रक्षा कर रहा है - और वह एक अंक, 18, सब कुछ क्यों बदल देता है।

भारतीय कानून में 18 वर्ष से कम आयु का हर व्यक्ति बच्चा है

POCSO अधिनियम, 2012

धारा 2(1)(घ): 'बालक' का अर्थ है अठारह वर्ष से कम आयु का कोई भी व्यक्ति। यह अधिनियम पूरी तरह लिंग-निरपेक्ष है - लड़के, लड़कियाँ और किसी भी लिंग पहचान के बच्चे समान रूप से संरक्षित हैं।

किशोर न्याय अधिनियम, 2015

बच्चा वह व्यक्ति है जिसने अठारह वर्ष पूरे नहीं किए हैं - इसमें कानून से संघर्षरत बच्चे और देखरेख व संरक्षण के जरूरतमंद बच्चे, दोनों शामिल हैं।

आईटी अधिनियम, 2000 - धारा 67B

बाल यौन शोषण सामग्री के अपराध के लिए 'बच्चा' वह व्यक्ति है जिसने अठारह वर्ष पूरे नहीं किए हैं।

डीपीडीपी अधिनियम, 2023

बच्चा वह व्यक्ति है जिसने अठारह वर्ष पूरे नहीं किए। बच्चे का डेटा इस्तेमाल करने से पहले प्लेटफॉर्म को माता-पिता की सत्यापित सहमति लेनी होगी।

बाल अधिकारों पर संयुक्त राष्ट्र समझौता

अनुच्छेद 1: अठारह वर्ष से कम आयु का हर मनुष्य। भारत ने 1992 में इसकी पुष्टि की।

भारतीय वयस्कता अधिनियम, 1875

भारत में वयस्कता की सामान्य आयु अठारह वर्ष है। इससे कम आयु में व्यक्ति इन मामलों में कानूनी रूप से मान्य सहमति नहीं दे सकता।

वह एक अंक सब कुछ क्यों तय करता है

इस परिभाषा से सीधे निकलने वाले चार परिणाम।

बच्चा सहमति नहीं दे सकता

18 वर्ष से कम आयु में यौन कृत्य या यौन सामग्री के लिए सहमति का कोई कानूनी अर्थ नहीं है। 'वह मान गई थी', 'उसने खुद भेजा था', 'दोनों रिश्ते में थे' - ये बचाव नहीं हैं।

आयु पर संदेह हो तो अदालत तय करती है

POCSO की धारा 34 के अनुसार विशेष न्यायालय आयु निर्धारित कर उसके कारण दर्ज करेगा। 'बच्चा बड़ा दिखता था' कहकर अपराधी बच नहीं सकता।

तस्वीर ही अपराध है

18 वर्ष से कम आयु के व्यक्ति की कोई भी यौन तस्वीर या वीडियो बाल यौन शोषण सामग्री (CSEAM) है - भले ही बच्चे ने स्वयं बनाई हो, भले ही स्वेच्छा से साझा की गई हो।

चुप्पी स्वयं एक अपराध है

POCSO की धारा 19 के तहत अपराध की जानकारी रखने वाले हर व्यक्ति को रिपोर्ट करना अनिवार्य है। रिपोर्ट न करना धारा 21 के तहत दंडनीय है।

लोग जो छह बातें कहते हैं - और कानून वास्तव में क्या कहता है

लोग क्या कहते हैं	कानून क्या कहता है
“दोनों रिश्ते में थे, इसलिए यह अपराध नहीं है।”	18 वर्ष से कम आयु में कोई मान्य सहमति होती ही नहीं। वयस्क, या जिसने वह सामग्री प्राप्त की, अपराध का दोषी है।
“POCSO सिर्फ लड़कियों की रक्षा करता है।”	POCSO लिंग-निरपेक्ष है। बड़ी संख्या में लड़के भी पीड़ित होते हैं, और उनके मामले बहुत कम दर्ज होते हैं।
“उसने सिर्फ देखा था; बनाया या भेजा तो नहीं।”	सितंबर 2024 में उच्चतम न्यायालय ने कहा कि ऐसी सामग्री डाउनलोड करना, रखना या देखना भी POCSO और आईटी एक्ट के तहत अपराध है।
“यह तो बस एडिट की हुई फोटो है, कुछ हुआ ही नहीं।”	बच्चे की मॉर्फ की गई या AI से बनाई गई यौन तस्वीरें भी शोषण सामग्री मानी जाती हैं। बच्चे को होने वाली हानि असली है और अपराध भी।
“यह ऑनलाइन हुआ है, इसलिए असली शोषण नहीं है।”	POCSO और आईटी एक्ट दोनों लागू होते हैं, चाहे सामग्री ऑनलाइन बनी हो या ऑफलाइन। ऑनलाइन ग्रूमिंग, धमकी और शोषण दंडनीय अपराध हैं।
“यह घर का मामला है; हम खुद निपट लेंगे।”	POCSO की धारा 19 के तहत रिपोर्ट करना कानूनी कर्तव्य है। आपस में समझौता करना अपराधी को बचाता है और बच्चे को असुरक्षित छोड़ देता है।

भाग 2

डिजिटल सच्चाई

आज कोई अजनबी बच्चे तक कुछ ही सेकंड में पहुँच सकता है - उस डिवाइस के ज़रिये जो बच्चे की जेब में है, उस कमरे में जहाँ बड़े उसे पूरी तरह सुरक्षित मानते हैं।

बच्चे असल में कहाँ हैं - और उन तक कैसे पहुँचा जाता है

इनमें से हर जगह पर डायरेक्ट मैसेज या वॉइस चैट का ऐसा रास्ता है जिसे कोई अजनबी इस्तेमाल कर सकता है।

सोशल मीडिया और मैसेजिंग

पब्लिक प्रोफाइल, स्टोरी रिप्लाई, DM रिक्वेस्ट, गायब हो जाने वाले मैसेज, गुमनाम सवाल पूछने वाले ऐप।

ऑनलाइन गेम

इन-गेम चैट, वॉइस चैनल, गिल्ड और क्लैन, तथा एहसान चढ़ाने के लिए स्किन, कॉइन और पास के तोहफे।

शॉर्ट वीडियो और लाइवस्ट्रीम

कमेंट सेक्शन, ड्युएट, गिफ्टिंग फीचर, और वायरल होने का आकर्षण।

पढ़ाई और होमवर्क ऐप

ट्यूटर चैट, डाउट सॉल्विंग ग्रुप, मैसेजिंग ऐप पर बिना निगरानी वाले स्टडी ग्रुप।

फैन और रुचि समूह

किसी गेम, बैंड, खेल या फैंडम के इर्द-गिर्द बने सर्वर और ग्रुप, जिनमें अक्सर वयस्क सदस्य भी होते हैं।

परिवार के और साझा डिवाइस

छोटे भाई-बहन को दिया गया पुराना फोन, साझा टैबलेट, बिना लॉक और बिना निगरानी वाला फोन ।

असली कारण ऐप नहीं है। असली कारण है एक वयस्क अजनबी और बच्चे के बीच का निजी चैनल, जिस पर कोई दूसरा बड़ा नज़र नहीं रख रहा।

भाग 3

अपराधी कैसे काम करते हैं

ऑनलाइन शोषण शायद ही कभी अचानक होने वाला हमला होता है। यह एक धैर्यपूर्ण प्रक्रिया है जिसके चरण पहचाने जा सकते हैं - और इसीलिए इसे बीच में रोका जा सकता है।

आठ खतरे, जिनके नाम आपको पता होने चाहिए

ज़्यादातर असली मामलों में इनमें से दो या तीन एक साथ होते हैं, सिर्फ एक नहीं।

ऑनलाइन ग्रूमिंग

एक वयस्क बच्चे का यौन शोषण करने के इरादे से उसका भरोसा जीतता है।

सेक्सटॉर्शन

और तस्वीरें भेजने या पैसे देने के लिए बच्चे की तस्वीरें सार्वजनिक करने की धमकी देना।

CSEAM (बाल यौन शोषण सामग्री)

बाल यौन शोषण सामग्री बनाना, साझा करना, रखना या देखना।

साइबर बुलिंग

साथियों द्वारा लगातार अपमान, बहिष्कार, धमकी या ट्रोलिंग।

साइबर स्टॉकिंग

बच्चे की इच्छा के विरुद्ध लगातार निगरानी, संपर्क और लोकेशन ट्रैकिंग।

डीपफेक और मॉर्फिंग

किसी असली, पहचाने जा सकने वाले बच्चे की AI से बनाई या एडिट की गई यौन तस्वीरें।

बहलाना और तस्करी

बच्चे को कहीं ले जाने के लिए नकली नौकरी, मॉडलिंग ऑफर, छात्रवृत्ति या प्रेम का इस्तेमाल।

धोखाधड़ी और पहचान की चोरी

गेमिंग स्कैम, नकली गिवअवे, अकाउंट हैक, बच्चे के डेटा का दुरुपयोग।

ग्रूमिंग: भरोसा जानबूझकर गढ़ना

शोषण आखिरी कदम है, पहला नहीं। उससे पहले की हर बात तैयारी है।

ग्रूमिंग क्या है

वह प्रक्रिया जिसमें एक वयस्क जानबूझकर बच्चे से भावनात्मक जुड़ाव बनाता है, ताकि उसकी सतर्कता कम कर सके, उसे संरक्षक बड़ों से अलग कर सके और अंततः उसका यौन या व्यावसायिक शोषण कर सके।

ग्रूमर धैर्यवान होते हैं। हफ्तों-महीनों की साधारण, अपनेपन भरी और ध्यान देने वाली बातचीत संयोग नहीं, एक निवेश है। जब तक कुछ यौन माँगा जाता है, बच्चे को लगता है कि वह अपने सबसे करीबी दोस्त से बात कर रहा है - और वह उस दोस्ती को बचाने की ज़िम्मेदारी अपने ऊपर महसूस करता है।

यह जानबूझकर धीमी होती है

हफ्तों में बना भरोसा बच्चे के लिए एक चौंकाने वाले मैसेज की तुलना में कहीं ज़्यादा मुश्किल से संदेह के घेरे में आता है।

आमतौर पर यह भेस बदला हुआ अजनबी नहीं होता

कई अपराधी बच्चे को ऑफलाइन भी जानते हैं - रिश्तेदार, ट्यूटर, कोच, पड़ोसी या बड़ी उम्र का साथी।

यह किसी कमी को निशाना बनाता है

अकेलापन, घर का तनाव, आत्मविश्वास की कमी, बड़ा दिखने की चाह। ग्रूमर ठीक वही देता है जिसकी कमी है।

छिपाव ही असली संकेत है

जो भी वयस्क बच्चे से कहे कि यह रिश्ता माता-पिता से छिपाकर रखो, वह सीमा पार कर चुका है - बाकी चाहे कुछ भी हुआ हो या न हुआ हो।

छह चरण - और आप यह कड़ी कहाँ तोड़ सकते हैं

आखिरी चरण पर पकड़ना ज़रूरी नहीं। किसी भी पहले चरण को रोक देना ही इसे खत्म कर देता है।

1 निशाना चुनना

ऐसा बच्चा चुनता है जो अकेला, बिना निगरानी या ध्यान का भूखा लगे। पब्लिक प्रोफाइल इसे आसान बना देती हैं।

2 दोस्ती करना

साधारण बातचीत। समान रुचियाँ। तारीफें। अक्सर हमउम्र या थोड़े बड़े मार्गदर्शक के रूप में पेश आता है।

3 कमी पूरी करना

वही बन जाता है जो बच्चे की सुनता है। तोहफे, गेम करेंसी, रिचार्ज, मोबाइल डेटा, किसी परेशानी में मदद।

4 अलग-थलग करना

“यह हमारा राज़ है।” बातचीत को निजी या गायब होने वाले मैसेज वाले ऐप पर ले जाता है। माता-पिता और दोस्तों की बुराई करता है।

5 यौन रंग देना

पहले मज़ाक, फिर सवाल, फिर तस्वीर की माँग से सीमा टटोलता है। इसे सामान्य और आपसी बताकर पेश करता है।

6 नियंत्रण बनाए रखना

धमकी, ब्लैकमेल, अपराधबोध। “दोष तुम पर भी आएगा।” माँगें बढ़ती जाती हैं; बच्चा खुद को फँसा हुआ महसूस करता है।

कड़ी तोड़ने के मौके

चरण 2 - वह बच्चा जो हर नए ऑनलाइन संपर्क के बारे में माता-पिता को बताता है।
चरण 3 - वह बड़ा जो बिना वजह मिले तोहफे, रिचार्ज या गेम करेंसी पर ध्यान देता है।
चरण 4 - वह परिवार जिसमें माता-पिता से कुछ भी छिपाने की ज़रूरत नहीं।
चरण 5 - वह बच्चा जो जानता है कि तस्वीर की कोई भी माँग का मतलब है: रुको और तुरंत बताओ।

असली चैट में यह कैसा सुनाई देता है

बच्चों को ये वाक्य पहचानना सिखाइए। इनमें से कोई एक भी रुककर किसी बड़े को बताने का कारण है।

"तुम अपनी उम्र से कहीं ज़्यादा समझदार हो। तुम बाकी बच्चों जैसे नहीं हो।"

ऐसी तारीफ जो बच्चे को उसके हमउम्र दोस्तों से अलग कर देती है।

"अपने माता-पिता को मत बताना, वे हमें नहीं समझेंगे।"

जानबूझकर बनाया गया छिपाव - सबसे साफ चेतावनी संकेत।

"चलो वहाँ बात करते हैं जहाँ मैसेज गायब हो जाते हैं।"

ऐसे चैनल पर ले जाना जहाँ न रिकॉर्ड बचे, न निगरानी हो।

"मैंने तुम्हें रिचार्ज / स्किन / गिफ्ट कार्ड भेजा है। कोई बड़ी बात नहीं।"

ऐसा एहसान चढ़ाना जिसे बच्चा चुकाने के लिए बाध्य महसूस करे।

"ज़रा एक सेकंड के लिए कैमरा चालू करो, बस तुम्हें देखना है।"

सीमा टटोलने की पहली कोशिश, जिसे मामूली और हानिरहित बताकर पेश किया जाता है।

"तुम्हारी तस्वीरें मेरे पास हैं। अब रुके तो सबको दिखा दूँगा।"

सेक्सटॉर्शन शुरू हो चुका है। यही मदद माँगने का समय है, माँग मानने का नहीं।

सेक्सटॉर्शन : जाल कैसे बंद होता है

अक्सर एक ही शाम में। रफ्तार और शर्म अपराधी के मुख्य हथियार हैं।

1 संपर्क

किसी आकर्षक अजनबी की दोस्ताना रिक्वेस्ट, अक्सर चुराई हुई प्रोफाइल फोटो के साथ।

2 बढ़ाना

बातचीत बहुत तेज़ी से छेड़छाड़ भरी हो जाती है और वीडियो कॉल या निजी ऐप पर पहुँच जाती है।

3 कैद करना

बच्चे को खुद को उजागर करने के लिए मनाया जाता है, या रिकॉर्डिंग/स्क्रीनशॉट ले लिया जाता है।

4 धमकाना

बच्चे के संपर्कों की सूची दिखाई जाती है। पैसे दो, या और भेजो, वरना सब देख लेंगे ।

5 लगातार वसूली

पैसे देने के बाद भी माँगें कभी नहीं रुकतीं। हर भुगतान साबित करता है कि धमकी काम कर रही है।

यह करें

- तुरंत जवाब देना बंद करें।
- सबसे पहले हर चीज़ का स्क्रीनशॉट लें - प्रोफाइल, मैसेज, माँगें।
- किसी भरोसेमंद बड़े को आज ही बताएँ, कल पर न टालें।
- cybercrime.gov.in पर शिकायत करें या 1930 पर कॉल करें, और पुलिस में शिकायत दर्ज कराएँ।
- बच्चे के लिए 1098 पर कॉल करें और काउंसलिंग की व्यवस्था करें।

यह कभी न करें

- पैसे न दें। भुगतान से चुप्पी नहीं, और माँगें मिलती हैं।
- समय पाने के लिए एक और तस्वीर न भेजें।
- चैट डिलीट न करें - वही सबूत है।
- बच्चे को दोष या सज़ा न दें। यही दोष अगले बच्चे को चुप रहने पर मजबूर करता है।
- अपराधी से खुद सौदेबाजी करने या उसकी पहचान उजागर करने की कोशिश न करें।

CSEAM: यह 'पोर्नोग्राफी' नहीं है, न ही कोई धुँधला क्षेत्र

बाल यौन शोषण एवं दुर्व्यवहार सामग्री - वही शब्द जिसे 2024 में उच्चतम न्यायालय ने अदालतों से इस्तेमाल करने को कहा।

CSEAM किसे माना जाता है

कोई भी फोटो, वीडियो, रिकॉर्डिंग, चित्र या कंप्यूटर से बनी छवि जिसमें 18 वर्ष से कम आयु के व्यक्ति को यौन रूप में दिखाया गया हो। इससे फर्क नहीं पड़ता कि इसे किसने बनाया, बच्चा राज़ी था या नहीं, यह कभी साझा हुई या नहीं, और छवि असली है या AI से बनी।

उच्चतम न्यायालय, सितंबर 2024

न्यायालय ने कहा कि ऐसी सामग्री को डाउनलोड करना, अपने पास रखना या देखना भी POCSO और आईटी एक्ट के तहत अपराध है - आरोपी का उसे बनाना या भेजना ज़रूरी नहीं। न्यायालय ने 'चाइल्ड पोर्नोग्राफी' शब्द छोड़कर CSEAM इस्तेमाल करने का आग्रह भी किया, क्योंकि पुराना शब्द बच्चे के शोषण को मनोरंजन की एक श्रेणी जैसा दिखाता है।

'निजी तौर पर देखना' जैसा कुछ नहीं होता

हर बार देखना माँग पैदा करता है। हर डाउनलोड नया प्रसार है। इसे बनाने के लिए एक असली बच्चे को नुकसान पहुँचाया गया है।

यह कभी पूरी तरह मिटती नहीं

एक बार फैलने के बाद सामग्री की अनगिनत नकलें बनती रहती हैं। इसीलिए रोकथाम, डिलीट करने से ज़्यादा मायने रखती है।

आगे भेजना भी अपराध है

'लोगों को सचेत करने' या 'उस व्यक्ति को बेनकाब करने' के लिए साझा करना भी CSEAM का प्रसार ही है। इसके बजाय शिकायत करें।

मिल जाए तो कार्रवाई करना अनिवार्य है

ऐसी सामग्री सामने आए तो न सेव करें, न आगे भेजें। पुलिस को या cybercrime.gov.in पर इसकी शिकायत करें।

साइबर बुलिंग और साइबर स्टॉकिंग

यहाँ अपराधी अक्सर कोई सहपाठी होता है, अजनबी नहीं - इसीलिए बच्चे के लिए बचना और मुश्किल हो जाता है।

उत्पीड़न और ट्रोलिंग

कई अकाउंट और ग्रुप में बार-बार अपमानजनक मैसेज, कमेंट और मिलकर हमला करना।

राज़ खोलना और डॉक्सिंग

निजी तस्वीरें, चैट, पता, फोन नंबर या भरोसे में बताया गया कोई राज़ सार्वजनिक कर देना।

बहिष्कार

बच्चे को जानबूझकर क्लास ग्रुप, सर्वर और आयोजनों से निकालना, और यह पक्का करना कि उसे पता चले।

फर्जी पहचान बनाना

बच्चे के नाम से नकली प्रोफाइल, जिन पर उसे शर्मिंदा या भड़काने वाली सामग्री डाली जाती है।

पीछा करना और ट्रैक करना

लगातार निगरानी, लोकेशन ट्रैकिंग, और ब्लॉक होने के बाद भी नज़र रखने के लिए नकली अकाउंट।

कभी न रुकने वाला हमला

स्कूल की बुलिंग के उलट, यह बच्चे के साथ घर तक, उसके कमरे तक, रात 2 बजे तक जाता है - और दर्शकों के सामने।

यह 'बच्चों की शरारत' नहीं है। ऑनलाइन पीछा करना BNS की धारा 78 के तहत अपराध है, आपराधिक धमकी धारा 351 के तहत, और बिना सहमति निजी तस्वीर प्रकाशित करना आईटी एक्ट की धारा 66E के तहत। यदि निशाना कोई बच्चा है तो POCSO भी लागू हो सकता है।

तेज़ी से बढ़ते दो रास्ते: गेमिंग और जनरेटिव AI

सबसे नए मामले इन्हीं दो जगहों से आ रहे हैं।

ऑनलाइन गेमिंग और लाइवस्ट्रीम

- वयस्क अजनबियों के साथ वॉइस और टेक्स्ट चैट, जिसका सेशन खत्म होते ही कोई रिकॉर्ड नहीं बचता।
- स्किन, कॉइन, पास और रिचार्ज के तोहफे, जिनसे एहसान और छिपाव पैदा किया जाता है।
- अकाउंट बूस्टिंग के ऑफर, जिनमें बच्चे का लॉगिन माँगकर बाद में अकाउंट बंधक बना लिया जाता है।
- लाइवस्ट्रीम गिफ्टिंग, जिसमें दर्शक जो कहें वह करने पर बच्चे को तुरंत इनाम मिलता है।
- नकली टूर्नामेंट और गिवअवे लिंक, जो लॉगिन, कॉन्टैक्ट और तस्वीरें चुरा लेते हैं।
- रात में लंबे, बिना निगरानी वाले सेशन - वही समय जब कोई बच्चे को टोकने वाला नहीं होता।

AI, डीपफेक और मॉर्फिंग

- पब्लिक प्रोफाइल से ली गई स्कूल या त्योहार की एक साधारण तस्वीर ही पर्याप्त कच्चा माल है।
- मुफ्त ऐप अब कुछ ही मिनटों में असली बच्चे का चेहरा यौन तस्वीरों में लगा सकते हैं।
- क्लोन की गई आवाज़ से बच्चे की नकली मदद-पुकार या दोस्त का नकली संदेश बनाया जाता है।
- गढ़ी हुई तस्वीरों से सेक्सटॉर्शन किया जाता है, भले ही बच्चे ने कुछ भी न भेजा हो।
- कानून की नज़र में यह भी शोषण सामग्री ही है। पहचाने जा सकने वाले बच्चे की मॉर्फ या AI से बनी यौन तस्वीर पर POCSO और आईटी एक्ट की धारा 67B लागू होती है।
- व्यावहारिक बचाव: बच्चों की तस्वीरें पब्लिक प्रोफाइल और खुले ग्रुप से दूर रखें।

बहकाना, तस्करी और नकली अवसर

पेशकश हमेशा वही होती है जिसकी बच्चे या परिवार को सबसे ज़्यादा चाह होती है।

मॉडलिंग और ऑडिशन के ऑफर

“स्क्रीन टेस्ट के लिए तस्वीरें भेजो।” पैसे का वादा होता है, पोर्टफोलियो माँगा जाता है, फिर माँगें बदल जाती हैं।

पार्ट-टाइम नौकरी और इंटर्नशिप के ऑफर

किशोरों को निशाना बनाते नकली वर्क-फ्रॉम-होम ऑफर, जो दस्तावेज़, तस्वीरें और बैंक जानकारी जुटाते हैं।

छात्रवृत्ति और दाखिले के फर्जीवाड़े

नकली फॉर्म, जो आधार, मार्कशीट, पारिवारिक जानकारी और तस्वीरें बटोर लेते हैं।

प्रेम के बहाने फँसाना

महीनों चली ऑनलाइन दोस्ती, जो अंत में अकेले और चुपचाप मिलने आने की माँग पर पहुँचती है।

घर छोड़ने में ‘मदद’ के ऑफर

घर के झगड़े से परेशान बच्चे को कोई अजनबी आसरा या टिकट देने की पेशकश करता है। तस्करी का यह आम रास्ता है।

परिजन बनकर की गई कॉल

क्लोन आवाज़ या फर्जी नंबर से यह कहना कि बच्चा मुसीबत में है, ताकि पैसे ऐंठे जा सकें या किसी को कहीं बुलाया जा सके।

परिवार का एक नियम इनमें से ज़्यादातर को रोक देता है: किसी ऑनलाइन संपर्क के ज़रिये कोई मुलाकात, कोई यात्रा, कोई दस्तावेज़, कोई तस्वीर और कोई भुगतान नहीं - कभी नहीं - जब तक परिवार का कोई बड़ा उसे स्वतंत्र रूप से जाँच न ले।

भाग 4

चेतावनी के संकेत

कोई अकेला संकेत कुछ साबित नहीं करता। पर कई संकेत एक साथ और हाल ही में दिखें, तो यह धीरे से बातचीत शुरू करने का कारण है।

बच्चे में दिखने वाले संकेत

बदलाव, संकेतों का एक साथ आना और समय देखिए - किसी एक नाटकीय लक्षण को नहीं।

भावनात्मक

- अचानक घबराहट, रुआँसा होना या गुस्सा, खासकर फोन इस्तेमाल करने के तुरंत बाद
- परिवार, दोस्तों और पसंदीदा गतिविधियों से दूरी बना लेना
- नींद और भूख में बदलाव; रात भर जागने से थकान
- फँस जाने, बेकार होने या कहीं गायब हो जाने की बात करना - इसे तुरंत गंभीरता से लें

व्यवहार संबंधी

- फोन को लेकर छिपाव; किसी के आते ही स्क्रीन घुमा लेना या छिपा लेना
- डिवाइस माँगने पर घबरा जाना या भड़क जाना
- बिना वजह नए पैसे, रिचार्ज, तोहफे, गेम करेंसी या नया डिवाइस
- स्कूल, ट्यूशन या ऐसी किसी गतिविधि से इनकार जहाँ कोई खास व्यक्ति मौजूद हो

रिश्तों से जुड़े

- कोई नया ऑनलाइन दोस्त, जिसका नाम या ज़िक्र वह नहीं करना चाहता
- उम्र से मेल न खाती वयस्क भाषा, यौन जानकारी या व्यवहार
- कोई बड़ी उम्र का व्यक्ति असामान्य दिलचस्पी ले रहा हो, लिफ्ट, तोहफे या अकेले में समय दे रहा हो
- पुराने दोस्तों को छोड़कर एक ही ऑनलाइन संपर्क में डूब जाना

डिवाइस पर दिखने वाले संकेत - और बच्चे चुप क्यों रहते हैं

इस स्लाइड का दूसरा हिस्सा बताता है कि अक्सर पहला हिस्सा ही आपको क्यों मिल पाता है।

डिवाइस पर

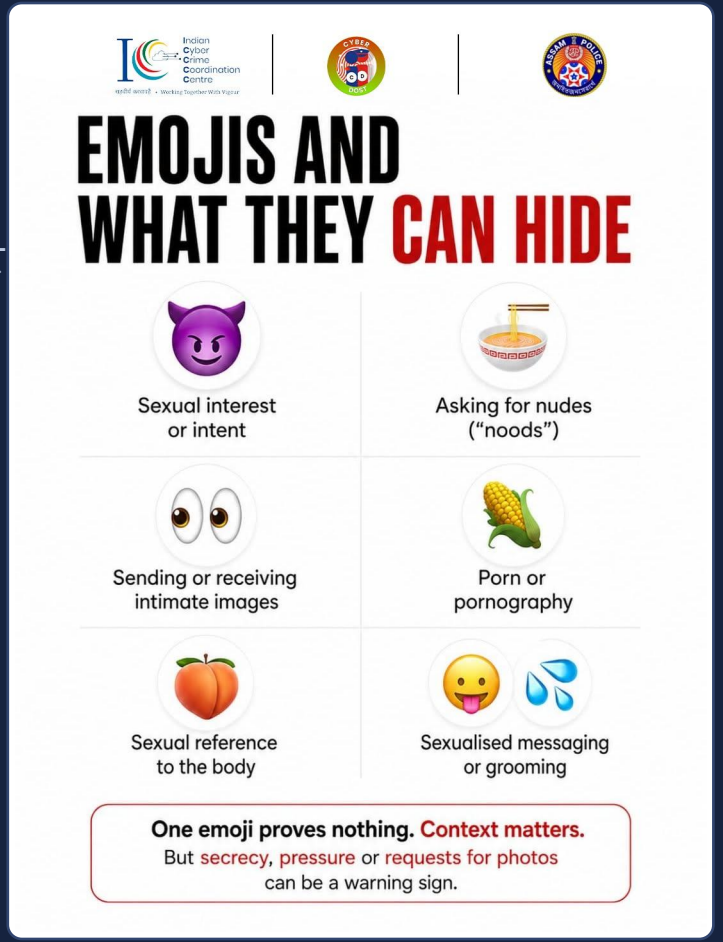
- परिवार की जानकारी के बिना आए नए ऐप, खासकर गायब होने वाले मैसेज या छिपे हुए वॉल्ट वाले ऐप
- चैट, कॉल लॉग या गैलरी बार-बार खाली करना
- एक ही प्लेटफॉर्म पर कई या गुप्त अकाउंट
- डेटा खर्च में बड़ा उछाल, या देर रात भारी इस्तेमाल
- ऐसे वयस्कों के मैसेज, फ्रेंड रिक्वेस्ट या वीडियो कॉल जिन्हें परिवार पहचान नहीं पाता
- पेमेंट ऐप की गतिविधि, गिफ्ट कार्ड की खरीद या इन-गेम टॉप-अप, जिनका बच्चा हिसाब नहीं दे पाता

वे बताते क्यों नहीं

- शर्म - उन्हें लगता है कि जवाब देकर या कुछ भेजकर उन्होंने ही यह करवाया है
- फोन, इंटरनेट या मिली हुई आज़ादी छिन जाने का डर
- अपराधी से ज़्यादा घर की प्रतिक्रिया का डर
- धमकी - अपराधी ने कह रखा है कि सब कुछ उनके परिवार को दिखा देगा
- वफादारी - वे अब भी अपराधी को ऐसा दोस्त मानते हैं जो उन्हें समझता है
- उन्हें पता ही नहीं कि यह अपराध है, या कि इसका कुछ हो भी सकता है

छिपे हुए इमोजी के वे अर्थ जो हर माता-पिता को जानने चाहिए

(ऑनलाइन अपराधी इनका इस्तेमाल बच्चे को ग्रूम करने के लिए कैसे कर सकते हैं।)



भाग 5

कानून और शिकायत कैसे करें

भारत में इसके लिए मज़बूत कानूनी ढाँचा है। सबसे कमज़ोर कड़ी यह है कि ज़्यादातर नागरिक नहीं जानते कि रिपोर्ट करना कर्तव्य है, या कहाँ रिपोर्ट करनी है।

NCRP (राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल)

राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल (NCRP) सरकार का वह मंच है जहाँ नागरिक हर तरह के साइबर अपराध की ऑनलाइन शिकायत कर सकते हैं।

नागरिकों के लिए मुख्य सुविधाएँ

- ✔ **कहीं से भी शिकायत:** किसी भी जगह से साइबर अपराध की ऑनलाइन शिकायत दर्ज करें।
- ✔ **वित्तीय धोखाधड़ी हेल्पलाइन:** ऑनलाइन पैसे की चोरी की शिकायत सिटिज़न फाइनेंशियल साइबर फ्रॉड रिपोर्टिंग एंड मैनेजमेंट सिस्टम के ज़रिये दर्ज कराने के लिए 1930 पर कॉल करें।
- ✔ **गुमनाम शिकायत:** महिलाओं और बच्चों के विरुद्ध संवेदनशील अपराधों की शिकायत अपनी पहचान बताए बिना सुरक्षित रूप से करें।
- ✔ **संदिग्ध की जाँच:** संदिग्ध वेबसाइट लिंक, फोन नंबर या सोशल मीडिया हैंडल जाँचने के लिए "रिपोर्ट एंड चेक सस्पेक्ट" टूल का उपयोग करें।
- ✔ **स्थिति देखें:** अपनी दर्ज शिकायत की प्रगति ऑनलाइन देखते रहें।

NCRP दो कार्यात्मक हिस्सों में बँटा है:

नागरिकों के लिए

साइबर अपराध से जुड़ी शिकायतें दर्ज करने के लिए **cybercrime.gov.in.**

कानून प्रवर्तन एजेंसियों (LEA) के लिए:

निगरानी, जाँच और कानूनी कार्रवाई के लिए **cyberpolice.nic.in**

नागरिक खंड आगे तीन भागों में बँटा है:

महिला एवं बाल संबंधी अपराध

नागरिक घटनाओं की शिकायत **गुमनाम रूप से** कर सकते हैं।

शिकायत **दर्ज करने और उसकी स्थिति देखने** की सुविधा भी है।

वित्तीय धोखाधड़ी

UPI ठगी, कार्ड धोखाधड़ी, क्रिप्टो करेंसी फ्रॉड और बैंकिंग से जुड़े ऑनलाइन वित्तीय अपराधों की शिकायत के लिए।

अन्य साइबर अपराध

साइबर बुलिंग, पीछा करना, फर्जी पहचान और साइबर आतंकवाद जैसे अपराध इसमें आते हैं।

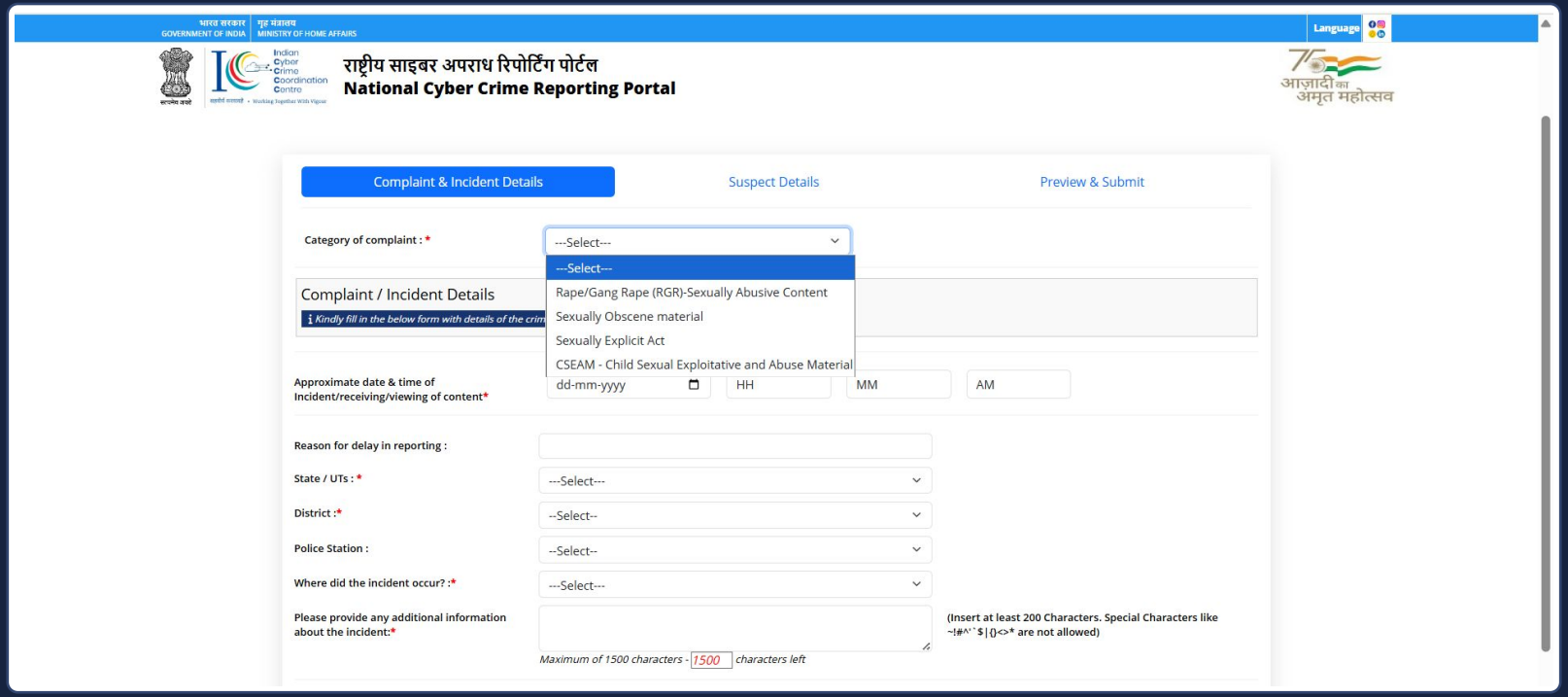
कानून प्रवर्तन एजेंसियों (LEA) के लिए:

यही **वर्गीकरण कानून प्रवर्तन एजेंसियों (LEA)** के पोर्टल पर भी उपलब्ध है, ताकि हर श्रेणी में **निगरानी , जाँच और उचित कानूनी कार्रवाई** की जा सके।

नागरिक शिकायत पोर्टल

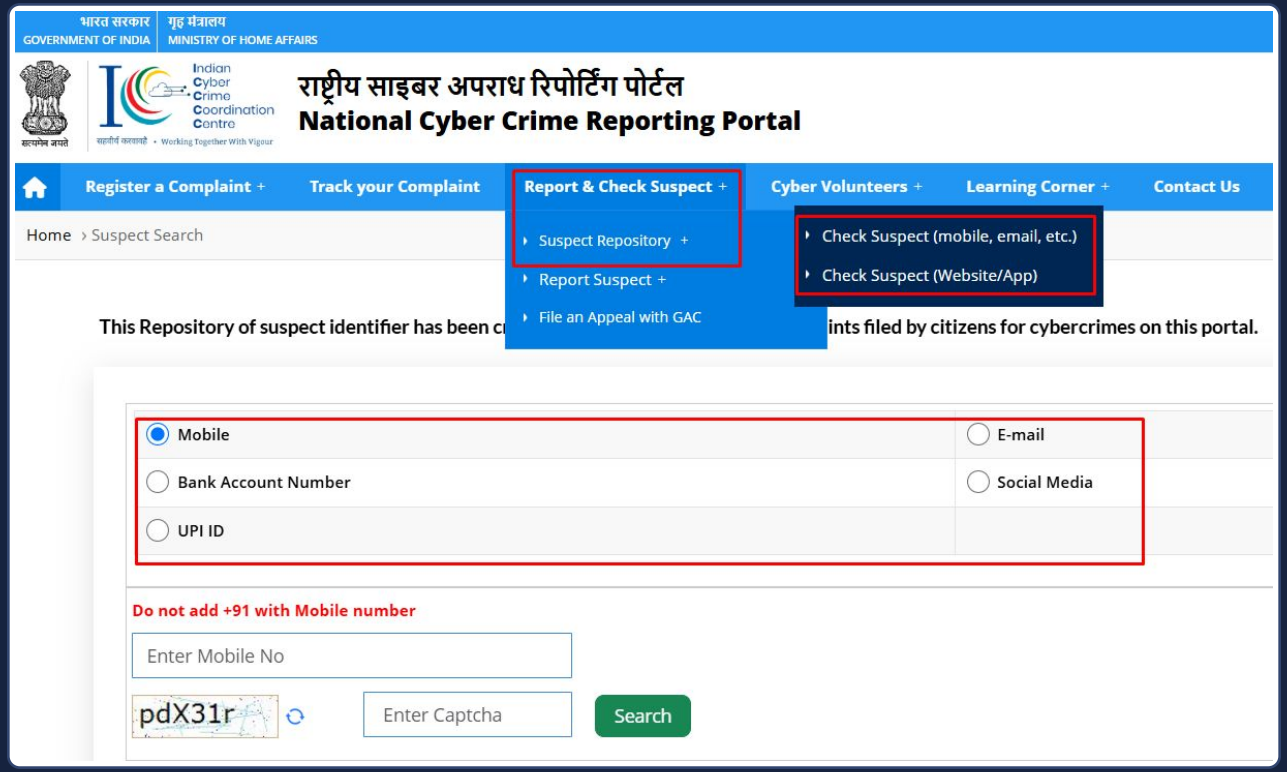
(URL: www.cybercrime.gov.in)

नागरिक ड्रॉप-डाउन मेन्यू से संबंधित श्रेणी चुन सकता है।



नागरिक शिकायत पोर्टल

(URL: www.cybercrime.gov.in)



OCWC, I4C द्वारा की गई कार्रवाई :

हम महिलाओं और बच्चों के विरुद्ध ऑनलाइन अपराध (OCWC) की शिकायतों की प्रतिदिन निगरानी करते हैं। जब भी अश्लील सामग्री वाला कोई सक्रिय लिंक या अकाउंट मिलता है, हम तुरंत सहयोग पोर्टल के माध्यम से उसे हटाने की सिफारिश करते हैं। यही प्रक्रिया सभी राज्य और केंद्र शासित प्रदेश अपनाते हैं।

बाल यौन शोषण एवं दुर्व्यवहार सामग्री (CSEAM) के अपराधियों से जुड़ी कोई भी जानकारी मिलने पर वह उचित कानूनी कार्रवाई हेतु संबंधित राज्य की कानून प्रवर्तन एजेंसी (LEA) को भेजी जाती है।

हम OCWC मामलों की जाँच और निपटान में सभी राज्यों और केंद्र शासित प्रदेशों को तकनीकी और कानूनी सहायता उपलब्ध कराते हैं।

भारत सरकार, गृह मंत्रालय (MHA) के I4C का **महिला एवं बाल ऑनलाइन अपराध (OCWC)** प्रभाग समाज के कमज़ोर वर्गों, विशेषकर महिलाओं और बच्चों को निशाना बनाने वाले साइबर अपराध की बढ़ती चुनौती से निपटने के लिए काम करता है। इंटरनेट की पहुँच बढ़ने के साथ ऑनलाइन उत्पीड़न, सेक्सटॉर्शन, साइबर स्टॉकिंग, CSEAM और शोषण के मामले व्यापक हो गए हैं, जिनके लिए केंद्रित कार्रवाई और रोकथाम की व्यवस्था आवश्यक है ।

रिपोर्ट करना विकल्प नहीं, कानूनी कर्तव्य है।

POCSO की धारा 19 हर व्यक्ति पर लागू होती है - सिर्फ माता-पिता, शिक्षकों और डॉक्टरों पर नहीं।

धारा 19

जिस किसी व्यक्ति को यह आशंका हो कि बच्चे के विरुद्ध अपराध होने वाला है, या जिसे जानकारी हो कि ऐसा अपराध हो चुका है, उसे विशेष किशोर पुलिस इकाई या स्थानीय पुलिस को सूचित करना होगा। बच्चा स्वयं भी शिकायत कर सकता है, और पुलिस को वह जानकारी ऐसी सरल भाषा में दर्ज करनी होगी जो बच्चा समझ सके।

धारा 21 - चुप रहने की कीमत

अपराध की सूचना न देना, या उसे दर्ज न करना, स्वयं में छह माह तक की कैद, या जुर्माना, या दोनों से दंडनीय है। यदि चूक करने वाला व्यक्ति किसी कंपनी या संस्था - स्कूल, हॉस्टल, कोचिंग सेंटर या देखरेख गृह - का प्रभारी है, तो यह एक वर्ष तक की कैद और जुर्माना हो सकता है।

सद्भावना में की गई शिकायत सुरक्षित है

सद्भावना से शिकायत करने वाले व्यक्ति पर कोई दीवानी या आपराधिक दायित्व नहीं आता, भले ही मामला बाद में साबित न हो।

बच्चे की पहचान सुरक्षित रहती है

पीड़ित बच्चे की पहचान मीडिया में उजागर करना प्रतिबंधित है, और POCSO के मुकदमे बंद कमरे में चलते हैं।

कोई समय-सीमा नहीं है

पीड़ित किसी भी उम्र में बाल यौन शोषण की शिकायत कर सकता है। देरी से अपराध समाप्त नहीं हो जाता।

संदेह हो तब भी शिकायत करें

आपको जाँच करने या निश्चित होने की ज़रूरत नहीं। आशंका ही पर्याप्त है। मामले का आकलन करना पुलिस और बाल कल्याण समिति का काम है।

शिकायत कहाँ करें - ये नंबर फोन में सेव रखें

सही माध्यम चुनने की चिंता न करें। इनमें से किसी का भी उपयोग करें, व्यवस्था शिकायत को सही जगह पहुँचा देगी।

1930

राष्ट्रीय साइबर अपराध हेल्पलाइन

साइबर वित्तीय धोखाधड़ी और साइबर अपराध में सहायता के लिए। पैसे जा चुके हों तो सबसे तेज़ रास्ता।

1098

चाइल्डलाइन

देखरेख और संरक्षण के जरूरतमंद बच्चों के लिए 24x7 राष्ट्रीय हेल्पलाइन। नि:शुल्क, और बच्चा खुद भी कॉल कर सकता है।

112

आपातकालीन सेवा

जब बच्चा तत्काल शारीरिक खतरे में हो, या अभी लापता हो।

cybercrime.gov.in

राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल

इसमें महिलाओं और बच्चों के विरुद्ध अपराधों के लिए, शोषण सामग्री सहित, अलग श्रेणी है। शिकायत गुमनाम रूप से भी की जा सकती है।

POCSO ई-बॉक्स

NCPCR शिकायत बॉक्स, ncpcr.gov.in

बच्चे, माता-पिता या किसी भी अन्य व्यक्ति के लिए सरल और गोपनीय ऑनलाइन शिकायत का रास्ता।

स्थानीय पुलिस / SJPU

निकटतम पुलिस स्टेशन

अपराध कहीं भी हुआ हो, FIR किसी भी थाने में दर्ज कराई जा सकती है। ज़ीरो FIR का प्रावधान लागू होता है ।

पहला घंटा: क्या करें और क्या कभी न करें

खासकर सेक्सटॉर्शन के मामलों में, पहला घंटा तय करता है कि आगे कितना नुकसान होगा।

1 शांत रहें और बच्चे के साथ रहें

आपकी पहली प्रतिक्रिया ही बच्चे के लिए इस बात की याद बन जाती है। कहें: मुझे तुम पर भरोसा है, इसमें तुम्हारी गलती नहीं, हम मिलकर इसे ठीक करेंगे।

2 अपराधी से हर संपर्क तोड़ दें

अब कोई जवाब नहीं, कोई भुगतान नहीं, कोई और तस्वीर नहीं। अगर ब्लॉक करने से सबूत तक पहुँच खत्म हो जाए तो अभी ब्लॉक न करें।

3 सबूत सुरक्षित रखें

चैट, प्रोफाइल, URL, यूज़रनेम, भुगतान की जानकारी और समय के स्क्रीनशॉट लें। तारीखें नोट करें। कुछ भी डिलीट न करें।

4 शिकायत करें

cybercrime.gov.in या 1930, और साथ ही पुलिस स्टेशन में शिकायत। सहायता के लिए 1098, और तत्काल खतरा हो तो 112 पर कॉल करें।

5 अकाउंट सुरक्षित करें

पासवर्ड बदलें, टू-स्टेप वेरिफिकेशन चालू करें, जुड़े हुए डिवाइस जाँचें और प्रोफाइल को निजी करें - सबूत सहेजने के बाद।

6 बच्चे को सहारा दिलाएँ

किसी काउंसलर या स्कूल काउंसलर से मिलें। बच्चे में अकेलेपन या निराशा के संकेत दिखें तो जल्द पेशेवर मदद लें।

✕ कभी नहीं

- पैसे कभी न दें। इससे अगली माँग को बढ़ावा और पक्की गारंटी मिलती है।
- समय पाने के लिए एक और तस्वीर कभी न भेजें।
- चैट कभी डिलीट न करें - वही सबूत है।
- अपराधी से खुद कभी भिड़ें, धमकाएँ या सौदा न करें।
- बच्चे के बताने पर सज़ा के तौर पर उसका फोन कभी न छीनें।
- यह सामग्री किसी को भी, चेतावनी देने के लिए भी, कभी साझा न करें - आगे भेजना स्वयं अपराध है।
- मदद माँगते समय बच्चे की तस्वीर या नाम सार्वजनिक रूप से कभी न डालें।

भाग 6

रोकथाम

इसमें से किसी के लिए तकनीकी कौशल नहीं चाहिए। चाहिए बस कुछ आदतें, जो खुलकर तय की गई हों, और एक ऐसा रिश्ता जिसमें सच बोलने पर बच्चे को कभी सज़ा न मिले।

माता-पिता, शिक्षकों और अभिभावकों के लिए

निगरानी नहीं, देखभाल। लक्ष्य है ऐसा बच्चा जो खुद आपको बताना चाहे।

पहली बातचीत जल्दी और शांति से करें

समस्या आने से पहले ऑनलाइन खतरों पर बात करें, छोटी-छोटी बातचीत में, बिना उपदेश दिए। जिस बच्चे से यह बात कभी हुई ही नहीं, वह संकट में भी नहीं बताएगा ।

एक ऐसा वादा करें जो कभी न टूटे

“ऑनलाइन कुछ भी तुम्हें डराए या उलझाए, तो मुझे बता सकते हो - मैं न तुम्हारा फोन लूँगा, न गुस्सा करूँगा।” और जिस दिन इसकी परीक्षा हो, उस दिन यह वादा निभाइए।

डिवाइस साझा जगहों पर रहें

रात में चार्जिंग बेडरूम के बाहर, स्क्रीन साझा कमरों में दिखती हुई। यह सज़ा नहीं - घर का नियम है, जो बड़ों पर भी लागू होता है।

अकाउंट साथ मिलकर बनाएँ

प्रोफाइल प्राइवेट, DM सीमित, कमेंट पर नियंत्रण, लोकेशन बंद, टू-स्टेप वेरिफिकेशन। यह बच्चे के साथ करें ताकि वह सीखे, उस पर थोपें नहीं।

ऑनलाइन दायरे को जानें

पूछिए कि वे किसके साथ खेलते और बात करते हैं, वैसे ही जैसे स्कूल के दोस्तों के बारे में पूछते हैं। जिस दोस्त का नाम बताने से वे इनकार करें, उसे ऐसे लें जैसे कोई बड़ा चुपके से घर आ रहा हो।

तस्वीरों की सार्वजनिक उपलब्धता घटाएँ

बच्चे की तस्वीरें, स्कूल का नाम और यूनिफॉर्म सार्वजनिक रूप से डालने से पहले सोचें। मॉर्फिंग और AI शोषण इसी सामग्री पर टिका है।

विद्यार्थियों के लिए: वे नियम जो नियंत्रण आपके हाथ में रखते हैं

इनमें से कोई भी आपको बदतमीज़, नीरस या बुरा दोस्त नहीं बनाता। ये आपको आसानी से शिकार बनने से बचाते हैं।

प्रोफाइल पूरी तरह सुरक्षित करें

अकाउंट प्राइवेट रखें। सिर्फ वे लोग जिन्हें आप असल ज़िंदगी में जानते हैं। DM और कमेंट सीमित करें। लोकेशन और सटीक लोकेशन हर जगह बंद रखें।

अंतरंग तस्वीर कभी न भेजें। किसी को भी नहीं।

न किसी साथी को, न उसे जिसने पहले भेजी हो, न मज़ाक में। एक बार फोन से निकल जाने पर वह आपकी नहीं रहती।

किसी भी चैट को कभी भी छोड़ सकते हैं

जो व्यक्ति आपको असहज करे, उसे न जवाब देना ज़रूरी है, न सफाई, न शिष्टाचार। ब्लॉक करें और रिपोर्ट करें - ये बटन इसीलिए हैं।

माता-पिता से छिपाव ही खतरे की घंटी है

जो व्यक्ति चाहता है कि आपकी दोस्ती परिवार से छिपी रहे, वह आपकी रक्षा नहीं कर रहा। यह एक नियम ही ज़्यादातर ग्रूमर पकड़ लेता है।

भरोसा करने से पहले जाँचें

प्रोफाइल फोटो को रिवर्स सर्च करें। अकाउंट कितना पुराना है और साझा दोस्त कौन हैं, देखें। जो ऑफर बहुत अच्छा, बहुत जल्दबाज़ी वाला और गुप्त हो, वह ठगी है।

कुछ गलत हो जाए तो उसी दिन किसी को बताएँ

आप मुसीबत में नहीं पड़ेंगे। स्क्रीनशॉट लें, जवाब देना बंद करें, और माता-पिता, शिक्षक या 1098 को बताएँ। जैसे ही किसी बड़े को पता चलता है, समस्या हल होने लगती है।

स्कूलों, कॉलेजों और समुदाय के लिए

संस्थाओं पर कर्तव्य भी बड़ा है - और चूक पर दंड भी बड़ा।

लिखित बाल संरक्षण नीति

स्टाफ, कोच और स्वयंसेवकों के लिए आचार संहिता। स्टाफ और विद्यार्थियों के बीच निजी अकाउंट पर आमने-सामने की मैसेजिंग नहीं।

नामित और सबको दिखने वाला संरक्षण अधिकारी

हर विद्यार्थी को पता हो कि किसके पास और कैसे जाना है। नाम, कमरा और हेल्पलाइन नंबर वहाँ लगाएँ जहाँ बच्चे देख सकें।

रिपोर्टिंग की तय प्रक्रिया, न कि अपने विवेक का फैसला

POCSO के तहत संस्था पुलिस को सूचित करती है। वह न आंतरिक जाँच करती है, न प्रतिष्ठा के नुकसान को तौलती है।

पाठ्यक्रम में डिजिटल सुरक्षा

हर साल विद्यार्थियों के लिए उम्र के अनुरूप सत्र, और माता-पिता के लिए अलग सत्र। उच्चतम न्यायालय ने विशेष रूप से इसका आग्रह किया है।

समुदाय की सजगता

रेजिडेंट एसोसिएशन, पंचायतें, युवा क्लब और धार्मिक स्थल हेल्पलाइन नंबर फैला सकते हैं और शिकायत करने को सामान्य बना सकते हैं।

सहारा, न कि उजागर करना

बच्चे की पहचान पूरी तरह गोपनीय रखें। काउंसलिंग दिलाएँ। ध्यान रखें कि बच्चे को अपनी बात बड़ों की कतार के सामने बार-बार न दोहरानी पड़े।

आज रात की चेकलिस्ट - इस स्लाइड की फोटो ले लीजिए

एक बार, पंद्रह मिनट की सेटिंग - हर उस डिवाइस पर जो बच्चा इस्तेमाल करता है।

अकाउंट

- हर प्रोफाइल प्राइवेट करें
- डायरेक्ट मैसेज कौन भेज सकता है, यह सीमित करें
- लोकेशन और सटीक लोकेशन बंद करें
- टू-स्टेप वेरिफिकेशन चालू करें
- ऐसे फॉलोअर हटाएँ जिन्हें बच्चा नाम से न जानता हो

डिवाइस

- स्क्रीन लॉक और ऐप-स्टोर पासवर्ड माता-पिता को पता हो
- बिना अनुमति ऐप इंस्टॉल और खरीद बंद करें
- ऐप की अनुमतियाँ जाँचें - कैमरा, माइक, लोकेशन, कॉन्टैक्ट
- प्लेटफॉर्म का टीन या सुपरवाइज़्ड अकाउंट मोड चालू करें
- रात में डिवाइस बेडरूम के बाहर चार्ज करें

आदतें

- घर के हर फोन में 1098, 1930 और 112 सेव करें
- स्क्रीन-टाइम और रात के नियम मिलकर, लिखित रूप में तय करें
- महीने में एक बार फ्रेंड और फॉलोअर सूची साथ मिलकर देखें
- हर ऐप पर ब्लॉक करना, रिपोर्ट करना और स्क्रीनशॉट लेना आना चाहिए
- वादा दोहराएँ: मुझे बताने की कीमत तुम्हारा फोन कभी नहीं होगी

अगर शक हो: बातचीत कैसे शुरू करें

यह सही किया तो बच्चा बता देगा। गलत किया तो वह सालों के लिए दरवाज़ा बंद कर लेगा।

1

सही मौका चुनें

आमने-सामने नहीं, साथ-साथ चलते हुए - गाड़ी में, टहलते हुए, खाना बनाते हुए। न कोई सुनने वाला, न हाथ में फोन, न समय का दबाव।

2

बताएँ, आरोप न लगाएँ

“मैंने देखा है कि फोन इस्तेमाल करने के बाद तुम उदास लगते हो।” न कि “तुम किससे बात कर रहे थे?”

3

खुले सवाल पूछें, फिर चुप रहें

“क्या चल रहा है?” फिर इंतज़ार करें। चुप्पी आपको असहज करती है, पर उनके लिए उपयोगी होती है। उसे भरने की कोशिश न करें।

4

पहले भरोसा करें, प्रतिक्रिया बाद में

“मुझे बताने के लिए शुक्रिया। इसमें तुम्हारी गलती नहीं है। तुम मुसीबत में नहीं हो।” अपना सदमा उनके कमरे से जाने के बाद के लिए रखें।

5

जिरह की तरह पूरा ब्यौरा न पूछें

आपको कार्रवाई के लिए पर्याप्त जानकारी चाहिए, पूरा विवरण नहीं। बार-बार पूछताछ बच्चे को नुकसान पहुँचाती है और मामले को कमज़ोर कर सकती है।

6

बताएँ कि आगे क्या होगा

समझाएँ कि आप मदद लेंगे, किससे संपर्क करेंगे, और आप उनके साथ रहेंगे। फिर उसी दिन उस पर अमल करें।

इस कमरे से ले जाने लायक दस बातें

अगर और कुछ याद न रहे, तो ये याद रखें।

1. भारत में 18 वर्ष से कम आयु का हर व्यक्ति बच्चा है - POCSO, JJ एक्ट, आईटी एक्ट और DPDP एक्ट, सभी में।
2. 18 से कम आयु में कोई मान्य सहमति नहीं होती। “वे राज़ी थे” कानून में बचाव नहीं है।
3. POCSO लिंग-निरपेक्ष है। लड़के भी पीड़ित होते हैं, और उनके मामले कहीं कम दर्ज होते हैं।
4. ग्रूमिंग छह पहचाने जा सकने वाले चरणों की धीमी प्रक्रिया है। आप इसे किसी भी चरण पर तोड़ सकते हैं।
5. वयस्क और बच्चे के बीच जानबूझकर बनाया गया छिपाव सबसे साफ चेतावनी संकेत है।
6. सेक्सटॉर्शन में: पैसे कभी न दें, और तस्वीरें न भेजें, सबूत सहेजें, और आज ही किसी को बताएँ।
7. बाल शोषण सामग्री देखना, डाउनलोड करना या आगे भेजना अपराध है - निजी मामला नहीं।
8. POCSO की धारा 19 के तहत रिपोर्ट करना कानूनी कर्तव्य है; चुप्पी धारा 21 के तहत दंडनीय है।
9. सद्भावना से की गई शिकायत कानूनन सुरक्षित है। आपका निश्चित होना या जाँच करना ज़रूरी नहीं।
10. 1098, 1930, 112, cybercrime.gov.in - अभी सेव करें, और इस हफ्ते तीन लोगों को बताएँ।

साइबर सुरक्षा के सुझाव :

क्या करें

खुद उदाहरण बनें:
मज़बूत और अलग-अलग पासवर्ड इस्तेमाल करें, और विद्यार्थियों को अपने अकाउंट पर मल्टी-फैक्टर ऑथेंटिकेशन (MFA) चालू करना सिखाएँ।

“रुको और सोचो” का नियम:
विद्यार्थियों को सिखाएँ कि संदिग्ध लिंक पर कभी क्लिक न करें और अनजान स्रोत से फाइल डाउनलोड न करें - खासकर गेमिंग प्लेटफॉर्म पर।

सॉफ्टवेयर अपडेट रखें:
समझाएँ कि सॉफ्टवेयर अपडेट “डिजिटल कवच” की तरह हैं, जो ऐप और डिवाइस की सुरक्षा खामियाँ ठीक करते हैं।

पहले निजता:
क्लासरूम ऐप की प्राइवेसी सेटिंग नियमित रूप से जाँचें और विद्यार्थियों को भी अपने सोशल मीडिया व गेमिंग प्रोफाइल पर ऐसा करने के लिए कहें।

खुली बातचीत:
ऐसा “बिना फैसले वाला माहौल” बनाएँ जिसमें विद्यार्थी कुछ अजीब देखने या ऑनलाइन गलती कर बैठने पर बेझिझक बता सकें।

क्या न करें

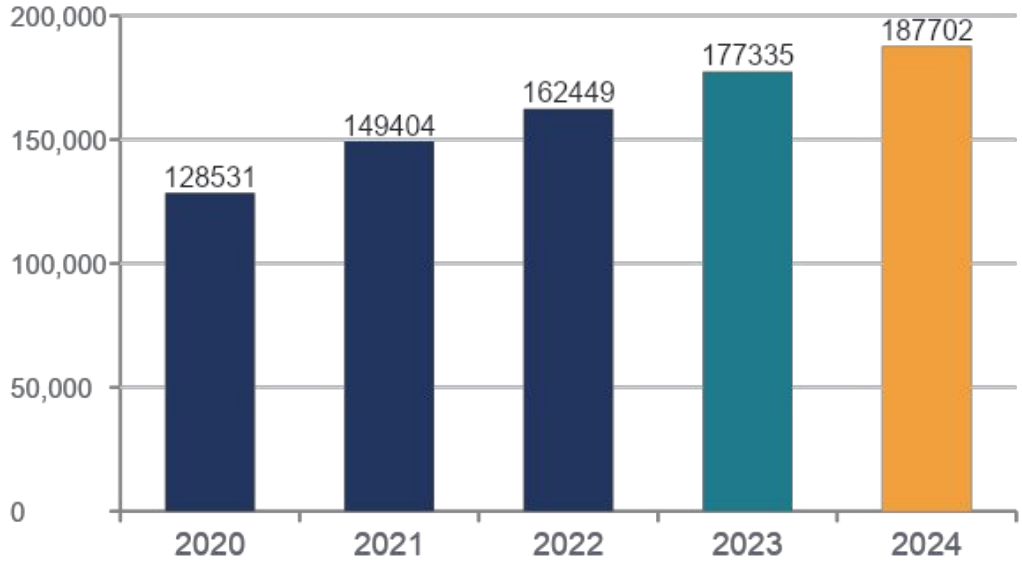
Roblox या Discord जैसे गेमिंग प्लेटफॉर्म पर अपना पूरा नाम, घर का पता या स्कूल का नाम जैसी निजी जानकारी साझा न करें।

अनजान भेजने वालों के लिंक पर क्लिक या फाइल डाउनलोड न करें, भले ही वे दोस्त लगें (उनका अकाउंट हैक हो सकता है!)।

स्कूल के काम के लिए वही पासवर्ड इस्तेमाल न करें जो सोशल मीडिया या गेम में लगाते हैं।

बच्चों के विरुद्ध अपराध, 2020 से 2024

पूरे भारत में दर्ज कुल मामले। स्रोत: राष्ट्रीय अपराध रिकॉर्ड ब्यूरो, क्राइम इन इंडिया 2024।



2024 में 1,87,702 मामले

2023 से 5.8% अधिक, और 2020 से 46% से भी अधिक।

जबकि देश में अपराध घट रहे हैं

इन्हीं चार वर्षों में भारत में कुल अपराध लगभग 10.8% घटे, 66.01 लाख से 58.86 लाख मामलों पर।

69,191 POCSO मामले

प्रति लाख बच्चों पर अपराध दर 15.6। धारा 4 और 6 के 44,567 पीड़ितों में 43,675 लड़कियाँ थीं।

भारत में बाल साइबर अपराध पर CSEAM हावी है

2024 में बच्चों के विरुद्ध दर्ज हर दस साइबर अपराध मामलों में से लगभग नौ यौन सामग्री से जुड़े थे।

1,238

2024 में आईटी एक्ट के तहत बच्चों के विरुद्ध दर्ज साइबर अपराध के मामले

1,099

इनमें से इतने मामले बच्चों की यौन सामग्री प्रकाशित या प्रसारित करने के थे

139

बाल साइबर अपराध की बाकी सभी श्रेणियाँ मिलाकर इतने मामले

बाल साइबर अपराध मामलों में हिस्सेदारी , 2024

कोई आधिकारिक 'CSEAM अपराध दर' नहीं है

NCRB केवल व्यापक श्रेणियों के लिए प्रति लाख जनसंख्या दर प्रकाशित करता है - 15.6 का आँकड़ा POCSO की दर है। CSEAM को मामलों की संख्या के रूप में बताएँ, दर के रूप में नहीं।

इन्हें वर्ष-दर-वर्ष श्रृंखला की तरह न पढ़ें

NCRB के अलग-अलग संस्करणों में बाल साइबर अपराध की गणना का आधार बदला है, इसलिए 2022 और 2024 के आँकड़ों की सीधी तुलना नहीं की जा सकती।

1,099

2024 में पूरे भारत में पुलिस द्वारा दर्ज CSEAM मामले

प्रति लाख बच्चों पर लगभग 0.02 मामले

69,00,000+

मार्च 2025 तक भारतीय राज्यों और केंद्र शासित प्रदेशों से साझा की गई NCMEC साइबरटिपलाइन रिपोर्ट

रिपोर्ट का मतलब अपराधी नहीं - पर बात पैमाने की है

और सामग्री खुद भी बदल रही है - NCMEC, 2025

7,000+

2025 में AI से बनी CSEAM बनाने या रखने वाले उपयोगकर्ताओं की रिपोर्ट

30,000+

अपलोड की गई तस्वीरों और प्रॉम्प्ट से ऐसी सामग्री बनाने की कोशिश करने वाले उपयोगकर्ताओं की रिपोर्ट

145,000+

AI टूल से मौजूदा CSEAM फाइलों को बदलने वाले उपयोगकर्ताओं की रिपोर्ट

संसाधन पृष्ठ

साइबर दोस्त को यहाँ फॉलो करें:

X (Twitter)

@Cyberdost

Facebook

CyberDostI4C

Instagram

@cyberdosti4c

YouTube

CyberDosti4c

व्हाट्सएप चैनल

CyberDost I4C

वेबसाइट

https://i4c.mha.gov.in/

https://i4c.mha.gov.in/awareness.aspx

VIEW MORE →

CYBER AWARENESS PRINTABLE MATERIAL

Comic Story (English)

Comic Story (Hindi)

DOs & Don'ts (English)

DOs & Don'ts (Hindi)

Dos & Don'ts 2 (English)

Cyber Dhamaka (English)

Cyber Dhamaka (Hindi)

The Cyber Safety Club (English)

The Cyber Safety Club (Hindi)

Spot the Scam Brochure (English)

Spot the Scam Brochure (Hindi)

Book on Cybercrime against Women (English)

गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS

Indian
Cyber
Crime
Coordination
Centre

CYBER SURAKSHINI

Your Guide to Staying Safe Online Available in English, Hindi & Regional Languages

STOP **THINK** **TAKE ACTION**

INDEX

Contextualising Online Crimes Against Women 03

Online Crimes Against Women & Children 04

Fake Social Media Profiles 05

Cyber Stalking 06

Online Trolling 07

Sexting 08

Online Sextortion 09

Doxxing 10

Cyber Flashing 11

Non-Consensual Intimate Media 12

Online Hate Crimes 13

Morphing 14

Romance Scam 15

Voice Cloning 16

गृह मंत्रालय
MINISTRY OF
HOME AFFAIRS

Indian
Cyber
Crime
Coordination
Centre

Mantra for
Digital Safety

STOP. THINK. THEN TAKE ACTION.

Report any Cybercrime at
www.cybercrime.gov.in

or Call Helpline Number **1930**

Follow @CyberDost
for daily cyber safety tips and
easy reporting options.

प्रश्न?

ऑनलाइन सुरक्षित बच्चा किसी एक चतुर सेटिंग या एक सख्त नियम का नतीजा नहीं होता।
यह उन बड़ों का नतीजा होता है जो ध्यान देते हैं, जो नज़र नहीं फेरते, और जिन्हें ठीक-ठीक पता होता है कि आगे क्या करना है।

1098
चाइल्डलाइन - 24x7

1930
साइबर अपराध हेल्पलाइन

112
आपातकालीन सेवा

ऑनलाइन शिकायत: cybercrime.gov.in | POCSO ई-बॉक्स: ncpcr.gov.in | निकटतम पुलिस स्टेशन या विशेष किशोर पुलिस इकाई

> बच्चों के लिए सुरक्षित इंटरनेट अकेले कानून प्रवर्तन से नहीं बन सकता। इसके लिए चाहिए ऐसे शिक्षक जो चेतावनी के संकेत पहचानें, ऐसे माता-पिता जो बिना फैसला सुनाए सुनें, ऐसे स्कूल जिनके पास प्रभावी सुरक्षा तंत्र हो, ऐसे प्लेटफॉर्म जो ज़िम्मेदारी से जवाब दें, और ऐसी कानून प्रवर्तन एजेंसियाँ जो तेज़ी और संवेदनशीलता से कार्रवाई करें।”

धन्यवाद !