INDIA CHILD PROTECTION FUND

ETT™

यॉर्क टेक प्राइवेट लिमिटेड
के सहयोग से

साइबर संरक्षक: ऑनलाइन सुरक्षा के लिए बच्चों की मार्गदर्शिका

"साइबर अपराधच्च को समझना और डिजिटल दुनिया में सुरक्षित रहना"

इंडिया चाइल्ड प्रोटेक्शन फण्ड
एल-6, कालकाजी, नई दिल्ली- 110019

01. साइबर अपराध:

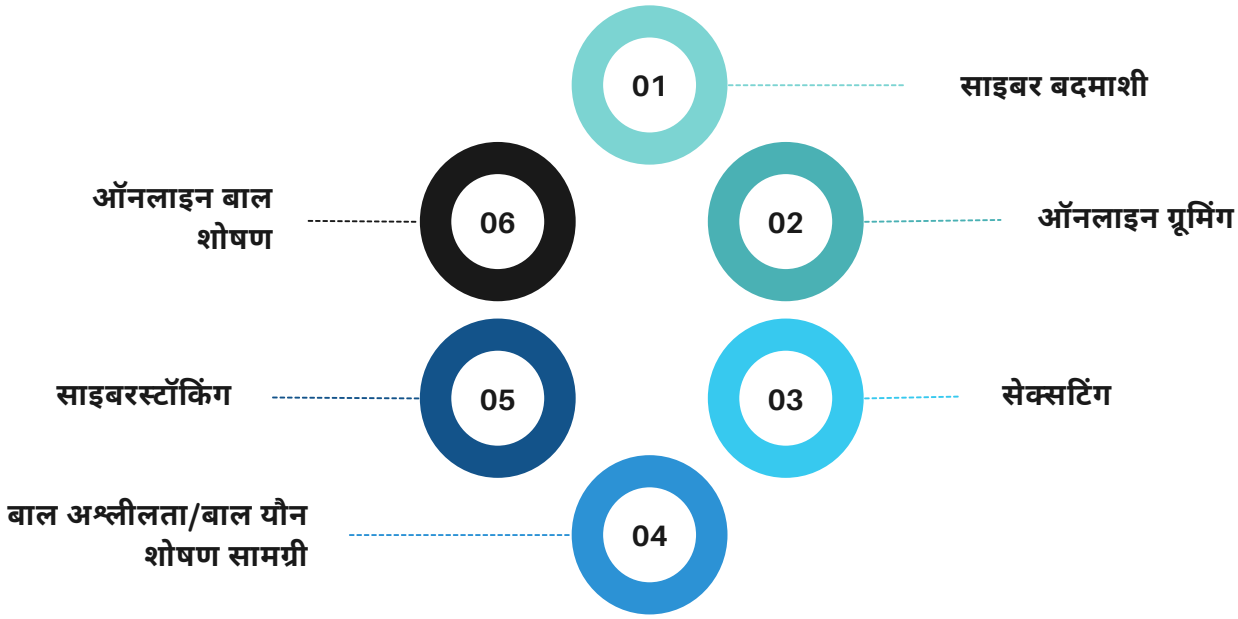
साइबर अपराध से तात्पर्य उन आपराधिक गतिविधियों से है जो कंप्यूटर, नेटवर्क या डिजिटल तकनीक का उपयोग करके की जाती हैं। ये अपराध विभिन्न रूप ले सकते हैं और इनमें अक्सर इंटरनेट या अन्य इलेक्ट्रॉनिक संचार प्रणालियों का उपयोग शामिल होता है।

सरल शब्दों में कहें तो साइबर क्राइम तब होता है जब लोग कंप्यूटर या इंटरनेट पर बुरे काम करते हैं।
कल्पना कीजिए कि अगर कोई कंप्यूटर का उपयोग उन चीज़ों को लेने के लिए करता है जो उसकी नहीं हैं या दूसरों को पैसे या रहस्य बताने के लिए बरगलाता है। वह साइबर क्राइम है। यह वैसा ही है जैसे हम स्कूल में सीखते हैं कि जो चीज़ आपकी नहीं है उसे लेना या झूठ बोलना गलत है।
साइबर अपराधी कुछ हद तक ऑनलाइन बदमाशों की तरह हो सकते हैं, लेकिन वे और भी बदतर हैं क्योंकि वे दूसरों को चोट पहुंचाने के लिए कंप्यूटर का उपयोग करते हैं। इसलिए, ऑनलाइन सुरक्षित रहना वास्तव में महत्वपूर्ण है और अगर कुछ सही नहीं लगता है तो वयस्कों या अपने माता-पिता को बताएं। ठीक वैसे ही जैसे आप एक शिक्षक को बताएंगे कि क्या स्कूल में कोई आपके साथ बुरा व्यवहार कर रहा है। इस तरह, साइबर अपराध को रोकने और इंटरनेट को एक सुरक्षित स्थान बनाने के लिए हर कोई मिलकर काम कर सकता है।

02. बच्चों के विरुद्ध साइबर अपराध:

आज की डिजिटल दुनिया में बच्चों के खिलाफ साइबर अपराध एक गंभीर चिंता का विषय है। इन अपराधों में डिजिटल तकनीक और इंटरनेट के उपयोग के माध्यम से बच्चों का शोषण, नुकसान या खतरे में डालने वाली गतिविधियाँ शामिल हैं। यहां बच्चों के विरुद्ध कुछ सामान्य प्रकार के साइबर अपराध हैं:

- साइबर बदमाशी
- ऑनलाइन ग्रूमिंग
- सेक्सटिंग
- बाल अश्लीलता/बाल यौन शोषण सामग्री
- साइबरस्टॉकिंग
- ऑनलाइन बाल शोषण
- चोरी की पहचान
- ऑनलाइन घोटाले आदि,



2.1: साइबरबुलिंग - जब लोग ऑनलाइन मतलबी होते हैं:

कभी-कभी, जब हम कंप्यूटर या अपने फोन का उपयोग करते हैं, तो कुछ बच्चे या यहां तक कि वयस्क भी हमारे लिए निर्दयी या चोट पहुंचाने वाली बातें कह सकते हैं, जैसे हमें अजीब नाम से बुलाना या हमारा मजाक उड़ाना। इसे साइबरबुलिंग कहा जाता है। यह वैसा ही है जैसे स्कूल में कोई आपके प्रति बुरा व्यवहार करता है, लेकिन ऐसा कंप्यूटर या फोन पर होता है। यह ठीक नहीं है, और यह हमें वास्तव में दुखी या डरा हुआ महसूस करा सकता है। यदि आपके या किसी दोस्त के साथ ऐसा होता है, तो किसी ऐसे वयस्क व्यक्ति को बताना याद रखें जिस पर आप भरोसा करते हैं, जैसे कि आपकी माँ, पिताजी या शिक्षक। वे इसे रोकने में मदद कर सकते हैं।

2.2: ऑनलाइन ग्रूमिंग - ट्रिकी फ्रेंड्स ऑनलाइन:

इंटरनेट पर हम उन लोगों से बात कर सकते हैं जिन्हें हम ठीक से नहीं जानते। लेकिन, वास्तविक जीवन की तरह, कुछ लोग हमारे मित्र होने का दिखावा कर सकते हैं जबकि वे नहीं हैं। वे शायद हमसे मिलना चाहते हैं या हमसे वो काम करवाना चाहते हैं जो हमें नहीं करना चाहिए। इसे ऑनलाइन ग्रूमिंग कहते हैं। यह याद रखना महत्वपूर्ण है कि अजनबियों से ऑनलाइन बात न करें और जिन लोगों से आप ऑनलाइन बात करते हैं उनके बारे में अपने परिवार से रहस्य न रखें।

यदि कोई ऑनलाइन आपको असहज महसूस कराता है या आपसे रहस्य छुपाने के लिए कहता है, तो हमेशा किसी ऐसे वयस्क को बताएं जिस पर आप भरोसा करते हैं।

2.3: साइबरस्टॉकिंग:

कल्पना कीजिए कि कोई हर समय आपका पीछा कर रहा हो, तब भी जब आप उसे नहीं चाहते हों। खैर, साइबरस्टॉकिंग कुछ-कुछ ऐसी ही है, लेकिन यह कंप्यूटर या इंटरनेट पर होती है। ऐसा तब होता है जब कोई व्यक्ति जिसे आप जानते हों या कोई ऐसा व्यक्ति जिसे आप नहीं जानते हों, वह आपको ऑनलाइन परेशान करता रहता है। वे आपको बहुत सारे संदेश या ईमेल भेज सकते हैं, आपके सोशल मीडिया पेजों पर बहुत बार जा सकते हैं, या इंटरनेट पर आपके बारे में घटिया बातें कह सकते हैं।
साइबर स्टॉकर आपको असहज या डरा हुआ महसूस कराते हैं क्योंकि जब आप चाहते हैं तो वे आपको अकेला नहीं छोड़ते हैं। यह ठीक नहीं है, और यदि आपके साथ कभी ऐसा होता है तो किसी ऐसे वयस्क व्यक्ति को बताना ज़रूरी है जिस पर आप भरोसा करते हैं। वे इसे रोकने और आपको सुरक्षित रखने में मदद करेंगे।

2.3: ऑनलाइन बाल शोषण क्या है?

ऑनलाइन बाल शोषण तब होता है जब कुछ बुरे लोग बच्चों को इंटरनेट पर गलत और हानिकारक तरीके से इस्तेमाल करने की कोशिश करते हैं। यह वैसा ही है जब कोई बच्चों से वो काम करवाना चाहता है जो उन्हें नहीं करना चाहिए या उनकी तस्वीरें या वीडियो लेना चाहता है जो ठीक नहीं हैं।
ये बुरे लोग बच्चों को ऑनलाइन उनसे बात करने या वे काम करने के लिए बरगलाने की कोशिश कर सकते हैं जो वे नहीं करना चाहते। यह सचमुच बहुत ग़लत है और इसकी अनुमति नहीं है।

2.4: पहचान की चोरी:

पहचान की चोरी तब होती है जब कोई आपके जैसा होने का दिखावा करता है। यह ऐसा है जैसे उन्होंने आपके चेहरे पर एक मुखौटा पहन रखा है। वे आपके नाम, आपकी तस्वीरों या आपकी अन्य चीज़ों का उपयोग उन चीज़ों को करने के लिए कर सकते हैं जिनके लिए आपने 'हाँ' नहीं कहा है। उदाहरण के लिए, वे आपकी जानकारी के बिना चीज़ें खरीदने या आपके बैंक से पैसे लेने के लिए आपके नाम का उपयोग कर सकते हैं।
पहचान की चोरी बिल्कुल भी अच्छी नहीं है, और यह नियमों के विरुद्ध है। यदि आपको कभी लगे कि कोई आपके जैसा होने का दिखावा कर रहा है या आपके नाम के साथ ऐसे काम कर रहा है जो आपने नहीं किया, तो तुरंत किसी ऐसे वयस्क को बताएं जिस पर आप भरोसा करते हैं। आप ऐसे अपराधों की रिपोर्ट 'नेशनल साइबर क्राइम रिपोर्टिंग पोर्टल' पर भी कर सकते हैं।

03. ऑनलाइन सुरक्षा के लिए युक्तियाँ:

1. **मजबूत पासवर्ड का प्रयोग करें**
   - ऑनलाइन खातों के लिए मजबूत, अद्वितीय पासवर्ड बनाएं।
   - अक्षरों, संख्याओं और प्रतीकों के मिश्रण का उपयोग करें।
2. **व्यक्तिगत जानकारी साझा न करें**
   - अपना पूरा नाम, पता, फ़ोन नंबर या स्कूल कभी भी ऑनलाइन साझा न करें।
3. **चित्रों से सावधान रहें**
   - तस्वीरें या वीडियो ऑनलाइन पोस्ट करने से पहले सोचें।
   - ऐसी तस्वीरें साझा करने से बचें जो आपके बारे में बहुत कुछ बताती हों।
4. **सोशल मीडिया को निजी रखें**
   - सोशल मीडिया प्रोफ़ाइल को निजी पर सेट करें ताकि केवल मित्र ही आपकी पोस्ट देख सकें।
5. **क्लिक करने से पूर्व सोचें**
   - अजनबियों के लिंक पर क्लिक न करें या अटैचमेंट न खोलें।
6. **चैटरूम में सावधान रहें**
   - केवल उन लोगों से चैट करें जिन्हें आप वास्तविक जीवन में जानते हैं।
   - चैटरूम में व्यक्तिगत जानकारी साझा करने से बचें।
7. **ऑनलाइन दयालु बनें**
   - दूसरों के साथ ऑनलाइन वैसा ही व्यवहार करें जैसा आप व्यक्तिगत रूप से करते हैं।
   - साइबरबुलिंग या हानिकारक व्यवहार में शामिल न हों।
8. **अजनबियों से बात न करें**
   - उन लोगों से चैट या जानकारी साझा न करें जिनसे आप ऑफ़लाइन नहीं मिले हैं।
9. **चिंताएँ रिपोर्ट करें**
   - यदि आपको ऑनलाइन कुछ ऐसा मिलता है जिससे आप असहज या भयभीत हो जाते हैं तो किसी विश्वसनीय वयस्क को बताएं।
10. **माता-पिता के नियंत्रण का उपयोग करें**
    - अपने माता-पिता या अभिभावकों से अपने उपकरणों पर अभिभावकीय नियंत्रण स्थापित करने के लिए कहें।
11. **अज्ञात स्रोतों से डाउनलोड करने से बचें**
    - ऐप्स, गेम या फ़ाइलें केवल ऐप स्टोर जैसे विश्वसनीय स्रोतों से ही डाउनलोड करें।
12. **प्रस्तावों पर संदेह करें**
    - उन प्रस्तावों से सावधान रहें जो सुनने में बहुत अच्छे लगते हैं। वे घोटाले हो सकते हैं.
13. **डिवाइस सुरक्षित रखें**
    - अपने डिवाइस को पिन या पासवर्ड से लॉक करें। - अपने उपकरणों को सार्वजनिक स्थानों पर लावारिस न छोड़ें।
14. **पासवर्ड साझा न करें**
    - कभी भी अपने पासवर्ड दोस्तों या किसी अन्य के साथ साझा न करें।
15. **गोपनीयता सेटिंग्स जांचें**
    - अपने सोशल मीडिया खातों पर गोपनीयता सेटिंग्स की नियमित रूप से समीक्षा करें और उन्हें समायोजित करें।
16. **ऑनलाइन मित्रों को सत्यापित करें**
    - मित्र अनुरोध स्वीकार करने से पहले, सुनिश्चित करें कि आप उस व्यक्ति को वास्तविक जीवन में जानते हैं।

17. **स्थान साझाकरण से सावधान रहें**
    - सोशल मीडिया ऐप्स पर अजनबियों के साथ अपना सटीक स्थान साझा करने से बचें।
18. **सुरक्षित वेबसाइटों का उपयोग करें**
    - उन वेबसाइटों और ऐप्स पर टिके रहें जो बच्चों के लिए हैं और जिनमें सुरक्षा सुविधाएँ हैं।
19. **ऑनलाइन दोस्तों से अकेले न मिलें**
    - यदि आप किसी ऑनलाइन मित्र से मिलना चाहते हैं, तो हमेशा अपने साथ एक विश्वसनीय वयस्क लाएँ।
20. **अपने माता-पिता या अभिभावकों से बात करें**

- अपने ऑनलाइन अनुभवों के बारे में अपने माता-पिता या अभिभावकों के साथ संचार का खुला सिलसिला रखें। वे आपको सुरक्षित रहने में मदद कर सकते हैं।

21. **प्रमाणीकरण का उपयोग करें**
    - टू-फैक्टर ऑथेंटिकेशन का उपयोग करें
    - मल्टी-फैक्टर ऑथेंटिकेशन ण का प्रयोग करें
    - टू-स्टेप वेरिफिकेशन का उपयोग करें

04. शिकायत/रिपोर्टिंग पोर्टल:

112
आपातकालीन प्रतिक्रिया

1930
ऑनलाइन वित्तीय धोखाधड़ी

बाल दुर्व्यवहार के किसी भी मुद्दे की रिपोर्ट करने के लिए कृपया कॉल करें (शिकायत कक्ष - बचपन बचाओ आंदोलन)

1800-102-7222

https://cybercrime.gov.in/