



CyberPeace



एन सी ई आर टी
NCERT

विद्यया ऽ मृतमश्नुते

सोशल मीडिया पर अधिक साझा करने के जोखिम और साइबर फर्स्ट रिस्पॉन्डर की भूमिका

कार्यशाला – छात्रों एवं शिक्षकों के लिए

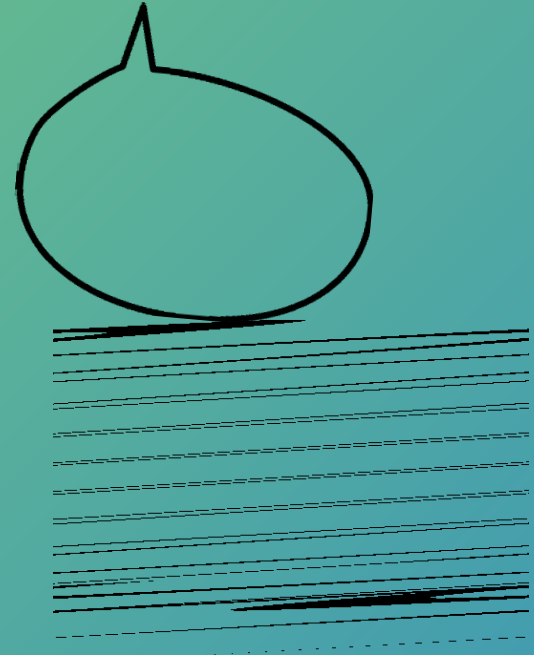
उद्देश्य

- सोशल मीडिया पर "ओवर-शेयरिंग" की पहचान
- इससे जुड़े साइबर जोखिम समझना
- साइबर फर्स्ट रिस्पॉन्डर की भूमिका जानना
- सुरक्षित और जिम्मेदार ऑनलाइन व्यवहार विकसित करना



सोशल मीडिया और हमारा जीवन

- संवाद, अभिव्यक्ति और पहचान का माध्यम
- शिक्षा और नेटवर्किंग का साधन
- छात्र, शिक्षक, अभिभावक – सभी सक्रिय
- पहचान और प्रतिष्ठा से जुड़ा
- हर आयु वर्ग की भागीदारी
- पर हर साझा की गई जानकारी सुरक्षित नहीं होती
- हर क्लिक, पोस्ट और सर्च का रिकॉर्ड बनता है

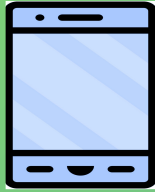


“अधिक साझा करना” क्या है?

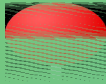
- हर पल की जानकारी ऑनलाइन डालना
- आवश्यकता से अधिक निजी जानकारी साझा करना
- बिना सोचे-समझे पोस्ट करना
- निजी जानकारी शेयर करना
- हर गतिविधि को सार्वजनिक करना
- सुरक्षा जोखिमों को नजरअंदाज करना



हम क्या-क्या अधिक साझा कर देते हैं?



- मोबाइल नंबर, ईमेल
- स्कूल का नाम, स्थान



- लाइव लोकेशन



- घर या यात्रा की जानकारी
- निजी फोटो और वीडियो



CyberPeace

विद्यया ऽ मृतमश्नुते



एन सी ई आर टी
NCERT

अधिक साझा करने के कारण

- लाइक और फॉलोअर्स की चाह
- ट्रेंड में रहने की इच्छा
- डिजिटल जागरूकता की कमी
- सोशल मीडिया ट्रेंड का दबाव
- “सब कर रहे हैं” वाली सोच



ओवर-शेयरिंग क्यों खतरनाक है?



- निजी जानकारी का दुरुपयोग
- साइबर अपराध का जोखिम
- मानसिक और सामाजिक नुकसान
- भविष्य में कानूनी परेशानी

जोखिम 1 - पहचान चोरी (Identity Theft)

- नाम और फोटो से फर्जी प्रोफाइल
- किसी और के नाम से अपराध
- बैंक या अकाउंट से जुड़ी समस्या
- कानूनी और सामाजिक खतरा



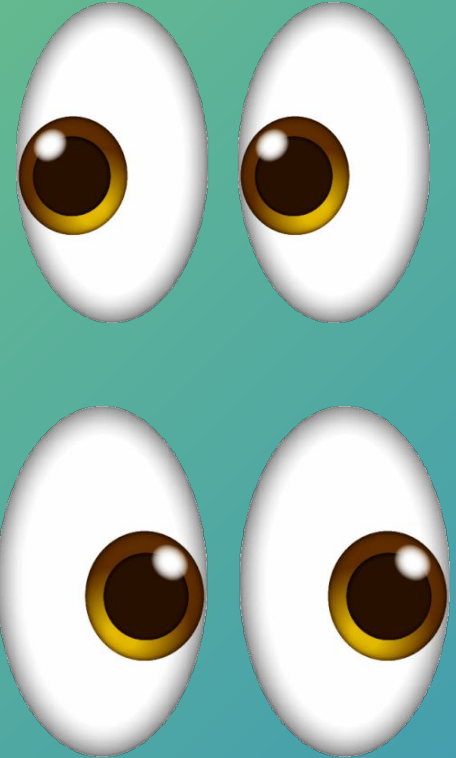
जोखिम 2 - साइबर बुलिंग (Cyber Bullying)



- अपमानजनक कमेंट और मीम
- पोस्ट को गलत तरीके से फैलाना
- मानसिक तनाव और डर
- आत्मविश्वास पर नकारात्मक असर

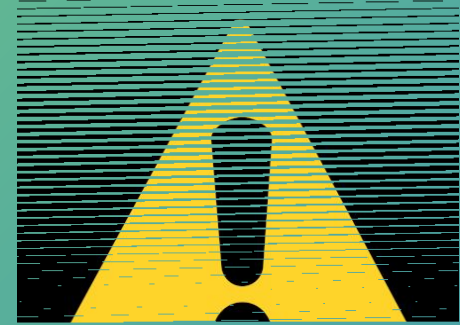
जोखिम 3 - साइबर स्टॉकिंग (Cyber Stalking)

- बार-बार मैसेज या फॉलो करना
- निजी गतिविधियों पर नजर
- डर और असुरक्षा की भावना
- मानसिक उत्पीड़न
- शारीरिक सुरक्षा को खतरा



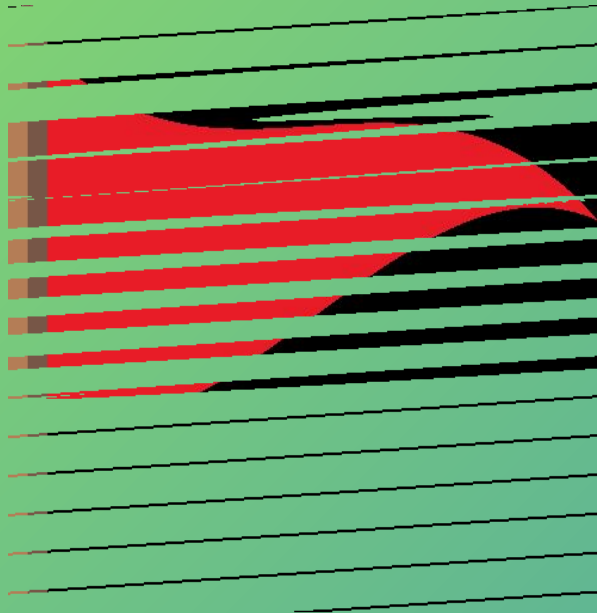
जोखिम 4 – ऑनलाइन धोखाधड़ी (Online Fraud)

- फर्जी लिंक और मैसेज (Phishing)
- नकली ऑफर और जॉब कॉल (Scams)
- OTP या डिजिटल पेमेंट फ्रॉड
- फोटो/डेटा का गलत उपयोग (deepfake)



जोखिम 5 - शारीरिक सुरक्षा

- लाइव लोकेशन शेयर करना
- घर खाली होने की जानकारी
- यात्रा की रियल-टाइम पोस्ट
- वास्तविक दुनिया में खतरा



छात्र क्यों अधिक संवेदनशील हैं?

- अनुभव की कमी
- भावनात्मक प्रतिक्रिया
- डिजिटल सीमाओं की समझ कम
- सामाजिक स्वीकृति (social approval) की चाह



शिक्षकों के लिए महत्व

- बच्चों की ऑनलाइन सुरक्षा
- अनदेखे डिजिटल खतरे
- समय पर जानकारी न मिलना
- व्यवहार में बदलाव



समाधान की दिशा

- केवल कानून पर्याप्त नहीं
- जागरूकता सबसे जरूरी
- समय पर सहायता आवश्यक
- समुदाय आधारित सहयोग
- पीड़ित को समझने की कोशिश करें



डिजिटल प्रतिष्ठा

- सकारात्मक कंटेंट = सकारात्मक छवि
- नकारात्मक पोस्ट = लंबे समय तक नुकसान
- सोच-समझकर ऑनलाइन व्यवहार करें
- साइबर बुलिंग, स्टाकिंग, एब्यूज, हरस्मेंट, खासकर लड़कियों के प्रति, न करें



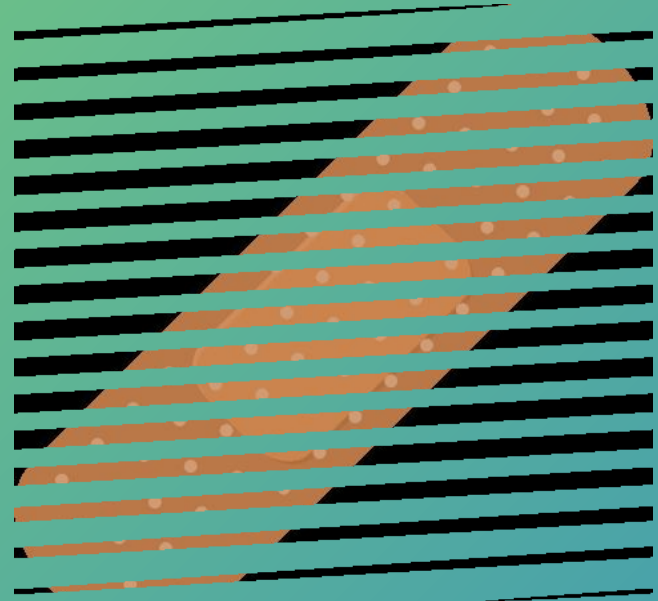
साइबर फर्स्ट रिस्पॉन्डर कौन है?



- साइबर समस्या में पहला सहायक
- पुलिस से पहले मदद करने वाला
- स्कूल/समुदाय में मौजूद व्यक्ति
- पीड़ित के लिए भरोसेमंद सहारा

साइबर फर्स्ट रिस्पॉन्डर की भूमिका

- पीड़ित को शांत करना
- सही सलाह देना
- गलत कदम से रोकना
- सही रिपोर्टिंग में मदद



स्कूल स्तर पर CFR कौन हो सकता है?

- शिक्षक
- स्कूल काउंसलर
- IT या कंप्यूटर शिक्षक
- प्रशिक्षित छात्र प्रतिनिधि

CFR क्या करता है?

- पीड़ित की बात ध्यान से सुनता है



- सबूत सुरक्षित रखने को कहता है



- अकाउंट सुरक्षा के उपाय बताता है



- सही रिपोर्टिंग प्लेटफॉर्म तक मार्गदर्श





CyberPeace

विद्यया ऽ मृतमश्नुते



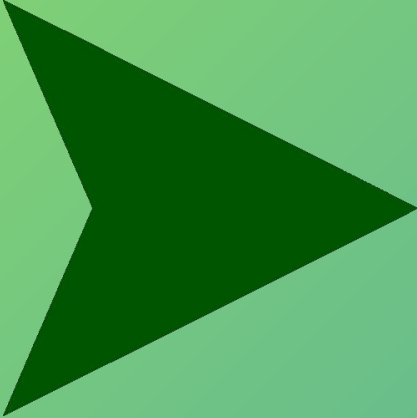
एन सी ई आर टी
NCERT

CFR क्या नहीं करता

- पीड़ित को दोष नहीं देता
- खुद जांच या सजा नहीं देता
- अफवाह नहीं फैलाता
- समस्या को हल्का नहीं समझता



रिपोर्टिंग क्यों जरूरी है?

- 
- अपराध दोहराने से रोकने के लिए
 - अपराधी की पहचान के लिए
 - पीड़ित की सुरक्षा के लिए
 - डिजिटल प्लेटफॉर्म की जिम्मेदारी तय करने के लिए

कानूनी दृष्टिकोण

- साइबर बुलिंग अपराध है
- निजी जानकारी साझा करना दंडनीय
- ऑनलाइन धोखाधड़ी कानूनन अपराध
- इंटरनेट पर किया गया कार्य भी वैध सबूत





CyberPeace

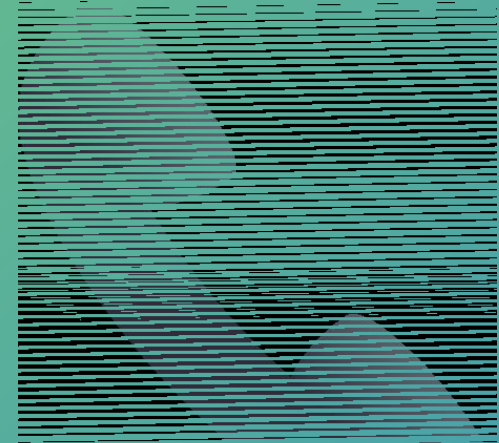
साइबर अपराध क्या-क्या हो सकते हैं



- हैकिंग/ अनधिकृत एक्सेस
- पहचान चोरी (Identity Theft)
- ऑनलाइन धोखाधड़ी और फर्जी वेबसाइट (Phishing)
- ईमेल, सोशल मीडिया या ऐप के माध्यम से ठगी (Fraud)
- मानहानि (Defamation)
- फर्जी खबरें फैलाना (Misinformation)
- बिना अनुमति फोटो साझा करना
- Ransomware, Malware, इत्यादि

भारत में रिपोर्टिंग के साधन

- सोशल मीडिया रिपोर्ट टूल
- साइबर क्राइम पोर्टल cybercrime.gov.in
- स्कूल या संस्था के माध्यम से
- हेल्पलाइन और सहायता केंद्र 1930
- साइबरपीस हेल्पलाइन +91 9570000066



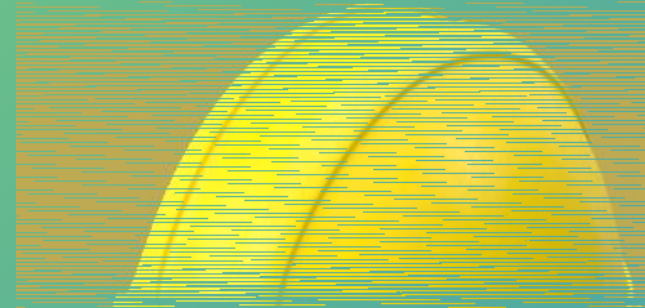
सोचें फिर साझा करें



- क्या यह जानकारी जरूरी है?
- कौन इसे देख सकता है?
- क्या इससे नुकसान हो सकता है?
- क्या मैं सहज महसूस करूँगा/ करूँगी ?

सुरक्षित सोशल मीडिया आदतें

- प्राइवेट अकाउंट रखें
- सीमित मित्र सूची
- लोकेशन शेयर बंद रखें
- अजनबी रिक्वेस्ट से सावधान



छात्रों के लिए 5 सुनहरे नियम

- सीमित और सोच-समझकर साझा करें
- सम्मानजनक भाषा का उपयोग
- समस्या छुपाएँ नहीं
- मदद माँगने से न डरें
- दूसरों को उत्पीड़ित / परेशां न करें



शिक्षकों की भूमिका

- विश्वासपूर्ण माहौल बनाना
- डिजिटल विषयों पर खुली बातचीत
- समय पर मार्गदर्शन
- साइबर फर्स्ट रिस्पॉन्डर बनना



निष्कर्ष

- ओवर-शेयरिंग से बचाव संभव है
- साइबर फर्स्ट रिस्पॉन्डर पहली सुरक्षा कड़ी
- मिलकर सुरक्षित डिजिटल समाज बनाएं
- जिम्मेदार डिजिटल नागरिक बनें



CyberPeace

विद्यया ऽ मृतमश्नुते



एन सी ई आर टी
NCERT

धन्यवाद