सत्यमेव जयते
RCSCE राजस्थान स्कूल शिक्षा परिषद्
स्कूल शिक्षा विभाग, राजस्थान सरकार
unicef for every child
CyberPeace Foundation

छात्र प्रशिक्षण सरलीकरण पुस्तिका

६-८

सत्यमेव जयते
RCSCE राजस्थान स्कूल शिक्षा परिषद्
स्कूल शिक्षा विभाग, राजस्थान सरकार
unicef for every child
CyberPeace Foundation

अधिक जानकारी के लिए कृपया संपर्क करें :

+91 957 0000 066 | helpline@cyberpeace.net

परिचय

छात्रों के लिए ऑनलाइन सुरक्षा पर सत्र संचालित करने हेतु शिक्षकों की सुविधा के लिए यह पुस्तिका तैयार की गई है। 45 मिनट लंबे सत्र के ज़रिए छात्रों को ऑनलाइन सुरक्षा के विभिन्न पहलूओं के बारे में बताया जाएगा जिससे समस्याओं से लड़ने और उबरने की क्षमता का निर्माण हो सके और साइबरस्पेस (साइबर जगत) को शांतिपूर्ण, सुरक्षित और सर्व समावेशी बनाया जा सके।

छात्रों के दो समूहो के लिए इस प्रकार सत्र संचालित किए जाएंगे:

किशोर छात्रों के लिए ऑनलाइन सुरक्षा – कक्षा 6ठी से 8वी तक

युवा वयस्कों के लिए ऑनलाइन सुरक्षा – कक्षा 9वी से 12वी तक

उद्देश्य

इंटरनेट का इस्तेमाल करते समय बच्चों द्वारा सामना किए जाने वाले विभिन्न खतरों और वे किस प्रकार इनसे निपट सकते हैं, इन सभी बातों को ध्यान में रखते हुए इस वर्कशॉप को तैयार किया गया है। इन मॉड्यूल द्वारा प्रतिभागियों में निम्न योग्यताओं का विकास हो सकेगा :

1. ऑनलाइन खतरों को कम करने के लिए ज़रुरी कौशल।
2. विभिन्न सुरक्षा साधनों और प्रणाली की जानकारी जिसका इस्तेमाल जोखिमों को कम करने के लिए किया जा सकता है।
3. विभिन्न समस्या निवारण प्रणालियाँ जिनका इस्तेमाल साइबर अपराध रिपोर्ट करने के लिए किया जा सकता है।

प्रशिक्षित किए गए शिक्षक डिजिटल साक्षरता और ऑनलाइन सुरक्षा पर स्वतंत्र रुप से जागरुकता सत्र संचालित कर सकते हैं और बड़े पैमाने पर छात्रों और उनके माता-पिता तक पहुँच सकते हैं।

कैसे पहचान करें यदि एक बच्चे के साथ साइबर बुलिंग की जा रही है या वह ऑनलाइन दुर्व्यवहार/ उत्पीड़न का सामना कर रहा है?

यदि बच्चों का शोषण या उत्पीड़न किया जा रहा हो तो आप उसके व्यवहार में कुछ परिवर्तन देख सकते हैं। सबसे ज़्यादा सामान्य रुप से देखे गए संकेतों में शामिल है:

1. खुद को अकेला/ अलग-थलग कर लेना

- इंटरनेट पर बहुत ज़्यादा समय बिताना।

- बहुत ज़्यादा गोपनीय हो जाना/ राज़ रखना/ बातें छुपाना - विशेष रुप से नई टेक्नोलॉजी के उनके उपयोग के बारे में।

- दरवाज़ा बंद करना और किसी और व्यक्ति के कमरे में प्रवेश करने पर जो कुछ स्क्रीन पर है उसे छिपाना।

- अपनी ऑनलाइन गतिविधि के बारे में खुलकर बात ना कर पाना।

- अपने मोबाइल फोन के बारे में अत्यधिक पज़ेसिव बन जाना और चिंतित हो जाना यदि कोई अन्य व्यक्ति उसे उठा ले या उसे देखना चाहे।

- फोन पर जवाब देते समय उत्तेजित व्यवहार और कॉल को गोपनीय रुप से लेने की ज़रुरत महसूस करना।

2. सामाजिक बदलाव

- वे कहाँ जा रहे हैं इसके बिना किसी स्पष्टीकरण के साथ परिवार के घर से काफी समय के लिए बाहर रहने का पैटर्न।

- एक नए दोस्त के बारे में अस्पष्ट बात लेकिन कोई भी आगे की जानकारी पेश ना करना।

- नए दोस्त के साथ ऑनलाइन गोपनीय तरीके से बात करने में काफी ज़्यादा समय बिताना।

- किसी विशिष्ट वयस्क या युवा व्यक्ति के साथ अकेले ना रहने की इच्छा।

3. भावनात्मक बदलाव

- अचानक व्यक्तित्व में समझ में ना आने वाले बदलाव और मूड स्विंग्स (बार बार मूड बदलना)।

- गुस्से या चिड़चिड़ेपन वाला व्यवहार।

- खुद को नुकसान पहुँचाने वाली हरकत/ गतिविधियाँ।

अध्यापक उन्हें भावनात्मक सहयोग प्रदान करें एवं संबल प्रदान करें। आवश्यकता होने पर उनके माता-पिता के माध्यम से वे मानसिक स्वास्थ्य संबंधित अधिकारी से संपर्क कर सकते हैं।

पहली-आवश्यकताएँ:

इनके बारे में मूलभूत ज्ञान:

- इंटरनेट और इंटरनेट इनेबल्ड उपकरण

- स्मार्टफोन के मूलभूत फीचर्स

- सोशल मीडिया प्लैटफॉर्म और लोकप्रिय ऐप्स

- लोकप्रिय रुप से इस्तेमाल किए जाने वाले प्लैटफॉर्म्स की बुनियादी सेटिंग

किशोर छात्रों के लिए ऑनलाइन सुरक्षा - कक्षा 6ठी से 8वीं के लिए
समय : 45 मिनट

संदर्भ स्थापित करना :

पिछले कुछ दशकों में हमने तकनीकी विकास के मामले में लंबा सफर तय किया है और आज जितने अवसर और रास्ते हैं उतने पहले कभी नहीं थे। इनमें से एक है इंटरनेट।

इंटरनेट का इस्तेमाल करने वाली दुनिया की सबसे बड़ी आबादी भारत में है। कुल आबादी के 50% लोग इंटरनेट का इस्तेमाल करते हैं। इस प्रतिशत का मतलब है 687.6 मिलियन (या 68.76 करोड़) इंटरनेट यूज़र्स। यह आंकड़ा कितना बड़ा है आपको इसका दूसरी तरह से अंदाज़ा देना हो तो, यदि आप प्रति सेकंड एक यूज़र की गिनती करते हैं तो आपको इतने सारे यूज़र की गिनती करने में 21 साल लग जाएंगे।

इंटरनेट और साइबरस्पेस

इंटरनेट दुनिया का सबसे बड़ा कम्प्यूटर नेटवर्क है जिसमें दुनिया भर के करोड़ों स्वतंत्र नेटवर्क जुड़े हुए हैं। इंटरनेट को "इन्फॉर्मेशन हाइवे" यानि "जानकारी महामार्ग" भी कहा जाता है। भौगोलिक जगहों से आगे बढ़ने की बजाय, यह आपके विचार और जानकारियों को साइबरस्पेस में आगे बढ़ाता है- विचारों और जानकारियों के इलेक्ट्रॉनिक आवाजाही की दुनिया। इंटरनेट पर किसी का स्वामित्व नहीं है। इसके लिए किसी प्रकार की औपचारिक प्रबंधन संस्था नहीं है। इंटरनेट के कई प्रकार के उपयोग हैं जिनमें शामिल है ईमेल भेजना, फ़ाइलें अपलोड या डाउनलोड करना, वेब सर्फिंग यानि इंटरनेट पर विभिन्न वेबसाइट्स पर जाना और कई अन्य।

हम सभी इंटरनेट नामक नेटवर्कों के एक नेटवर्क द्वारा भारत के अंदर और बाहर की सारी दुनिया में एक दूसरे से जुड़े हुए हैं। इसने हम सभी को साइबरस्पेस नामक वर्चुअल समुदाय का एक हिस्सा बना दिया है, जो अब पांचवां आयाम है।

साइबर सेल द्वारा आपके मामले में ध्यान दिया जाएगा, छानबीन की जाएगी और उचित कार्रवाई की जाएगी।
यदि आपको एफआईआर दर्ज करने में मुश्किल हो रही हो, तो आप या तो पुलिस अधीक्षक या आपके ज़िले के ज़िला मजिस्ट्रेट को एक पत्र लिख सकते हैं, जिनके बारे में विवरण आप ऑनलाइन प्राप्त कर सकते हैं।
एक बार एफआईआर दर्ज किए जाने के बाद, जाँच की जाएगी जिसके बाद अपराधी को गिरफ्तार किया जाएगा।

हेल्पलाइनें और अन्य पोर्टल

यदि आपको कानून प्रवर्तन एजेंसियों तक जाने में सहज महसूस न हो रहा हो तो आप cybercrime.gov.in पोर्टल पर जाकर भी शिकायत ऑनलाइन दर्ज कर सकते हैं। महिला/बच्चों से संबंधित विषयों के लिए एक अलग विभाग है। शिकायत पंजीकृत किए जाने के बाद आपको एक शिकायत संख्या दिया जाएगा और आप ऑनलाइन अपने शिकायत के स्टेटस को देख भी सकते हैं।
यहाँ आप अज्ञात रुप से भी शिकायत दर्ज कर सकते हैं।
सुनिश्चित करें कि आप शिकायत दर्ज कराते समय सबूत व प्रमाण भी अपलोड करें।

इसके साथ ही आप पोक्सो ई-बॉक्स के जरिए भी शिकायत कर सकते हैं। यह एक विशेष पोर्टल है जिसे राष्ट्रीय बाल अधिकार संरक्षण आयोग (एनसीपीसीआर) द्वारा 18 वर्ष से कम उम्र के यूज़र्स के लिए विशेष रुप से तैयार किया गया है। भारत में बाल अधिकार एवं संबंधित विषयों से निपटने के लिए एनसीपीसीआर सर्वोच्च संस्था है। केवल https://ncpcr.gov.in/user_complaints.php इस लिंक पर जाएँ और फॉर्म भरें। आपकी शिकायत दर्ज कर ली गई है और उचित कार्रवाई की जाएगी।
यदि आपको परिवार की सहायता ना मिल रही हो, तो बाल कल्याण समितियाँ (सीडब्ल्यूसी) इन मामलों में शामिल हो जाएंगी और आपके लिए ज़रुरी समर्थन और सहायता देने के लिए उचित कार्रवाई की जाएगी।

सभी प्रमुख प्लैटफॉर्म में "रिपोर्ट" फीचर करीब करीब एक ही तरह काम करता है।

पहला कदम : आप जिस अकाउंट या कंटेंट को रिपोर्ट करना चाहते हैं उसके कोने में तीन डॉट देखिए।

दूसरा कदम : तीन डॉट पर क्लिक करें और आपको रिपोर्ट का विकल्प दिखाई देगा।

तीसरा कदम : रिपोर्ट पर क्लिक करें, और इसके बाद आपके सामने कारणों की एक सूची प्रस्तुत की जाएगी इस बात की पुष्टि (कन्फर्म) करने के लिए की आप अकाउंट या कंटेंट को क्यों रिपोर्ट कर रहे हैं।

चौथा कदम : आप रिपोर्ट करने के अनुरोध के लिए उचित कारण चुनें और कन्फर्म करें।

ज़्यादातर प्लैटफॉर्म्स द्वारा आपके रिपोर्ट करने के अनुरोध के लिए स्वीकृति संदेश दिया जाता है। सुनिश्चित करें कि आप रिपोर्टिंग के लिए उपयुक्त कारण को चुन रहे हैं। जब कोई रिपोर्ट के लिए अनुरोध भेजा जाता है तो प्लैटफॉर्म द्वारा रिपोर्टिंग के लिए कारण और रिपोर्ट किए गए कंटेंट को मिलाकर देखा जाता है। उदाहरण के लिए यदि एक अश्लील फोटो को "स्पैम" रिपोर्ट किया गया हो तो प्लैटफॉर्म द्वारा हो सकता है कोई कार्रवाई ना की जाए क्योंकि कंटेंट स्पैम के तौर पर योग्य नहीं है। सभी कारणों को पढ़ें और ऐसा कारण चुनें जो उस परिस्थिति का सबसे अच्छी तरह से वर्णन करता है।

कानून प्रवर्तन एजेंसी को रिपोर्ट करना

पहला कदम : आपके स्थानीय पुलिस थाने में जाएँ और एक एफआईआर दर्ज कराएँ।

दूसरा कदम : एफआईआर की एक कॉपी प्राप्त करें, जो आपका अधिकार है।

तीसरा कदम : आपके एफआईआर की कॉपी के साथ आपके सबसे करीबी साइबर सेल में जाएँ।

ज़िम्मेदार ऑनलाइन व्यवहार

ऑनलाइन होना अब केवल मज़े और मनोरंजन के लिए नहीं है। कई लोगों के लिए, यह अपनेपन और एक समुदाय का एक हिस्सा होने की भावना देता है, जहाँ अजनबी होने के बावजूद उन्हें स्वीकार किया जाता है।
सुरक्षा की यह भावना अक्सर तब चूर-चूर हो जाती है जब ऑनलाइन होने पर उनके साथ दुर्व्यवहार किया जाता है या उन्हे निशाना बनाया जाता है। जिस तरह भौतिक दुनिया में समुदायों के कुछ सिद्धांत और आचार संहिता होती है, ऑनलाइन में भी यही चीज़ें लागू होती हैं।

इंटरनेट, विशिष्ट रुप से सोशल मीडिया प्लैटफॉर्म्स तस्वीरें, मीम्स, वीडियो और पता नहीं किन प्रकार के चीजों से भरे हुए हैं। अक्सर यूज़र्स अपनी गतिविधियों में बहक जाते हैं और अक्सर ऐसी आदतों में लिप्त हो जाते हैं जो असभ्य या कुछ मामलों में गैरकानूनी भी हो सकते हैं। ट्रोल करना ऐसा ही एक उदाहरण है। सेलिब्रिटीज़ से लेकर राजनेताओं और सामान्य यूज़र्स तक, किसी को भी बख्शा नहीं गया है। हालांकि यदि सही भावना में लिया जाए तो ट्रोल करना नकारात्मक चीज़ नहीं है, लेकिन ऐसे कई मामले हुए हैं जहाँ साझा किया गया कंटेंट पूरी तरह से अश्लील और आपत्तिजनक था। दिलचस्प बात यह है कि जो चीज़ एक के लिए मज़ेदार है वही दूसरे के लिए अपमानजनक हो सकती है।
तो मज़ाकिया और आपत्तिजनक होने के बीच आप किस तरह एक रेखा खींच सकते हैं?
"ऑनलाइन कोई ऐसी चीज़ ना करें या कहें जो आप ऑफलाइन भी नहीं करते हैं", इस व्यवहार का पालन एक ऐसा सरल नियम है जो यह सुनिश्चित भी करता है कि आपका व्यवहार किसी और के लिए आपत्तिजनक या चोट पहुंचाने वाला नहीं है।

इंटरनेट द्वारा पेश की गई गुमनामी का इस्तेमाल कई लोगों द्वारा उनकी सामाजिक चिंता विकार (सोशल एंक्ज़ाइटी) को मात देने और धीरे धीरे उनके संकोची स्वभाव से बाहर आने के लिए किया जाता रहा है। लेकिन इसके साथ ही समान रुप से, बल्कि बड़े पैमाने पर, जब अशोभनीय और दूसरों को परेशान करने वाली गतिविधियों में लिप्त होना होता है तो इसका इस्तेमाल पहचान छुपाने के लिए किया जाता है। हमें यह हमेशा याद रखना चाहिए कि इंटरनेट एक मूल्य मुक्त क्षेत्र नहीं है और ऑफलाइन दुनिया की तरह ही यहां किए गए कार्यों के परिणाम होते हैं, इसे करने वाले और निशाना बनाए गए व्यक्ति दोनों पर। इसे ध्यान में रखते हुए यूज़र के लिए कुछ सिद्धांतों का पालन करना

डाटा सुरक्षा का सबसे महत्वपूर्ण पहलू है सुरक्षित रुप से साझा करना; कहाँ और किस तरह से आपका डाटा उपलब्ध कराया जा रहा है।

सोशल मीडिया के ज़रिए बेहद आसान तरीके से डाटा जोखिम में आ सकता अपराधी बेहद बारिकी से सोशल मीडिया पर नज़र रखते हैं और ऐसी जानकारी तलाश में रहते हैं जिसका वे गलत तरीके से इस्तेमाल कर सकते हैं, जैसे अपडेट, फोटो, वीडियो, इत्यादि। कई बार हम पोस्ट और स्टोरिज के रुप में बारे में गहन जानकारी अन्य यूज़र्स के लिए उपलब्ध करा देते हैं।

चैटिंग करते समय :

सोशल मीडिया पर आपको लोगों का जिस तरह प्रोफाइल दिखता है, हो सकता है वास्तव में वे वैसे ना हों। कोई भी निजी जानकारी ना दें, विशेष रुप से उन लोगों से चैटिंग के दौरान जिन्हें आप वास्तविक जीवन में नहीं जानते हैं।

निजी जानकारी किसे माना जाता है?

मोबाइल नंबर, पता, स्कूल का नाम, माता-पिता से संबंधित कोई जानकारी इत्यादि। कोई भी ऐसी जानकारी जिसे आप किसी अजनबी के साथ साझा नही करेंगे। जो 'दोस्त' आप ऑनलाइन बनाते हैं उनके साथ साझा ना करें। ऐसे यूज़र्स के साथ जुड़ने से बचें जो आपको किसी भी तरह की निजी जानकारी साझा करने के लिए कहता है।

सोशल मीडिया पर :

- इस जोखिम को कम करने के लिए प्रायवेसी सेटिंग का इस्तेमाल करें। सभी प्लैटफॉर्म विभिन्न प्रकार के सेटिंग्ज़ और फीचर्स उपलब्ध कराते हैं और आपका डाटा सुरक्षित करने में मदद करते हैं।

- आम लोगों के लिए आपकी प्रोफाइल फोटो और अन्य जानकारी सार्वजनिक ना करें। आप आपके पोस्ट के लिए दर्शक चुन सकते हैं। आपके पोस्ट, स्टोरिज और अपडेट्स केवल भरोसेमंद दोस्तो के ही देखने के लिए सीमित रखें।

- आपके सभी खातों के लिए अलग पासवर्ड का इस्तेमाल करें। यदि आप एक ही पासवर्ड का इस्तेमाल करते हैं तो आपके अकाउंट के संकट में आने की संभावना बढ़ जाती है।

- उन लोगों के प्रोफाइल की विस्तारपूर्वक जॉच करें जो आपके अकाउंट में दोस्त और फॉलोअर्स के रुप में जुड़ना चाहते हैं। एकबार उन्हें जोड़ लेने के बाद वे आपकी सभी पोस्ट और ऑनलाइन गतिविधियों को देख सकते हैं।

जैसा कि स्पष्ट है, विभिन्न प्लैटफॉर्म के अपने अलग-अलग नियम / मानक होते है और हमारा व्यवहार इसके अनुसार ही होना चाहिए।

यदि कोई आपके नाम और फोटो का इस्तेमाल करते हुए जाली (फेक) अकाउंट तैयार करे तो आप क्या करेंगे?

ऐसे अकाउंट इम्पर्सोनेटेड अकाउंट (दूसरे की पहचान का इस्तेमाल कर तैयार किए गए अकाउंट) के रुप में वर्गीकृत किए जाते हैं। यह करीब करीब प्रत्येक प्लैटफॉर्म के समुदाय के नियमों/ मानकों का उल्लंघन है और इसके साथ ही गैर-कानूनी भी है।

साइबर स्टॉकिंग

साइबर स्टॉकिंग (इंटरनेट पर पीछा करना) का मतलब है किसी भी इलेक्ट्रॉनिक
साधनों द्वारा एक व्यक्ति को बार बार या लगातार फॉलो करना, उस पर निगरानी रखना या संपर्क करना। ऐसे मामले जिनमें पीड़ित की आवाजाही पर नज़र रखी जाती है और उसकी निजता का उल्लंघन किया जाता है या टेक्स्ट, ईमेल, सोशल मीडिया, या अन्य डिजिटल प्लैटफॉर्म के माध्यम से उसकी मर्जी के बिना लगातार संपर्क करने की कोशिश की जाती है। एक बच्चे की साइबर स्टॉकिंग उसका यौन उत्पीड़न करने या फिर अन्य दुर्भावनापूर्ण इरादे के लिए की जा सकती है। इसे एक वयस्क व्यक्ति या फिर एक बड़ी उम्र के बच्चे द्वारा भी किया जा सकता है। किसी बच्चे की साइबर स्टॉकिंग करना भारतीय दंड संहिता (आईपीसी) की धारा 354 डी के अंतर्गत एक दंडनीय अपराध है।

अश्लील सामग्री साझा करना

भारतीय कानूनों के अंतर्गत ऐसी सामग्री भेजना जो अश्लील और यौन रुप से स्पष्ट हो, एक दंडनीय अपराध है। यह आपके पोस्ट पर निजी संदेश या टिप्पणी जोड़ने के रुप में हो सकता है। भारतीय कानूनों के अंतर्गत कामोत्तेजक सामग्री को अश्लील माना गया है। सरल शब्दों में कहें तो कोई भी ऐसी सामग्री जो लैंगिक प्रवृत्ति की हो, वह अश्लीलता के दायरे में आती है।

रिपोर्ट करना

साइबर अपराध रिपोर्ट करने के लिए, या तो उस प्लैटफॉर्म पर जा सकते है जहाँ गैर-कानूनी/अनुचित गतिविधियाँ चल रही हैं या फिर सीधे कानून प्रवर्तन एजेंसियों के पास जा सकते हैं।

प्लैटफॉर्म पर रिपोर्ट करना

यदि आप ऐसे कोई अकाउंट, पोस्ट या गतिविधि देखते हैं जो आपको लगता है कि प्लैटफॉर्म पर नहीं होने चाहिए, तो आप इसे रिपोर्ट कर सकते हैं और यह सुनिश्चित कर सकते हैं कि इन्हें हटा लिया जाए या कम से कम इसे आगे साझा करने से रोका जाए ।

डाटा चोरी

इसे कम्प्यूटर या कम्प्यूटर नेटवर्क के असली मालिक की अनुमति के बिना डाटा कॉपी करने के रुप में परिभाषित किया जा सकता है। इसके कई प्रकार होते हैं, जैसे कार्यस्थल के कम्प्यूटर सिस्टम में अनधिकृत रुप से प्रवेश करना और गोपनीय और संवेदनशील जानकारी कॉपी करना। बिजनेस कम्यूनिकेशन, ग्राहकों के संपर्कों का विवरण, पता, पासवर्ड, यूज़रनेम और अन्य संबंधित दस्तावेज जैसी चीजें डाटा के प्रकार में हो सकती हैं।

वायरस और मैलवेयर (दुर्भावनापूर्ण सॉफ्टवेयर) फैलाना

इसमें शामिल है दुर्भावनापूर्ण कोड, वायरस, वॉर्म, ट्रोजन, स्पायवेयर, ऐडवेयर और रुटकिट्स इंजेक्ट करना और फैलाना। इन्हे निशाना बनाए जाने वाले कम्प्यूटर सिस्टम में इन्स्टॉल किया जाता है और इससे सिस्टम की संवेदनशील जानकारी तक पहुँचा और दूसरी जगह भेजा जा सकता है और कभी कभी इस प्रकार संक्रमित कम्प्यूटर का इस्तेमाल अन्य प्रकार के साइबर अपराध को अंजाम देने के लिए साधन के रुप में किया जा सकता है।

पहचान चोरी

इसका मतलब है जानबूझकर किसी और की पहचान का इस्तेमाल करना, आमतौर पर आर्थिक लाभ उठाने या किसी अन्य व्यक्ति के नाम पर कर्ज़ और अन्य लाभ प्राप्त करना, और संभावित रुप से अन्य व्यक्ति की असुविधा और नुकसान करने का एक तरीका। यूज़र कई साधनों के द्वारा संवेदनशील जानकारी प्राप्त कर सकता है जैसे फिशिंग, ईमेल के ज़रिए पीड़ित को कोई लिंक भेजना और गोपनीय जानकारी प्रस्तुत करने के लिए कहना, या सोशल इंजीनीयरिंग के ज़रिए जानकारी प्राप्त करना, की-लॉगर्स का इस्तेमाल करना, इत्यादि।

जाली (फेक) अकाउंट्स के बारे में?

जब किसी संस्था के लिए, जो वास्तव में नहीं है, या एक इंसान को छोड़कर किसी अन्य चीज़ के लिए एक अकाउंट बनाया जाता है तो ऐसे अकाउंट का वर्गीकरण एक जाली (फेक) अकाउंट के रुप में किया जाता है। फेसबुक उनके "कम्यूनिटी स्टैंडर्ड" (समुदाय मानकों) के अंतर्गत जाली (फेक) अकाउंट के इस्तेमाल किए जाने की अनुमति नहीं देता। वहीं दूसरी ओर इन्स्टाग्राम द्वारा जाली (फेक) अकाउंट तैयार करने और इस्तेमाल किए जाने पर कोई प्रतिबंध नहीं लगाया जाता है।

प्रत्येक समुदाय सम्मान पर आधारित होता है। इसलिए यह ज़रुरी है कि यूज़र्स ऑफलाइन और ऑनलाइन दोनों जगह सम्मानजनक तरीके से पेश आएँ। इसमें, जब हम ऑनलाइन हों तो हमारा व्यवहार और भाषा दोनों शामिल है। भले ही, हमारा सामना ऐसे यूज़र्स से हो सकता है जो इसका पालन नहीं करते, लेकिन हमें व्यक्तिगत स्तर पर सभी लोगों के प्रति सम्मानजनक व्यवहार रखना चाहिए चाहे वो किसी भी पृष्ठभूमि, लिंग, आयु-वर्ग और श्रेणी के हों। शारीरिक रुप से अनुभव कर पाने का अपवाद छोड़ दें, तो यह ध्यान में रखना महत्वपूर्ण है कि ऑनलाइन दुनिया हमारी भौतिक दुनिया की तरह ही है। इसका मतलब यह है कि हमारे एक्शन्स (कृत्य) ऑनलाइन भी उतने ही प्रभावी होती हैं जितना वे भौतिक दुनिया में होते हैं, इसलिए उन्हें नियंत्रण में रखना आवश्यक है।

सुरक्षित डाउनलोडिंग

कंटेंट मुफ्त में डाउनलोड कर पाना इंटरनेट द्वारा पेश की जाने वाली शायद सबसे आकर्षक सेवा है। लेकिन हर वो चीज़ जो आपको मुफ्त में मिलती है वह आपके और आपके उपकरणों के लिए सुरक्षित नहीं होती है।

- ध्यान में रखने वाली पहली सूचना यह है कि मुफ्त कंटेंट के पीछे मत भागिए। इस बात का ख्याल रखें कि मुफ्त में कुछ नहीं मिलता और हर चीज़ के लिए एक कीमत देनी होती है। एप्लिकेशन्स के लिए यह सलाह दी जाती है कि आपको फोन बनाने वाली कम्पनियों के विश्वसनीय एप्लिकेशन स्टोर, जैसे आईओएस आधारित उपकरणों के लिए ऐपस्टोर और एंड्रॉइड उपकरणों के लिए प्लेस्टोर, का ही इस्तेमाल करना चाहिए। अन्य स्त्रोतों की तुलना में यहाँ अपलोड किए गए ऐप्स ज़्यादा भरोसेमंद होते हैं।

- ध्यान में रखने वाली दूसरी सलाह यह है कि जब भी आप ऐप्स डाउनलोड करें तो हमेशा स्त्रोत और डेवलपर की जाँच कर लें। आप जिन ऐप्स को डाउनलोड करना चाहते हैं उनके डेवलपर्स की खोज कर सकते हैं, जिससे यह सुनिश्चित किया जा सके कि आपके उपकरण पर आप सही ऐप्स इन्स्टॉल कर रहे हैं।

- तीसरी सलाह यह है कि डाउनलोड करने से पहले एप्लिकेशन के अन्य पहलू जैसे उनकी रेटिंग्स और रिव्यु (समीक्षा) की जाँच कर लें।

डिजिटल वेल बिंग (डिजिटल स्वास्थ्य)

ज़िम्मेदार व्यवहार के लिए ऑनलाइन और ऑफलाइन के बीच संतुलन बनाए रखना आवश्यक हो जाता है। उचित तरीके से टेक्नोलॉजी के इस्तेमाल से इसके वश मे आने की बजाय हमारे जीवन की गुणवता मे सुधार आएगा। आगे कुछ अच्छी आदतें दी गई हैं जिन्हें हमें हमारे जीवन में शामिल करने की ज़रुरत है।

- जितना समय आप ऑनलाइन बिताते हैं उतना ही समय स्कूल असाइनमेंट, सामाजिक मेल-मिलाप और बाहरी गतिविधियों जैसी अन्य गतिविधियों मे बिताकर संतुलन बनाएँ रखें।

- मोबाइल, लैपटॉप्स, डेस्कटॉप और टैबलेट पर समय बिताने के लिए सीमा निश्चित करें जिससे हम अन्य महत्वपूर्ण चीज़े भी कर पाएँ और एक संतुलित और संतुष्ट जीवन जी सकें। यह कहना कठिन है कि 'कितना', बहुत ज़्यादा होता है। आपके समय के इस्तेमाल को नियंत्रित और संतुलित कर हम हमारे समय के ज़िम्मेदार इस्तेमाल और अच्छी परख का प्रदर्शन कर सकते हैं।

- हमें जो जानकारी प्राप्त होती है उसकी एक सीमा तय करने से हमारे पास पहले से मौजूद जानकारी को प्रोसेस करने में मदद मिलती है, और किस प्रकार की ज़्यादा जानकारी हमें हासिल करने की ज़रुरत है, उसकी पहचान करने में भी हमें मदद मिलती है। मैसेजिंग एप्लिकेशन्स हमें ऐसे फीचर्स हटाने का विकल्प देते हैं, जो हमारी चिंता बढ़ा रही हो। उन विकल्पों का इस्तेमाल करें, हमें दिनभर यह सोचने की ज़रुरत नहीं है कि कौन सा व्यक्ति क्या करेगा।

- मोबाइल फोन पर एप्लिकेशन्स इन्स्टॉल करते समय बेहद सावधानी से इनका चुनाव करें। बहुत संख्या में ऐप्स (विशेष रुप से सोशल नेटवर्किंग के लिए) हमें अत्यधिक इस्तेमाल करने के लिए लुभा सकते हैं। जहाँ एक ओर कम्यूनिकेशन (संचार) के विकल्प बढ़ जाते हैं वहीं दूसरी ओर नोमोफोबिया (स्मार्टफोन की लत) से पीड़ित एक

साइबर अपराध और उनके निराकरण के लिए क्या करें?

अपराध हमारे समाज का एक हिस्सा रहे हैं और इन्हें पूरी तरह खत्म कर पाना हमेशा ही मुश्किल रहा है। लेकिन इंटरनेट और इन्फॉर्मेशन टेक्नोलॉजी की शुरुआत के साथ ऐसे अपराधों को अंजाम देना काफी आसान हो गया है जिनका पता नहीं लगाया जा सकता। यह साइबर अपराध की श्रेणी मे आते हैं। साइबर अपराध को विकिपीडिया एक ऐसे अपराध के रुप में परिभाषित करता है जिसमें एक कम्प्यूटर और एक नेटवर्क शामिल होता है। इसका मतलब यह है कि गैर-कानूनी डाउनलोडिंग से लेकर आर्थिक घोटाले, जाली पहचान वाले अकाउंट, यह सभी साइबर अपराध हैं और दंडनीय हैं। इससे पहले की हम इससे जुड़े कानूनों के बारे मे बात करें, यह समझना महत्वपूर्ण है कि साइबर अपराध के विभिन्न प्रकार क्या हैं और उनका क्या मतलब है।

समाज को नुकसान पहुँचाने वाले विभिन्न अपराधों और गैर-कानूनी गतिविधियों से निपटने के लिए भारत में कई कानूनों का प्रावधान है। आईए भारत मे विभिन्न प्रकार के साइबर अपराधों पर एक नजर डालते हैं।

ग्रूमिंग

कई बार अनजाने व्यक्ति या फिर परिचित लोग भी, यौन दुर्व्यवहार या उत्पीड़न/शोषण के लिए छोटे बच्चों और युवाओं का भरोसा जीतने के लिए उनके साथ ऑनलाइन या आमने सामने एक भावनात्मक संबंध तैयार करते हैं। कई बच्चे और युवा लोग यह महसूस करने लगते हैं कि एक विशेष दोस्ती या संबंध विकसित हो रहा है और उन्हें समझ में नहीं आता कि उन्हें तैयार किया जा रहा है (ग्रूमिंग)। ऐसे दरिंदों का प्रमुख लक्ष्य आपको असंवेदनशील बनाना है और अनुचित व्यवहार को सामान्य महसूस कराना है। वे उपहार, पैसे या फिर गेम्स जैसी चीज़ें देकर आपको लालच दे सकते हैं।

हैकिंग

हैकिंग एक व्यापक शब्द है और इसको इस तरह परिभाषित किया जा करने, चोरी करने या कम्प्यूटर में मौजूद डाटा को नष्ट करने के इरादे कम्प्यूटर में प्रवेश प्राप्त करना। इसे आम तौर पर ऐसे लोगों द्वारा किया जाता है जो कम्प्यूटर टेक्नोलॉजी को अच्छी तरह जानते हैं और कम्प्यूटर सिस्टम में मौजूद कमज़ोरियों का गलत फायदा उठाकर ऐसे अपराध करते हैं।