साइबर बुलिंग

साइबर बुलिंग में किसी के बारे में नकारात्मक, हानिकारक, झूठी या गलत जानकारी और सामग्री भेजना, पोस्ट करना या साझा करना शामिल है। यह एक गंभीर अपराध है जो साइबर कानून के अंतर्गत दंडनीय है।

साइबर बुलिंग में शामिल है

- आपकी पोस्ट या आप से संबंधित पोस्ट पर गंदी टिप्पणियां करना।
- कोई आपके नाम से नकली प्रोफ़ाइल बना रहा है और आपको बदनाम करने की कोशिश कर रहा है।
- ऑनलाइन या मोबाइल फोन पर धमकी भरे या अपमानजनक संदेश भेजना।
- ऑनलाइन समूहों और मंचों से बाहर रखा जाना।
- आपकी अनुमति के बिना ऑनलाइन शर्मनाक तस्वीरें डाल देना।
- साइट पर आपके बारे में अफवाहें और झूठ फैलाना।
- आपके खाते का पासवर्ड चुराना और आपके खाते से अवांछित/अनुचित संदेश भेजना।
- आपत्तिजनक चैट करना।
- आपको बदनाम करने के इरादे से बनाई गई नकली ऑनलाइन प्रोफाइल।

साइबर बुलिंग

प्रतिक्रिया न दें।

अगर कोई आपको साइबर बुलिंग कर रहा है, तो आपको भी वैसा ही करने की ज़रूरत नहीं, कोई प्रतिक्रिया न दें। साइबर बुलिंग का जवाब देना या बदला लेना इस मामले को और भी खराब कर सकता है या आपको किसी बड़ी परेशानी में भी डाल सकता है।

स्क्रीनशॉट

ऐसी कोई भी क्रिया/वस्तु जो आपको लगे कि वह साइबर बुलिंग हो सकती है उसका स्क्रीनशॉट लें और रिकॉर्ड रखें।

ब्लॉक और रिपोर्ट

अधिकांश ऑनलाइन पटल में यह सुविधा होती है, कि यदि कोई आपको परेशान करता है, तो सोशल मीडिया पटल पर उस व्यक्ति को ब्लॉक एवं उसकी रिपोर्ट कर सकते हैं।

इसके बारे में बात करें

साइबर बुलिंग आपको कई तरह से प्रभावित कर सकती है। ऐसा होने पर खुदको अकेला न महसूस करें। अपने माता-पिता और शिक्षकों को बताएं कि क्या हो रहा है। इसे सिर्फ खुद तक कभी न रखें।

निजता रखें

अपने सोशल मीडिया खाते में उच्च गोपनीयता सेटिंग्स रखें और किसी ऐसे व्यक्ति से न जुड़ें जिसे आप ऑफ़लाइन नहीं जानते हैं। जब आप सड़क पर अनजान लोगों से बात नहीं करते हैं, तो इसे ऑनलाइन क्यों करें

सावधान रहें

साइबर दुनिया में सभी निवारक और सुरक्षा उपायों से अघटन रहें।

साइबर दुनिया में सुरक्षित रहें

विद्ययाऽमृतमश्नुते

एन सी ई आर टी
NCERT

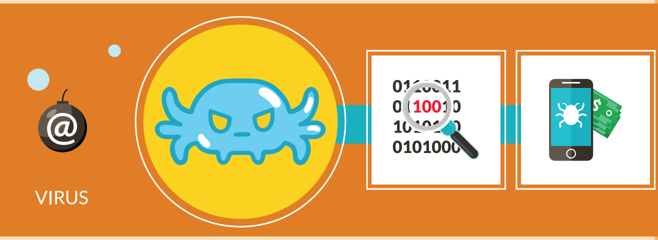
केंद्रीय शैक्षिक प्रौद्योगिकी संस्थान
राष्ट्रीय शैक्षिक अनुसंधान और प्रशिक्षण परिषद्
श्री अरविंद मार्ग, नई दिल्ली -110016

Tel. :- 011-26962580 | Fax :- 011-26864141
E-mail:- jdciet.ncert@nic.in
ncert.nic.in | ciet.ncert.gov.in
PM eVidya IVRS : #8800440559
MANODARPAN IVRS : #844 844 0632

साइबर सुरक्षा और बचाव की मूल बातें

साइबर सुरक्षा और बचाव की मूल बातें

साइबर सुरक्षा सूचना और संचार प्रौद्योगिकी का सुरक्षित और जिम्मेदार उपयोग है। यह केवल जानकारी को सुरक्षित रखने के बारे में नहीं है, बल्कि उस जानकारी के प्रति जिम्मेदार होने, ऑनलाइन अन्य लोगों का सम्मान करने और अच्छे 'नेटिकेट' (इंटरनेट शिष्टाचार) का व्यवहार करने के बारे में भी है। इसमें नेटवर्क, कंप्यूटर, प्रोग्राम और डेटा को हमले, क्षति या अनधिकृत पहुँच से बचाने के लिए डिज़ाइन की गई तकनीकी प्रक्रियाओं और आचरणों के निकाय शामिल हैं।



कंप्यूटर सुरक्षा और बचाव

- जब उपयोग में न हो तो अपने कंप्यूटर को लॉग ऑफ कर दें और उसे अप्राप्य न रहने दें।
- कंप्यूटर को सीधे इलेक्ट्रोनिक बोर्ड आउटलेट में प्लग न करें क्योंकि पावर सर्ज कंप्यूटर को खराब कर सकता है। इसके बजाय, कंप्यूटर को प्लग करने के लिए स्टेबलाइज़र का उपयोग करें।
- पायरेटेड सॉफ़्टवेयर का उपयोग न करें।
- अज्ञात उपकरणों को अपने कंप्यूटर से कनेक्ट न करें क्योंकि उनमें वायरस हो सकते हैं।
- केवल सत्यापित खुले संसाधनों या प्रमाणित सॉफ़्टवेयर और अघटन का उपयोग करें
- जाँचें कि प्रत्येक सिस्टम में एंटीवायरस सॉफ़्टवेयर नियमित रूप से अपडेट होते हैं कि नहीं।
- एक मजबूत फायरवॉल में खर्च करें।
- कंटेन्ट फ़िल्टरिंग सॉफ़्टवेयर का उपयोग करके फ़ाइल एक्सटेंशन जैसे .bat, .cmd, .exe, .pif को ब्लॉक करें।
- विशिष्ट मजबूत पासवर्ड दिशानिर्देशों के साथ एक पासवर्ड प्रोटोकॉल रखें, अपने पासवर्ड को बार-बार बदलें, पुराने पासवर्ड का पुन: उपयोग न करें।
- यह सुनिश्चित करें कि कंप्यूटर सिस्टम और लैब में केवल अधिकृत कर्मियों द्वारा ही सहायता प्रदान की जाए।
- नेटवर्क पर व्यक्तिगत उपकरणों जैसे USB या हार्ड ड्राइव के उपयोग से बचें।

इंटरनेट सुरक्षा और नैतिकता

- अन्य लोगों की निजता का सम्मान करें।
- चैटिंग, ब्लॉगिंग और ईमेल करते समय भाषा के उपयोग में उचित व्यवहार का पालन करें।
- अन्य लोगों के ईमेल खातों में लॉग इन न करें।
- कॉपीराइट सामग्री को डाउनलोड एवं उपयोग न करें।
- दुर्भावनापूर्ण साइटों की पहचान सुनिश्चित करने के लिए स्वचालित ब्राउज़र अपडेट सक्षम करें।

सुरक्षित ईमेल प्रथाएं

- अज्ञात व्यक्ति के ईमेल का जवाब न दें, भले ही वह एक प्रामाणिक ईमेल की तरह लग रहा हो।
- नाम, जन्म तिथि, स्कूल का नाम, पता, माता-पिता का नाम या कोई अन्य जानकारी जैसी व्यक्तिगत जानकारी न दें
- आकर्षक ऑफ़र/छूट के झांसे में न आएं क्योंकि वे अज्ञात स्रोत से आ रहे हैं और यह संभव है कि यह विश्वसनीय न हो। उन मेल्स को इग्नोर/डिलीट करें
- संलग्नक न खोलें या अज्ञात व्यक्ति द्वारा भेजे गए मेल के लिंक पर क्लिक न करें, क्योंकि उनमें दुर्भावनापूर्ण फ़ाइलें हो सकती हैं जो आपके डिवाइस को प्रभावित कर सकती हैं। केवल उन वेबसाइटों के लिंक और डाउनलोड पर क्लिक करें जिन पर आप भरोसा करते हैं।
- लुभावने/झाँसा देने वाले वेबसाइटों से सावधान रहें। वेबसाइट सुरक्षित है या नहीं, इसकी पुष्टि करने के लिए URL की जाँच करें।
- स्पैम या संदिग्ध ईमेल को दूसरों को फॉरवर्ड न करें।

सुरक्षित सोशल नेटवर्किंग

- अपनी उम्र, पता, टेलीफोन नंबर, स्कूल का नाम इत्यादि जैसी अपनी व्यक्तिगत जानकारी का बहुत अधिक खुलासा करने से बचें क्योंकि इससे आपके पहचान की चोरी हो सकती है।
- सोशल नेटवर्किंग साइट्स पर अपनी गोपनीयता सेटिंग बहुत सावधानी से करें।
- अपना पासवर्ड कभी भी अपने माता-पिता या अभिभावक के अलावा किसी और को न बताएं।
- केवल उन लोगों के साथ संवाद और सहयोग करें जिन्हें आप जानते हैं।
- ऐसा कुछ भी पोस्ट न करें जिससे दूसरों की भावनाओं को ठेस पहुंचे।
- सोशल नेटवर्किंग साइट्स पर तस्वीरें, वीडियो और किसी भी अन्य संवेदनशील जानकारी को करते समय हमेशा सावधान रहें क्योंकि वे डिजिटल फुटप्रिंट्स छोड़ देते हैं जो हमेशा के लिए ऑनलाइन रहते हैं।
- अपने दोस्तों की जानकारी नेटवर्किंग साइट्स पर पोस्ट न करें, जो संभवत: उन्हें जोखिम में डाल सकती हैं। समूह फ़ोटो, स्कूल के नाम, स्थान, आयु आदि पोस्ट न करके अपने मित्रों की गोपनीयता की रक्षा करें।
- नेटवर्किंग साइटों पर अपनी योजनाओं और गतिविधियों को पोस्ट करने से बचें।
- किसी भी सोशल नेटवर्किंग साइट पर अपने लिए फर्जी प्रोफाइल न बनाएं। यदि आपको संदेह है कि आपके सोशल नेटवर्किंग अकाउंट के विवरण से छेड़छाड़ की गई है या चोरी हो गई है, तो तुरंत नेटवर्किंग साइट की सहायता टीम को रिपोर्ट करें।
- सोशल मीडिया पर जो कुछ भी आप पढ़ते हैं, उसे किसी विश्वसनीय स्रोत से सत्यापित किए बिना फॉरवर्ड न करें।
- सोशल नेटवर्किंग साइट्स के माध्यम से हमेशा लिंक और अटैचमेंट खोलने से बचें।
- लॉग इन करने के बाद कभी भी अपने खाते को खुला न छोड़ें, जब आप इसका उपयोग नहीं कर रहे हों तो तुरंत लॉग आउट करें।