शिकायत दर्ज करने की प्रक्रिया

साइबर क्राइम की शिकायतों को साइबर क्राइम सेल में दर्ज किया जा सकता है। शिकायत दर्ज करने की प्रक्रिया ऑनलाइन और ऑफलाइन दोनों तरह से होती है और पीड़ित अपनी सुविधा के अनुसार प्रक्रिया चुन सकता है।

- **ऑफलाइन प्रक्रिया**

साइबर क्राइम का शिकार साइबर क्राइम सेल में लिखित शिकायत दर्ज करा सकता है। लिखित शिकायत साइबर क्राइम सेल के प्रमुख को पीड़ित के संपर्क विवरण और उस विशेष साइबर अपराध से संबंधित दस्तावेजों के साथ संबोधित की जानी चाहिए।

- **ऑनलाइन प्रक्रिया**

साइबर अपराध की शिकायतें राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल पर दर्ज की जा सकती हैं। आवश्यक विवरण हैं आकस्मिक विवरण [घटना का वर्णन करना], संदिग्ध का विवरण और शिकायतकर्ता का विवरण।

हालाँकि, यदि अपराध महिलाओं या बच्चों से संबंधित है, तो इसे गुमनाम रूप से भी दर्ज किया जा सकता है।

क्या होता है साइबर क्राइम?

भारत में समर्पित साइबर सुरक्षा कानून नहीं है।

सूचना प्रौद्योगिकी अधिनियम, 2000 साइबर सुरक्षा, साइबर अपराध के साथ-साथ इलेक्ट्रॉनिक डेटा की सुरक्षा पर कुछ प्रावधानों से संबंधित है।

अधिनियम और विभिन्न मामलों के तहत साइबर अपराध का अर्थ है:

जब कोई अपराध कंप्यूटर, कंप्यूटर नेटवर्क, इंटरनेट या किसी अन्य इंटरनेट सेवा या इलेक्ट्रॉनिक उपकरण के उपयोग या उसकी भागीदारी के साथ किया जाता है, तो इसे साइबर अपराध कहा जाता है।

अनिवार्य रूप से, 'साइबर' शब्द में कंप्यूटर, कंप्यूटर नेटवर्क, कंप्यूटर डिवाइस, सॉफ्टवेयर, इंटरनेट, ईमेल, वेबसाइट, डेटा स्टोरेज डिवाइस और अन्य इलेक्ट्रॉनिक डिवाइस (मोबाइल फोन, एटीएम मशीन, आदि) से संबंधित सभी चीजें शामिल हैं।

॥वसुधैव कुटुम्बकम्॥

SYMBIOSIS
LAW SCHOOL, NOIDA

साइबर सुरक्षा और डेटा की सुरक्षा

न्याय बंधु
Pro Bono Legal Services

NYAYA BANDHU
PRO BONO LEGAL SERVICES

अधिकारक्षेत्रा

- पीड़ित के लिए यह आवश्यक नहीं है कि वह उस शहर के साइबर क्राइम सेल में शिकायत दर्ज कराए जिसमें वे रह रहे हैं या जहां अपराध किया गया था।

- साइबर क्राइम की शिकायत भारत में स्थापित किसी भी साइबर क्राइम सेल में दर्ज की जा सकती है।

साइबर सेल हेल्पलाइन्स

- साइबर धोखाधड़ी के लिए राष्ट्रीय हेल्पलाइन - 155260 (छत्तीसगढ़, दिल्ली, मध्य प्रदेश, राजस्थान, तेलंगाना, उत्तराखंड और उत्तर प्रदेश के लिए लागू)

- राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल -https://cybercrime.gov.in/

- उत्तर प्रदेश साइबर क्राइम - sp-cyber.lu@up.gov.in

इंटरनेट सुरक्षा युक्तियाँ

- **मजबूत पासवर्ड चुनें:**

Eएक आसान पासवर्ड आपके साइबर सिक्योरिटी को मुश्किल में डाल सकता है। एक मजबूत पासवर्ड वह है जो अद्वितीय और जटिल है - कम से कम 10 वर्ण लंबा, अक्षरों, संख्याओं और विशेष वर्णों को मिलाकर।

- **अपडेटेड एंटीवायरस रखें:**

इंटरनेट सुरक्षा सॉफ़्टवेयर अधिकांश मैलवेयर का पता लगाएगा और उन्हें हटा देगा। अपने ऑपरेटिंग सिस्टम के अपडेट और आपके द्वारा उपयोग किए जाने वाले एप्लिकेशन के अपडेट के साथ अपडेट रहना सुनिश्चित करें।

- **अपनी गोपनीयता सेटिंग सेट करें:**

वेब ब्राउज़र और मोबाइल ऑपरेटिंग सिस्टम दोनों में ऑनलाइन आपकी गोपनीयता की सुरक्षा के लिए सेटिंग्स उपलब्ध हैं। कभी-कभी इन सेटिंग्स को ढूंढना मुश्किल होता है क्योंकि कंपनियां आपकी व्यक्तिगत जानकारी को उसके मार्केटिंग मूल्य के लिए चाहती हैं। सुनिश्चित करें कि आपने इन गोपनीयता सुरक्षा उपायों को सक्षम किया है, और उन्हें सक्षम रखें।

*स्रोत: कास्परस्की संसाधन

साइबरस्पेस के प्रचलित अपराध

- **फ़िशिंग**

Pफ़िशिंग हमलों का उद्देश्य किसी की व्यक्तिगत जानकारी को पुनः प्राप्त करना और इसका उपयोग पीड़ितों को ईमेल और वेबसाइटों का उपयोग करके उन्हें नुकसान पहुँचाने के लिए करना है जो हानिरहित या सुरक्षित लगते हैं।

- **वेष बदलना**

किसी की ऑनलाइन उपस्थिति को "प्रतिरूपित" करने और फिर उस व्यक्ति की प्रतिष्ठा को नुकसान पहुंचाने के लिए सामग्री भेजने या पोस्ट करने के लिए विभिन्न ऑनलाइन टूल का उपयोग किया जा सकता है।

- **मोर्फिंग**

मॉर्फिंग का अर्थ है इंटरनेट पर उपलब्ध टूल का उपयोग करके एक छवि को दूसरी छवि में बदलना। इन विकृत छवियों का इस्तेमाल पीड़ितों को समझौता करने की स्थिति में दिखाकर ब्लैकमेल करने के लिए किया जा सकता है।