IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

सोशल नेटवर्किंग साइट्स पर साइबर अपराध

प्रियांशु सिंह[1]

मुशीरा जावेद[2]

शोध छात्र , राजनीति विज्ञान विभाग, काशी हिन्दू विश्वविद्यालय।

शोध छात्रा , राजनीति विज्ञान विभाग, काशी हिन्दू विश्वविद्यालय।

सारांश

उभरती हुई इंटरनेट प्रौद्योगिकी के विकास और इसके व्यापक ज्ञान ने सुरक्षा समस्या और साइबर-अपराधों जैसी समस्या उत्पन्न की है। सोशल नेटवर्किंग वेबसाइटों का उपयोग दुनिया भर में लोगों के बीच बातचीत के लिए एक संचार के रूप में किया जाता है, यह लोगों के जीवन को जोड़ने, उत्पाद खरीदने, जानकारी साझा करने आदि में मदद करता है, लेकिन दुर्भाग्य से, इन अनगिनत फायदों के साथ कई खतरे भी आते हैं। भले ही ऐसा प्रतीत होता है कि सोशल मीडिया ने दुनिया को करीब ला दिया है, लेकिन इसका एक दूसरा पक्ष भी है। कई अपराधी इसका उपयोग पहचान की चोरी, साइबर आतंकवाद, आपत्तिजनक संदेश भेजना इत्यादि जैसे अपराध को अंजाम देने के एक संवेदनशील साधन के रूप में करते है और जागरूकता की कमी या सोशल नेटवर्किंग साइटों के अत्यधिक उपयोग के कारण हममें से कई लोग ऐसे जाल में फंस जाते हैं। पेपर का उद्देश्य इस बात पर प्रकाश डालना है कि कैसे सोशल नेटवर्किंग वेबसाइटों के विकास और बढ़ते उपयोग ने साइबर अपराधियों को अपनी अवैध गतिविधियों को अंजाम देने के लिए और अधिक गुंजाइश प्रदान की है और इन सोशल नेटवर्किंग साइटों पर होने वाले साइबर अपराधों से संबंधित मामलों ने लोगों का ध्यान आकर्षित किया है। पेपर में साइबर अपराधों को विनियमित करने के लिए विभिन्न धाराओं के तहत बनाए गए कानूनों को भी शामिल किया गया है।

संकेत शब्द : साइबर अपराध , सोशल मीडिया , नेटवर्किंग , इंटरनेट , साइबर ला

प्रस्तावना

वेब का व्यापक उपयोग साइबर अपराधियों को एक मंच प्रदान करता है। सोशल मीडिया नेटवर्किंग बढ़ाने और डेटा को ऑनलाइन साझा करने के विचार पर बनाई गई वेबसाइटों और एप्लिकेशन का एक वर्गीकरण है। लोकप्रिय सोशल मीडिया एप्लिकेशन फेसबुक, व्हाट्स ऐप, ट्विटर, स्काइप, इंस्टाग्राम, यूट्यूब आदि हैं। पिछले कुछ वर्षों में सोशल मीडिया ने समाज में लोकप्रियता प्राप्त की। विश्व स्तर पर सोशल मीडिया द्वारा प्रदान किए जाने वाले असंख्य लाभों के बावजूद, लोगों को सोशल मीडिया से जुड़े खतरों के प्रति जागरूक करने की आवश्यकता है। दुर्भाग्य से, सोशल मीडिया साइबर अपराधियों के लिए अपनी गंदी गतिविधियों को अंजाम देने का पसंदीदा मंच बन गया है। साइबर अपराधी वे हैं जो नियमों और विनियमो और कानून जिसे साइबर-अपराध के रूप में जाना जाता है का उल्लंघन करते हुए कंप्यूटर नेटवर्क के माध्यम से आपराधिक गतिविधियों को अंजाम देते हैं। साइबर अपराधों के सामान्य उदाहरण में डाटा चोरी, क्षति, सॉफ़्टवेयर चोरी आदि आते हैं। साइबर अपराधी सोशल मीडिया उपयोगकर्ताओं को उनके व्यक्तिगत विवरण जैसे उम्र, लिंग, पता, फोन नंबर, आदि को प्रकाशित करने के लिए उन्हे उकसाते हैं, जिससे वह प्राप्त उन व्यक्तिगत जानकारियों का गलत उपयोग कर सके अपने अवैध उद्देश्यों की पूर्ति के लिए। अतः हम कह सकते हैं कि सोशल मीडिया साइबर अपराधियों को व्यक्तिगत जानकारी में हेरफेर करने और अपराध करने के लिए इसका उपयोग करने के लिए मंच प्रदान करता है।

[1] शोध छात्र , राजनीति विज्ञान विभाग, काशी हिन्दू विश्वविद्यालय।

[2] शोध छात्रा , राजनीति विज्ञान विभाग, काशी हिन्दू विश्वविद्यालय।

सोशल मीडिया

सोशल नेटवर्क एक ऐसी वेबसाइट या एप्लिकेशन है जो उपयोगकर्ताओं को डेटा, टिप्पणियां, संदेश, चित्र आदि पोस्ट करके एक दूसरे के साथ संवाद करने की अनुमति देता है। सोशल मीडिया कंप्यूटर आधारित ऐसी तकनीक है जो वर्चुअल नेटवर्क और समुदायों के निर्माण के माध्यम से विचारों, अवधारणाओ, योजनाओ और डेटा को साझा करने की सुविधा प्रदान करती है। सोशल मीडिया की शुरुवात या प्रारंभ दोस्तों और परिवार के साथ बात-चीत या संवाद करने के तरीके के रूप में हुई थी, हालांकि बाद में इसे उन व्यवसायों द्वारा अपनाया गया जो एक लोकप्रिय नई संचार पद्धति के माध्यम से ग्राहकों तक पहुंचना चाहते थे। फोर्ब्स के मुताबिक पूरी दुनिया में करीब 1 अरब सोशल मीडिया अकाउंट हैं, ये अकाउंट लगभग सभी देशों में बने हैं जो लोगों को एक दूसरे से जोड़े हुए है. आज की आधुनिक दुनिया में सोशल मीडिया बहुत आम है, सोशल मीडिया को मानवता की सबसे बड़ी उपलब्धियों और सफलताओ में से एक माना जाता है।

साइबर अपराध

साइबर-अपराध कंप्यूटर या डिजिटल उपकरणों से जुड़ा एक खतरनाक अपराध है, जिसके दौरान एक पी.सी या तो अपराध का लक्ष्य है, अपराध का एक उपकरण है या इसमें अपराध का सबूत है। साइबर अपराध कानूनी ढांचे में सबसे जटिल वैश्विक मुद्दों में से एक बन गया है। साइबर अपराध मुख्य रूप से इंटरनेट पर होने वाली किसी भी आपराधिक गतिविधि की रूपरेखा तैयार करता है। . ऐसे कई उदाहरण हैं जैसे धोखाधड़ी, मैलवेयर जैसे वायरस, पहचान की चोरी और साइबर स्टॉकिंग। साइबर अपराधों को मोटे तौर पर तीन समूहों में वर्गीकृत किया गया है जिन्हे हम निम्न के विरुद्ध हम देख सकते हैं:

व्यक्ति : व्यक्तियों के विरुद्ध साइबर अपराध में मुख्य रूप से ऐसी गतिविधियाँ शामिल होती हैं जिनमें किसी व्यक्ति से प्रत्यक्ष या अप्रत्यक्ष रूप से निजी जानकारी निकालने के लिए एक उपकरण के रूप में इंटरनेट और कंप्यूटर का उपयोग किया जाता है, और व्यक्ति की सहमति के बिना या व्यक्ति की प्रतिष्ठा को ख़राब करने के लिए इसे ऑनलाइन प्लेटफ़ॉर्म पर अवैध रूप से प्रकट किया जाता है। व्यक्ति के विरुद्ध साइबर अपराधों में हम साइबर स्टॉकिंग, फिशिंग, पहचान की चोरी, मैलवेयर हमले, रैंसमवेयर संक्रमण, हैकिंग इत्यादि अपराधों को देख सकते हैं।

संपत्ति : साइबर अपराधों की दूसरी श्रेणी सभी प्रकार की संपत्ति के खिलाफ साइबर अपराधों की है, इन अपराधों में साइबरस्पेस के माध्यम से अनधिकृत कंप्यूटर अतिक्रमण, कंप्यूटर वैन्डलिज़म, हानिकारक कार्यक्रमों का प्रसारण और कम्प्यूटरीकृत जानकारी पर अनधिकृत कब्ज़ा शामिल है। अर्थात इस प्रकार के साइबर अपराध में किसी व्यक्ति के बैंक विवरण चुराना और पैसे उड़ा देना शामिल है; बार-बार ऑनलाइन खरीदारी करने के लिए मास्टरकार्ड का दुरुपयोग करना, किसी संगठन की वेब साइट तक पहुंच प्राप्त करने या संगठन के सिस्टम को बाधित करने के लिए मेलिसियस पैकेज का उपयोग करना इत्यादि शामिल हैं।

सरकार : सरकार के विरुद्ध अपराधों में साइबर आतंकवाद भी शामिल है। यदि अपराधी सफल हो जाते हैं, तो इससे नागरिकों में तबाही और दहशत फैल सकती है। इस वर्ग में अपराधी सरकारी वेबसाईट, सैन्य वेबसाईट हैक कर लेते हैं।

सोशल मीडिया पर साइबर अपराध

1. हैकिंग

हैकिंग का तात्पर्य आमतौर पर कंप्यूटर या नेटवर्क में अनधिकृत घुसपैठ से है। साइबर लक्षित उपयोगकर्ताओं के डिजिटल उपकरणों तक पहुंच का आग्रह करने के लिए अपराधी पूरी तरह से अलग हमले की तकनीकों का उपयोग करते हैं। साइबर अपराधी सोशल मीडिया उपयोगकर्ता को ईमेल या संदेश भेजते हैं, जब उपयोगकर्ता उस लिंक पर

क्लिक करते हैं तो अपराधी उसे हैक कर लेते हैं। हैकिंग का तात्पर्य नॉन-मेलिसियस गतिविधियों से भी हो सकता है, जिसमें आमतौर पर उपकरण या प्रक्रियाओं में असामान्य या तात्कालिक परिवर्तन शामिल होते हैं।

2. आइडेंटिटी थेफ्ट

आइडेंटिटी थेफ्ट या पहचान की चोरी एक गंभीर अपराध है जिसका पीड़ितों पर हानिकारक और व्यापक प्रभाव पड़ता है। ऑनलाइन पहचान की चोरी सबसे आम साइबर अपराध है। पहचान की चोरी, उपयोगकर्ताओं की अनुमति के बिना नकदी चुराने या धोखाधड़ी करने के लिए किसी की पहचान चुराने के लिए की जाती है। पहचान धोखाधड़ी के लिए लोगों का निजी डेटा प्राप्त करने के लिए पहचान चोर अधिक से अधिक प्रौद्योगिकी का उपयोग कर रहे हैं। साइबर अपराधी लक्षित उपयोगकर्ताओं का डेटा इकट्ठा करने के लिए सोशल मीडिया का उपयोग करते हैं। अपराधी अवैध गतिविधियों को अंजाम देने के लिए चुराए गए डेटा का उपयोग करते हैं।

3. फिशिंग

यह सर्वविदित है कि ईमेल संदेश, टेक्स्ट और फोन कॉल आम तौर पर अपराधियों द्वारा धन या पहचान संबंधी धोखाधड़ी करने के उद्देश्य से उपयोग में लाई जाने वाली रणनीतियाँ हैं। साइबर अपराधियों के बीच सोशल मीडिया फ़िशिंग हमला पहली पसंद है। फ़िशिंग सोशल मीडिया पर एक आम ख़तरा है जिसके दौरान अपराधी नकली वेबसाईट बनाता और नियंत्रित करता है, ऐसी वेबसाइटें जो पीड़ितों को व्यक्तिगत जानकारी प्रकट करने के लिए, लुभाने के लिए वास्तविक प्रतीत होती हैं। आम तौर पर, उपयोगकर्ताओं को सोशल नेटवर्किंग साइटों पर लिंक प्राप्त होते हैं और जब वे उस लिंक पर टैप करते हैं तो अपराधी सभी उपयोगकर्ताओं का डेटा एकत्र कर लेते हैं और फिर उस प्राप्त डाटा का उपयोग अपने अवैध उद्देश्यों को पूरा करने के लिए करते हैं।

4. साइबर बुलिङ्ग और साइबर स्टॉकिंग

सोशल नेटवर्किंग साइटों से संबंधित कुछ सामान्य खतरे साइबर बदमाशी और साइबरस्टॉकिंग हैं। साइबर बुलिङ्ग किसी व्यक्ति को परेशान करने, धमकी देने, शर्मिंदा करने या निशाना बनाने के लिए इंटरनेट, ईमेल और सोशल नेटवर्किंग साइटों जैसी तकनीक का उपयोग है। साइबर बुलिङ्ग या किसी भी प्रकार की बुलिङ्ग कानून के विरुद्ध है। इसके भयानक परिणाम हो सकते हैं। साइबर स्टॉकिंग को ऐसे व्यक्ति के रूप में परिभाषित किया गया है जो स्पष्ट इंटरनेट या ऑनलाइन संचार में अरुचि के संकेत के बावजूद उस व्यक्ति का पीछा करता है या उससे संपर्क करता है। इन अपराधों के लिए कानून में सजा और यह तक की कारावास का भी प्रावधान हैं।

5. आपराधिक गतिविधियों के वीडियो पोस्ट करना

जैसे-जैसे स्मार्टफोन और सोशल मीडिया तकनीक में निरंतर सुधार हो रहा है, बहुत सारे और अधिक अपराधी अपने अपराधों के वीडियो सोशल मीडिया पर पोस्ट कर रहे हैं। हालाँकि यह कुछ हद तक नृशंस लगता है, लेकिन कई पुलिस विभागों के रूप में यह बहुत ही अदूरदर्शी है और अभियोजक इन अपराधियों को गिरफ्तार करने और दोषी ठहराने के लिए इन वीडियो पर निर्भर रहने में सक्षम हैं।

भारत में केसेस

- गूगल इंडिया प्राइवेट लिमिटेड बनाम विसाका इंडस्ट्रीज़ लिमिटेड

निर्माण सामग्री कंपनी विसाका इंडस्ट्री लिमिटेड ने 2011 में आपराधिक साजिश रचने और कंपनी के बारे में झूठी मानहानिकारक सामग्री प्रकाशित करने के लिए Google इंडिया के खिलाफ मामला दर्ज किया था। आरोप है कि गोपाल कृष्ण नाम के एक ब्लॉगर ने सामग्री फैलाने के लिए Google के Blogspot.com का इस्तेमाल किया जिसमें कहा गया था कि, कंपनी का संबंध कांग्रेस पार्टी से है और इसलिए कंपनी एस्बेस्टस का निर्माण कर सकती है। ए.पी. उच्च न्यायालय ने गूगल इंडिया को उत्तरदायी ठहराया और इसलिए उसने एस.सी. में अपील दायर की जो अभी भी लंबित है।

- सुहास कट्टी बनाम तमिलनाडु

  यह भारत में पहला मामला था जहां आईटी अधिनियम, 2000 की विवादास्पद धारा 67 के तहत इंटरनेट पर अश्लील संदेश पोस्ट करने के संबंध में सजा सुनाई गई थी। मामले में एक महिला ने पुलिस से एक शख्स की शिकायत की जो याहू मैसेज ग्रुप में उसे अश्लील मैसेज भेज रहा था. आरोपी ने पीड़िता के नाम से खोले गए फर्जी खाते में प्राप्त ईमेल भी अग्रेषित किए। पीड़िता को ऐसे लोगों के फोन भी आए जिन्होंने मान लिया कि वह एक वेश्या है।

- जनहित मंच एवं अन्य बनाम भारत संघ

  इस याचिका में अश्लील वेबसाइटों पर पूर्ण प्रतिबंध लगाने की मांग की गई। एनजीओ ने तर्क दिया था कि स्पष्ट यौन सामग्री प्रदर्शित करने वाली वेबसाइटों से लोगों पर अत्यधिक बुरा प्रभाव पड़ता है जिनमें विशेषकर युवाओं पर, जिससे युवा अपराधी पथ पर अग्रसर होते हैं।

- श्रेया सिंघल बनाम भारत संघ

  इस मामले में आईटी एक्ट की धारा 66ए की वैधता को सुप्रीम कोर्ट में चुनौती दी गई थी। श्रेया सिंघल बनाम भारत संघ वाद में सर्वोच्च न्यायालय ने कहा कि "धारा 66A मनमाने ढंग से, अत्यधिक और विषमतापूर्ण रूप से अभिव्यक्ति की स्वतंत्रता के अधिकार पर हमला करती है और इस तरह के अधिकार तथा युक्तियुक्त प्रतिबंधों के बीच संतुलन को भी विचलित करती है।"

सोशल मीडिया पर होने वाले अपराधों से संबंधित कानूनी प्रावधान

सूचना प्रौद्योगिकी अधिनियम, 2000 सोशल मीडिया पर अपराधों से संबंधित कानूनी प्रावधान प्रदान करता है:

1. साइबर मानहानि
   कंप्यूटर या इंटरनेट की मदद से किसी अन्य व्यक्ति के खिलाफ अपमानजनक सामग्री प्रकाशित करना साइबर मानहानि कहलाता है। मानहानि का अपराध आईपीसी की धारा 500 के तहत 2 साल तक की साधारण कैद या जुर्माना या दोनों से दंडनीय है। सूचना प्रौद्योगिकी अधिनियम की धारा 66 ए, 2000 विशेष रूप से साइबर मानहानि के अपराध से संबंधित नहीं है, लेकिन यह अपमान, अपकार या आपराधिक धमकी के लिए घोर आपत्तिजनक सामग्री भेजने के कार्य को दंडनीय बनाता है।
2. साइबर अश्लीलता एवं पॉर्नाग्रफी
   आईटी अधिनियम, 2000 साइबर अश्लीलता के सभी पहलुओं का प्रावधान करता है और इसके लिए दंड देता है:

- धारा **66**ई **(**गोपनीयता का उल्लंघन**)** : जो कोई जानबूझकर या विशेष उद्देश्य से किसी व्यक्ति की गोपनीयता का उल्लंघन करने वाली परिस्थितियों में उसकी सहमति के बिना उसके निजी क्षेत्र की कार्य-क्रियाओं को कैप्चर, प्रकाशित या प्रसारित करता है, उसे कारावास से दंडित किया जाएगा जिसे तीन साल तक बढ़ाया जा सकता है या दो लाख तक जुर्माना लगाया जा सकता हैं।
- धारा **67** इलेक्ट्रॉनिक रूप में अश्लील सामग्री प्रकाशित या प्रसारित करने के लिए सजा **:** जो कोई ऐसी सामग्री इलेक्ट्रॉनिक रूप में प्रकाशित या प्रसारित करता है जो कामुक, उत्तेजित करने वाला या ऐसा जो निम्न मानसिक प्रवित्ती वाले व्यक्ति हो उनको अपने प्रभाव में ले सके। ऐसी प्रासंगिक परिस्थितियों में,

उसमें निहित या सन्निहित मामले को पढ़ने, देखने या सुनने के लिए, पहली बार दोषी ठहराए जाने पर एक अवधि के लिए कारावास से दंडित किया जाएगा जो कि तीन साल तक बढ़ाया जा सकता तीन है और जुर्माना जो पांच लाख रुपये तक बढ़ाया जा सकता है और दूसरी या बाद की सजा की स्थिति में एक अवधि के लिए कारावास की सजा हो सकती है। इसे पांच साल तक बढ़ाया जा सकता है और जुर्माना भी लगाया जा सकता है, जो दस लाख रुपये तक हो सकता है।

- धारा **67**ए इलेक्ट्रॉनिक रूप में स्पष्ट यौन कृत्य आदि वाली सामग्री को प्रकाशित या प्रसारित करने के लिए सजा : जो कोई भी ऐसी सामग्री को इलेक्ट्रॉनिक रूप में प्रकाशित या प्रसारित या प्रकाशित या प्रसारित करने का कारण बनता है जिसमें स्पष्ट यौन कार्य या आचरण शामिल है, उसे प्रथम दोषसिद्धि पर एक अवधि के लिए कारावास से दंडित किया जाएगा जिसे पांच साल तक बढ़ाया जा सकता है और जुर्माना भी लगाया जा सकता है। दस लाख रुपये तक बढ़ाया जा सकता है और दूसरी या बाद की सजा की स्थिति में कारावास की सजा दी जा सकती है या तो एक अवधि के लिए विवरण जो सात साल तक बढ़ाया जा सकता है और जुर्माना भी जो दस लाख रुपये तक बढ़ाया जा सकता है।

- धारा **67**बी चाइल्ड पोर्नोग्राफी **:** इसके अंतर्गत पहली बार दोषी पाए जाने पर अपराधी को 5 साल तक की कैद और 10 लाख रुपये तक का जुर्माना और दूसरी या उसके बाद की सजा पर 7 साल तक की कैद और 10 लाख रुपये तक का जुर्माना हो सकता है।

3. साइबर स्टॉकिंग

इसके अंतर्गत पहली बार दोषी पाए जाने पर अपराधी को 3 साल तक की कैद और जुर्माना हो सकता है और दूसरी बार या उसके बाद दोषी पाए जाने पर 5 साल तक की कैद और जुर्माना हो सकता है।

4. हैकिंग और कंप्युटर वायरस

यह एक कंप्यूटर अतिक्रमण है जहां हैकर वास्तविक मालिक की अनुमति के बिना कंप्यूटर संसाधन में प्रवेश करते हैं। आईटी अधिनियम, 2000 की धारा 43 के तहत अपराध के लिए 3 साल तक की कैद या 5 लाख रुपये तक का जुर्माना या दोनों से दंडित किया जा सकता है।

5. निजता का हनन

धारा 72 गोपनीयता और निजता के उल्लंघन के लिए जुर्माना की व्यवस्था करता है। इस अधिनियम के तहत कोई भी व्यक्ति किसी व्यक्ति के इलेक्ट्रॉनिक रिकॉर्ड, पुस्तक, रजिस्टर, पत्राचार, सूचना, दस्तावेज़ या अन्य सामग्री उस संबंधित व्यक्ति की सहमति के बिना किसी अन्य व्यक्ति को प्रकट नहीं कर सकता। और यदि वह ऐसा करता हैं तो उसे दो साल तक की कैद या एक लाख तक के जुर्माने या दोनों के साथ दंडित किया जा सकता है।

बचाव के तरीके

साइबर अपराध का शिकार बनने से बचने के लिए, हम सभी को ऑनलाइन अपनी सुरक्षा और संरक्षा की जिम्मेदारी स्वीकार करने की आवश्यकता है। इसका तात्पर्य यह है कि हमे सुरक्षित ऑनलाइन सेवाओं का उपयोग करना चाहिए और उन तरीकों से अवगत रहना है जिनसे अपराधी ऑनलाइन व्यक्तिगत जानकारी प्राप्त करने का प्रयास करते हैं।

साइबर-अपराध से बचाव और रोकथाम में मदद के लिए आप कुछ व्यावहारिक चीजें कर सकते हैं जिनमे निम्न बाते शामिल हैं:

· ईमेल स्कैम से सतर्क रहना,

· अपने कंप्यूटर को साइबर-अपराध हमलों से सुरक्षित करना,

· सोशल मीडिया पर सुरक्षित रहना,

· ऑनलाइन खरीदारी करते समय सावधानी बरतना,

· अपनी व्यक्तिगत जानकारी को सुरक्षित रखना, और

· अनुपयुक्त ऑनलाइन सामग्री के संपर्क को रोकने के लिए रणनीतियाँ अपनाना इत्यादि।

निष्कर्ष

इंटरनेट हर किसी के लिए वरदान और अभिशाप दोनों ही रहा है। एक तरफ सब कुछ इतना आसान और सुविधाजनक हो गया है, और दूसरी तरफ इसने साइबर अपराधियों को स्थिति का फायदा उठाने के लिए मजबूर कर दिया है। सोशल नेटवर्किंग साइटों का उपयोग करने वाले उपयोगकर्ताओं की अत्यधिक विविधता और कई व्यक्तियों के बीच जागरूकता की कमी के कारण साइबर अपराधी सोशल मीडिया में अधिक रुचि लेने लगे हैं। हम सोशल मीडिया प्लेटफॉर्म का उपयोग करते समय थोड़ा जागरूक होकर साइबर हमले या साइबर अपराध के खतरे को कम कर सकते हैं। बहुत ही कम प्रयास से उन सोशल मीडिया प्लेटफॉर्म के आपके व्यक्तिगत डेटा की सुरक्षा सुनिश्चित करना संभव है। अपना पासवर्ड अपने किसी मित्र या सहकर्मी या यहां तक कि किसी ऑनलाइन फॉर्म पर भी साझा न करें। क्रेडिट/डेबिट कार्ड धोखाधड़ी से बचने के लिए यह भी सुझाव दिया जाता है कि इन सोशल मीडिया नेटवर्क पर अपने डेबिट या क्रेडिट कार्ड के बारे में जानकारी साझा करने से बचें।

संदर्भ ग्रंथ सूची

1. अग्रवाल, एम. (2022). साइबरक्राइम्स अगैन्स्ट विमेन इन इंडिया: अ रिव्यू ऑफ लिटरेचर. जर्नल ऑफ क्रीमीनोलॉजी एण्ड क्रिमिनल जस्टिस.
2. गॉर्डन, एस. (2006). ऑन द डेफीनिशन एण्ड क्लाससीफ़िकिशन ऑफ साइबरक्राइम.
3. अम्मार यासिर, एस. एन. (2012). साइबरक्राइम: अ थ्रेट टू नेटवर्क सिक्युरिटी. इंटरनेशनल जर्नल ऑफ कंप्युटर साइंस एण्ड नेटवर्क.
4. कुलकर्णी, जे. (2016). साइबरक्राइमस् अगैन्स्ट वीमेन इन इंडिया. उद्योग सॉफ्टवेयर.
5. चटर्जी, डी. (2017). जेन्डर एण्ड सोशल मीडिया: अ क्रिटिकल अनैलिसिस. रटलेज.
6. मेनन, एन. (2018). साइबर सेक्सिज़म इन इंडिया: डिजिटाईज़िंग मिसॉजीनी. कैंब्रिज यूनिवर्सिटी प्रेस.
7. मण्डल, एस. (2020). साइबरक्राइम अगैन्स्ट वीमेन: लॉ, एन्फोर्स्मन्ट, एण्ड जस्टिस इन इंडिया. सेज पब्लिकेशन्स.
8. दास, आर. एवं पीटर, जे. (2018). डिजिटल डिसप्शन एण्ड डेमोक्रेसी: एक्सपलोरींग द इमप्लिकेशनस् ऑफ द इंटरनेट इन इंडिया. सेज पब्लिकेशन.
9. गाइटॉनदे, आर. (2020). डिजिटल सेक्शुअल वॉइलेन्स: एन इनकंप्लीट गाइड. फेमिनिज़म इन इंडिया.
10. सिट्रॉन, डी. के. (2014). हेट क्राइमस् इन साइबरस्पेस. हार्वर्ड यूनिवर्सिटी प्रेस.