International Journal of Engineering Research & Management Technology
ISSN: 2348-4039
Jan-Feb 2018 Volume 5, Issue-1
Email: editor@ijermt.org www.ijermt.org

भारत में साइबर सुरक्षा
(Cyber Security in India)

विपिन कुमार
रिसर्च स्कालर
ओपीजेएस विश्वविद्यालय, राजस्थान

सारांश

आज के समय में साइबर सुरक्षा सबसे बड़ी आवश्यकता बनी हुये है। ऑनलाइन धोखाधड़ी, ब्लैकमेलिंग, धमकी, स्पैमिंग, भड़काने वाले कमेंट्स, हैकिंग आदि बहुत ही आम समस्याएं हो गई हैं। इससे निपटने के लिए सख्त से सख्त कदम उठाने की जरुरत है।बैंक अकाउंट्स/खातो से पैसे को एक मिनिट में एक फोन कॉल से उड़ रहे हैं, सरकार द्वारा इन सभी अपराधों से निपटने हेतु विभिन्न प्रकार के नियम बनाये जा चुके है ओर कुछ नियमों को बनाया जा रहा है, लेकिन फिर भी यह साइबरअपराध कम होते नहीं दिखाई पड रहे हैं, दिन प्रतिदिन बडते ही जा रहे हैं। भारत सरकार द्वारा घोषित निश्चित मैक इन इंडिया पहल और आने वाले महीनों और वर्षों में लगभग 5 बिलियन से अधिक डिवाइस इंटरनेट से कनेक्ट होने की रिपोर्ट के साथ, हमारे देश को ठोस साइबर सुरक्षा योजनाओं और नीतियों को तैयार करने की आवश्यकता है।

प्रस्तुत शोध पत्र में हम साइबर सुरक्षा की परिभाषा, अपराध एंवसुरक्षा के प्रकार, सुरक्षा कीचुनौतियां, साइबर सुरक्षा से जुड़े भारतीय कानून और साइबर सुरक्षा के सुदृढ़ता हेतु उठाए गए कदमो पर चर्चा करेंगे।

कुंजी शब्दः साइबर सुरक्षा,साइबर अपराध,चाइल्ड पोर्नोग्राफी,साइबर आतंकवाद।

अनुसांधान क्रिया विधि एवं अध्ययन की आवश्यकता :

प्रस्तुत लेख द्वितीयक आंकड़ों पर आधारित है। लेख को लिखने के लिए न्यूज पेपर लेखों, पत्रिकाओं, इंटरनेट वेबसाइटों आदि से सहायता प्राप्त की गयी है।

अध्ययन का उद्देश्यः—शोध का उद्देश्य साइबर क्राईम के माध्यम से होने वाले अपराधों के बारे में जागरुक करना ओर साइबर अपराधों के मामलों में भारतीयों पर इसका क्या प्रभाव पड राह है। साइबर अपराध या कम्प्यूटर अपराध, इन्टरनेट द्वारा किया जाता है। यूजर के लिए साइबर क्राइम बहुत ही जाना पहचाना नाम है, साइबर क्राईम किस तरह से किसी के भी जीवन में परेशानियाँ बढ़ा देता है। शोध के माध्यम बताया गया है, कि व्यक्ति को अपने व्यक्तिफगत जानकारी को कैसे सुाक्षित करें। ओरकसे इस अपराध से निपटा जा सके। साइबर हमलों की बढ़ती मात्रा और जटिलता के साथ, संवेदनशील व्यवसाय और व्यक्तिगत जानकारी की सुरक्षा के साथ—साथ राष्ट्रीय सुरक्षा की रक्षा के लिए अधिक ध्यान देने की आवश्यकता है।

संकेत सूची

- प्रस्तावना

- साइबर सुरक्षा की परिभाषा।
- साइबर सुरक्षा की जरूरत क्यों है।
- साइबर अपराधके प्रकार।
- साइबर सुरक्षा में सामने आ रही चुनौतियां हैं।
- साइबर सुरक्षा से सम्बधित भारतीय कानूनं।
- साइबर सुरक्षा के सुदृढ़ता हेतु भारत सरकार के कदम।
- सूचना तकनीक कानून, 2000 के अंतर्गत साइबरस्पेस में क्षेत्राधिकार संबंधी प्रावधान।
- भारतीय दण्ड संहिता (आईपीसी) में साइबर अपराधों से संबंधित प्रावधान।
- सइबर अपराध से बचने के लिए समान्य सुझाव।
- भारत में साइबर सुरक्षा को बेहतर बनाने हेतु सुझाव।
- उपसंहार।

प्रस्तावना/परिचयः

एकदेश/राज्य को चार प्रकार के खतरों से खतरा हो सकता जो निम्न प्रकार हैः–

- आंतरिक
- बाहरी
- आंतरिक रूप से सहायता प्राप्त बाहरी
- बाहरी सहायता प्राप्त आंतरिक

भारत की आंतरिक सुरक्षा खतरे की धारणा के ऊपर परिभाषित खतरों के सभी चार प्रकार का मिश्रण है, बदलते बाहरी परिवेश का असर हमारी आंतरिक सुरक्षा पर भी पड़ता है। श्रीलंका, पाकिस्तान, बांग्लादेश, नेपाल और म्यांमार की घटनाओं का हमारी आंतरिक सुरक्षा से प्रत्यक्ष या अप्रत्यक्ष संबंध है।

2013 में स्नोडेन खुलासे (विकीलीक्स) ने यह स्पष्ट कर दिया था कि भविष्य के युद्ध पारंपरिक युद्ध नहीं होंगे जो जल, थल और वायु पर लड़े जाते हैं। क्योंकि आज 21वीं सदी में हर देश अपने दुश्मन देश पर हैकिंग या अन्य प्रकार के साइबर हमले कर रहा है,ये अत्यंत ही खतरनाक हमले होते है क्योंकि अन्य प्रकार के हमले के लिए तो सेना है लेकिन क्या साइबर हमलों से निपटने में हमारा देश अभी सशक्त है।

साइबर सुरक्षा की परिभाषाः

साइबर सुरक्षा तकनीकी शब्द है, सूचना सुरक्षा से भी जुड़ी है, जिसे संघीय कानून में अखंडता, गोपनीयता और उपलब्धता प्रदान करने के लिए अवैध पहुंच, उपयोग, प्रकटीकरण, व्यवधान, संशोधन या क्षति से सूचना और सूचना प्रणाली की रक्षा के रूप में समझाया गया है। साइबर सुरक्षा कंप्यूटर, नेटवर्क, प्रोग्राम और डेटा को अनपेक्षित या अनधिकृत पहुंच, परिवर्तन या विनाश से बचाने पर केंद्रित है। साइबर हमलों की बढ़ती मात्रा और जटिलता के साथ, संवेदनशील व्यवसाय और व्यक्तिगत जानकारी की सुरक्षा के साथ–साथ राष्ट्रीय सुरक्षा की रक्षा के लिए अधिक ध्यान देने की आवश्यकता है।

साइबर अपराध इंटरनेट, कंप्यूटर या किसी अन्य परस्पर जुड़े बुनियादी ढांचे सहित आपराधिक गतिविधि को दर्शाता है।

साइबर अपराध कितने प्रकार के होते हैंः

वह शब्द जिसमें फिशिंग, क्रेडिट कार्ड धोखाधड़ी, अवैध डाउनलोडिंग, औद्योगिक जासूसी, चाइल्ड पोर्नोग्राफी, घोटाले, साइबर आतंकवाद, वायरस का निर्माण औरध्या वितरण, स्पैम आदि जैसे अपराध शामिल हैं, वह सब साइबर अपराध है।

हमारे देश भारतमें निम्नलिखित प्रकार के साइबर अपराध होते हैं।

साइबर स्टॉकिंग

साइबर स्टॉकिंगको ऐंसे परिभाषित किया गया है जो अक्सर व्यक्तियों के निजी जीवन में गुप्त रूप से नजर रखके संकट, चिंता और भय पैदा करने के लिए किया जाता है।

साइबर स्टॉकिंग व्यक्ति को मनोवैज्ञानिक रूप से परेशान करती है इसलिए इसे कभी–कभी "मनोवैज्ञानिक बलात्कार" या "मनोवैज्ञानिक आतंकवाद" भी कहा जाता है।

बौद्धिक संपदा की चोरी

बौद्धिक संपदा को एक नवाचार, नए शोध, पद्धति, मॉडल और सूत्र के रूप में परिभाषित किया गया है जिसका आर्थिक अर्थ है। बौद्धिक संपदा पेटेंट और ट्रेडमार्क होने के साथ–साथ वीडियो और संगीत पर कॉपीराइट के साथ सुरक्षित है। जब कोई व्यक्ति इस कॉपीराइट वाले डेटा को चुरा लेता है या विभिन्न पद्धतियों का प्रयोग करके इस कॉपीराइट वाले डेटा को अपने नाम से पेटेंट करवा लेता है तो वह बौद्धिक संपदा की चोरी कहलाती हैं।

सलामी अटैक

सलामी अटैक में साइबर अपराधी और हमलावर एक बड़ी रकम पाने के लिए कई बैंक खातों से छोटी –छोटी रकम में पैसे चुराते हैं। जिससे छोटी रकम चोरी होने पर कोई शिकायत भी नही करता ओर ना ही किसी से शेयर करना चाहता है।

ई–मेल बमबारी

ई–मेल बमबारी, साइबर हमले में अपराधी एक व्यक्ति को भारी मात्रा में ई–मेल भेज कर पैसे, ब्लैकमेलिंग, लालच देकर किसी विशेष संदिग्ध लिंक में क्लिक करने को बोलेंगे जब वह व्यक्ति लिंक में क्लिक करेगा तो वह उसके अकाउंट से पैसे निकल जाएंगे। इस प्रकार की ऑनलाईन चोरी ई–मेल बमबारी के तहत आती है।

फिशिंग

एक प्रकार का कपटपूर्ण प्रयास है जो किसी व्यक्तिगत और वित्तीय जानकारी हासिल करने के लिए ईमेल के माध्यम से किया जाता है। अपराधी ई–मेल भेजता है जो जाने–माने और भरोसेमंद पते से आता है और आपकी वित्तीय जानकारी जैसे बैंक का नाम, क्रेडिट कार्ड नंबर, खाता संख्या या पासवर्ड वन टाइम पासवर्ड (OTP)मांगता है। फिशिंग प्रयासों करने वालो के लिए यह आम बात होती है कि ई–मेल उन साइटों और कंपनियों से आते हैं जिनके पास बैंक खाता भी नहीं है।

पहचान की चोरी

पहचान की चोरी एक प्रकार की धोखाधड़ी होती है जिसमें व्यक्ति किसी और के होने का दिखावा करता है और किसी दुसरे के नाम से अपराध करता है। अपराधी किसी व्यक्ति का रूप धारण करने के लिए नाम, पता, क्रेडिट कार्ड नंबर, बैंक खाता संख्या जैसी महत्वपूर्ण जानकारी चुराता है और उसके नाम पर अपराध करता है।

स्पूफिंग

एक ऐसी तकनीक को होती है जिसमें कंप्यूटर तक अनधिकृत पहुंच होती है, जिससे अपराधी एक आईपी एड्रेस के साथ नेटवर्क वाले कंप्यूटर पर संदेश भेजता है। प्राप्तकर्ता को ऐसा लगता है कि संदेशों को एक भरोसेमंद स्रोत से प्रेषित किया जा रहा है।

वाइरस

कंप्यूटर वायरस तभी प्रभावी/एकटीव होता है जब वह किसी भी प्रकार के प्रोग्राम या निष्पादन योग्य फाइलों से जुड़ जाता है। वायरस के जुडने के बाद जब सहायक फाइलों को चलाते हैं तो वायरस अपना संक्रमण छोड़ देता है।

ट्रोजेन हॉर्सेज

ट्रोजन हॉर्स, एक बार में उपयोगी सॉफ्टवेयर के रूप में लगता है लेकिन वास्तव में कंप्यूटर और उसके सॉफ्टवेयर को नुकसान पहुंचाता है क्योंकि यह कम्यूटर में इंस्टॉल हो जाता है। कुछ ट्रोजन हॉर्सेज को साइबर अपराधी उपयोगकर्ताओं के कंप्यूटर को दूर से ही नियंत्रित करने के लिए एक तरह के पिछले दरवाजे (Back Door)का निर्माण करते हैं, जिससे गोपनीय और व्यक्तिगत जानकारी की चोरी हो जाती है।

पोर्नोग्राफी

पोर्नोग्राफी एक प्रकार का साइबर अपराध से जुडा होता है जिसमे उत्तेजक फोटो और वीडियो को लोकप्रिय सोशल मीडिया के माध्यम से फैलाया जाता है।

साइबर सुरक्षा की जरूरत क्यों है

हमें साइबर सुरक्षा की जरूरत जिंदगी के प्रत्येक क्षेत्र में पड़ती है। साइबर सुरक्षा की आवश्यकताओं को निम्न बिंदुओं में समझते हैं।

- सोशल नेटवर्किंग साइट्स पर किसी व्यक्ति द्वारा साझा की गई तस्वीरें, वीडियो और अन्य व्यक्तिगत जानकारी दूसरों द्वारा अनुपयुक्त रूप से उपयोग की जा सकती है, जिससे गंभीर और यहां तक कि जान माल की घटनाएं भी हो सकती हैं।

- भारत की केंद्र सरकार या राज्य सरकार (भौगोलिक, सैन्य रणनीतिक संपत्ति आदि) और नागरिकों से संबंधित बड़ी मात्रा में गोपनीय डेटा रखती है। ग्राहकों और जनता के डेटा तक अनधिकृत पहुंच से किसी देश की प्राइवेसी और सुरक्षा पर गंभीर खतरा हो सकता है।

- किसी व्यापार के लिएः कंपनियों के पास अपने सिस्टम पर बहुत सारा डेटा और जानकारी होती है। साइबर हमले से प्रतिस्पर्धी जानकारी (जैसे पेटेंट या मूल कार्य) का नुकसान हो सकता है, कर्मचारियों और ग्राहकों का निजी डेटा चोरी हो सकता है जिससे किसी विशेष संगठन अथवा एजेंसी की प्राइवेसी पर जनता का विश्वास पूरी तरह से समाप्त हो सकता है।

साइबर सुरक्षा की क्या चुनौतियां है

भारत जैसे बड़े और विकासशील देश में साइबर सुरक्षा को लेकर निम्नलिखित चुनौतियां सामने आ रही हैं।

- **खराब साइबर सुरक्षा अवसंरचनाः** भारत के बहुत कम शहरों में साइबर अपराध सेल्स हैं और भारत में समर्पित साइबर न्यायालयों की संख्या भी कम है।

- **जागरूकता की कमी:** कम जागरूक होने के कारण और उत्पीड़न के डर से लोग साइबर अपराधों की रिपोर्ट नहीं करते हैं। अधिकांश भारतीय डेटा भारत के बाहर स्थित डेटा केंद्रों में संग्रहीत किया जाता है। इसलिए, डेटा स्टोर करने वाली कंपनियां भारत को साइबर हमले की सूचना नहीं देती हैं। बढ़ते ऑनलाइन लेनदेन ने साइबर अपराधियों के लिए बड़ा प्रोत्साहन दिया है।

- **अधिकारियों में साइबर कौशल और प्रशिक्षण की कमी:** जिन कानून प्रवर्तन एजेंसियों को साइबर जांच करने की आवश्यकता होती है, उनमें अक्सर अपेक्षित साइबर कौशल और प्रशिक्षण की कमी होती है।

- **गुमनामी:** साइबरस्पेस व्यक्तियों को एन्क्रिप्टिंग टूल का उपयोग करके किसी की प्रोफाइल को छिपाने या गलत तरीके से प्रस्तुत करने की अनुमति देता है। इस प्रकार की जांच के दौरान बड़ी चुनौतीया पैदा होती है।

- **पुरानी रणनीतियाँ:** भारत की राष्ट्रीय साइबर सुरक्षा रणनीति, जिसे एनएससी द्वारा मसौदा तैयार किया गया है राष्ट्रीय साइबर सुरक्षा नीति 2013 के लिए एक बहुत जरूरी अद्यतन अभी तक जारी नहीं हो पाया है।

- **विश्वसनीय साइबर प्रतिरोध रणनीति का अभाव:** एक विश्वसनीय साइबर प्रतिरोध रणनीति की अनुपस्थिति का मतलब है कि राज्यों और केंद्रशासित प्रदेशो को समान रूप से विभिन्न उद्देश्यों की पूर्ति के लिए एक परंपरागत निम्न–स्तरीय साइबर नियम का संचालन करने के लिए निर्देशित किया जाता है।

- **साइबर संघर्ष से निपटने के लिए अनुचित दृष्टिकोण:** भारत में अभी तक किसी भी एक सिद्धांत को स्पष्ट रूप से स्पष्ट नहीं गया है जो साइबर संघर्ष के लिए अपने दृष्टिकोण को समग्र रूप से प्रदर्शित करता हो।

साइबर सुरक्षा से जुड़े भारतीय कानून

भारत सरकार ने अभी कुछ वर्षों से साइबर अपराधों की ओर ध्यान देना शुरु किया है और निम्नलिखित कानून बनाए हैं।

- **साइबर सुरक्षा नीति:** राष्ट्रीय साइबर सुरक्षा नीति, 2013 को भारत के नागरिकों और व्यापरीयों के लिए सुरक्षित और लचीला साइबर स्पेस बनाने के लिए विकसित किया गया था।

- **आईटी अधिनियम, 2000:** वर्तमान में, सूचना अधिनियम, 2000 देश में साइबर अपराध और डिजिटल वाणिज्य से निपटने के लिए प्राथमिक कानून है।

- **भारतीय साइबर अपराध समन्वय केंद्र Indian Cybercrime Coordination Centre(I4C):** केंद्र सरकार ने देश में साइबर अपराध से संबंधित मुद्दों को व्यापक और समन्वित तरीके से संभालने के लिए भारतीय साइबर अपराध समन्वय केंद्र Indian Cybercrime Coordination Centre (I4C) की स्थापना के लिए एक योजना शुरू की है।

- **महिलाओं और बच्चों के लिये साइबर अपराध निवारण योजना:** यह योजना ऑनलाइन उत्पीड़न के खिलाफ शिकायतों के लिए ऑनलाइन पोर्टल स्थापित करने, एकत्र किए गए सबूतों को देखने और संरक्षित करने के लिए फोरेंसिक इकाइयों की स्थापना, कानून लागू करने वाले अधिकारियों की क्षमता निर्माण, साइबर स्पेस से अश्लील सामग्री को हटाने के लिए उपकरणों के अनुसंधान और विकास की अनुमति देती है और जनता को जागरूक करती है।

भारत सरकार के साइबर सुरक्षा के सुदृढ़ता हेतु कदम

भारत सरकार ने साइबर सुरक्षा से निपटने हेतु निम्नलिखित कदम उठाए हैं।

साइबर क्राइम वालंटियर्स

भारत सरकार के गृह मंत्रालय के तहत भारतीय साइबर अपराध समन्वय केंद्र Indian Cybercrime Coordination Centre(I4C) ने नागरिकों को "साइबर अपराध स्वयंसेवकों" के रूप में पंजीकृत करने की अनुमति देने के उद्देश्य से साइबर अपराध स्वयंसेवक कार्यक्रम शुरू किया।

साइबर क्राइम रिपोर्टिंग पोर्टल

भारत सरकार ने ऑनलाइन साइबर अपराध रिपोर्टिंग पोर्टल, cybercrime.gov.in लॉन्च किया ताकि शिकायतकर्ता बाल पोर्नोग्राफी/बाल यौन शोषण सामग्री, बलात्कार/सामूहिक बलात्कार छवियों, या यौन स्पष्ट सामग्री से संबंधित शिकायतों की रिपोर्ट कर सकें। साइबर क्राइम हेल्पलाइन नंबर 1930 है।

साइबर स्वच्छता केंद्र

कार्यक्रमों का पता लगाने और ऐसे कार्यक्रमों को हटाने के लिए मुफ्त उपकरण प्रदान करने के लिए साइबर स्वच्छता केंद्र (बॉटनेट सफाई और मैलवेयर विश्लेषण केंद्र) शुरू किया गया।

राष्ट्रीय साइबर समन्वय केंद्र (एनसीसीसी)

यह देश में आने वाले इंटरनेट यातायात को स्कैन करने और वास्तविक समय स्थितिजन्य जागरूकता प्रदान करने और विभिन्न सुरक्षा एजेंसियों को सतर्क करता है।

साइबर और सूचना सुरक्षा (सीआईएस) डिवीजन

साइबर खतरों, चाइल्ड पोर्नोग्राफी और ऑनलाइन स्टाकिंग जैसे इंटरनेट अपराधों से निपटने के लिए एक नया कानुन बनाया गया है।

भारत में साइबर सुरक्षित पहल

साइबर सुरक्षित भारत पहलकी शुरुआत भारत में साइबर सुरक्षा पारिस्थिति के तंत्र को मजबूत करने के लिए की गई है। यह इस तरह की पहली सार्वजनिक निजी भागीदारी है और साइबर सुरक्षा के लिये भारत की आईटी कंपनी सहयोग दे रही है।

सूचना तकनीक कानून, 2000 के अंतर्गत साइबरस्पेस में क्षेत्राधिकार संबंधी प्रावधान

मानव समाज के विकास के लिए सूचना और संचार तकनीकों की खोज को बीसवीं शताब्दी का सबसे महत्वपूर्ण अविष्कार माना जा सकता है। सामाजिक विकास के विभिन्न क्षेत्रों, खासकर न्यायिक प्रक्रिया में इसके इस्तेमाल की महत्ता को कम करके नहीं माना जा सकता, क्योंकि इसकी तेज गति, बहुत सारी छोटी–मोटी दक्कितों से छुटकारा, मानवीय गलतियों की कमी, कम खर्चीला होना जैसे गुणों के चलते यह न्यायिक प्रक्रिया को विश्वसनीय बनाने में अहम भूमिका निभा सकती है। इतना ही नहीं, ऐसे मामलों के निष्पादन में, जहां सभी संबद्ध पक्षों की शारीरिक उपस्थिति अनिवार्य न हो, यह सर्वश्रेष्ठ विकल्प सिद्ध हो सकता है।

सूचना तकनीक कानून के अंतर्गत उल्लिखित आरोपों की सूची निम्नवत है:

1. कंप्यूटर संसाधनों से छेड़छाड़ की कोशिश–धारा 65

2. कंप्यूटर में संग्रहित डाटा के साथ छेड़छाड़ कर उसे हैक करने की कोशिश–धारा 66
3. संवाद सेवाओं के माध्यम से प्रतिबंधित सूचनाएं भेजने के लिए दंड का प्रावधान–धारा 66 ए
4. कंप्यूटर या अन्य किसी इलेक्ट्रॉनिक गैजेट से चोरी की गई सूचनाओं को गलत तरीके से हासिल करना–धारा 66 बी
5. किसी की पहचान चोरी करना–धारा 66 सी
6. अपनी पहचान छुपाकर कंप्यूटर की मदद से किसी के व्यक्तिगत डाटा तक पहुंचाना–धारा 66 डी
7. किसी की निजता भंग करना–धारा 66 इ
8. साइबर आतंकवाद के लिए दंड का प्रावधान–धारा 66 एफ
9. आपत्तिजनक सूचनाओं के प्रकाशन से जुड़े मामले–धारा 67
10. इलेक्ट्रॉनिक माध्यमों से सेक्स/ अश्लील सूचनाओं को प्रकाशित या प्रसारित करना–धारा 67 ए
11. इलेक्ट्रॉनिक माध्यमों से ऐसी आपत्तिजनक सामग्री का प्रकाशन या प्रसारण, जिसमें बच्चों को अश्लील अवस्था में दिखाया गया हो–धारा 67 बी
12. मध्यस्थों द्वारा सूचनाओं को बाधित करने या रोकने के लिए दंड का प्रावधान–धारा 67 सी
13. सुरक्षित कंप्यूटर तक अनाधिकार पहुंच बनाने से संबंधित प्रावधान–धारा 70
14. डाटा या आंकड़ों को गलत तरीकों से पेश करना–धारा 71
15. आपसी विश्वास और निजता को भंग करने से संबंधित प्रावधान–धारा 72 ए
16. कॉन्ट्रैक्ट की शर्तों का उल्लंघन कर सूचनाओं को सार्वजनिक करने से संबंधित प्रावधान–धारा 72 ए
17. फर्जी डिजिटल हस्ताक्षर का प्रकाशन–धारा 73

भारतीय दण्ड संहिता (आईपीसी) में साइबर अपराधों से संबंधित प्रावधान।

1. ईमेल के माध्यम से धमकी भरे संदेश भेजना–आईपीसी की धारा हो–आईपीसी की धारा 499
2. फर्जी इलेक्ट्रॉनिक रिकॉर्ड्स का इस्तेमाल–आईपीसी की धारा 463
3. फर्जी वेबसाइट्स या साइबर फ्रॉड–आईपीसी की धारा 420
4. चोरी–छुपे किसी के ईमेल पर नजर रखना–आईपीसी की धारा 463
5. वेब जैकिंग–आईपीसी की धारा 383
6. ईमेल का गलत इस्तेमाल–आईपीसी की धारा 500

सइबर अपराध से बचने हेतु समान्य सुझाव।

1. व्यक्तिगत/वित्तीय जानकारी चाहने वाले अज्ञात स्रोत से प्राप्त संदेश का जवाब न दें, चाहे वह आपको कितना भी फोंस करें या आपके बैंक खाते में धन जमा करने का कथन करते हों।
2. संदिग्ध ई–मेल का जवाब न दें और न ही संदिग्ध लिंक पर क्लिक करें।
3. अविश्वसनीय अज्ञात बैंक खाते में कभी भी रूपए अंतरित न करें।
4. लॉटरी से सम्बधित कथन के लिए ध्यान रहे कि आप तब तक लॉटरी नहीं जीत सकते है, जब तक कि आपने लॉटरीप्रक्रिया में भाग ना लिया हो।
5. ई–मेल खाते में स्पैम फिल्टर को इनेबल रखें।
6. अगर आपके पास कोई कॉल आता है कि आपका कार्ड ब्लॉक कर दिया गया है तोभ्रमित न हों। बैंक ऐसी सूचना कभी भी फोन के द्वारा नहीं देते हैं। किसी अजनबी से अपना पिन, पासवर्ड, कार्ड नंबर, सीवीवी नंबर, ओटीपी आदि साझा न करें, भले ही वह बैंक कर्मचारी होने का दावा करे। बैंक कमी भी ऐसीमहत्त्वपूर्ण सूचना नहीं मांगता है। बैंको द्वारा भी समय समय पर सन्देस भेजकर सचेत किया जा रहा है।

7. अपने बैंक के कस्टमर केयर नंबर को सुरक्षित रखें ताकि आपके खाते के किसीसंदिग्ध अथवा अनधिकृत लेन–देन की सूचना तुरन्त बैंक को दी जा सके।
8. हमेशा समाचार पत्रों में प्रकाशित नौकरियों के लिए हीआवेदन करने हेतु अधिकरित पोर्टल,समाचार पात्रों से प्राप्त जानकारी का प्रयोग करें।
9. खाते को लॉग आउट किए बिना ब्राउजर विंडो को बंद न करें।
10. यदि आप किसी अन्य के कम्प्यूटर का उपयोग करते हैंतो दो चरणीय सत्यापन जैसे– वन–टाइम पासवर्ड (ओटीपी) का उपयोग करें।
11. वेब ब्राउजर पर उपयोगकर्ता पहचान (User ID) और पासवर्ड सेव न करें।
12. अज्ञात व्यक्ति/संस्था/कंपनी को अपने पहचान प्रमाणों जैसे– आधार कार्ड, पैन कार्ड, वोटर कार्ड, ड्राईविंग लाइसेन्स आदि का विवरण या प्रतिलिपि कभी न दें।
13. पहचान प्रमाण की फोटो प्रति संस्था/कंपनी में जब भी उस पर देने का उद्देश्य लिखें, ताकि उसका पुनः उपयोग नहीं किया जा सके।
14. अपने क्रेडिट, डेबिट या एटीएम कार्ड की रसीदों को बैंक/एटीएम या स्टोरमें ना छोड़ें और ना ही सार्वजनिक स्थानों पर फेंके।हमेशा यह सुनिश्चित करें कि आपका क्रेडिट या डेबिट कार्ड शॉपिंग मॉल, पैट्रोल पंपों पर आपकी उपस्थिति में स्वाइप किया जाए विक्रेता को अपना कार्ड स्वाइप करने के लिए दूर ले जाने की अनुमति न दें।

भारत में साइबरसुरक्षा को बेहतर बनाने हेतुसुझाव

भारत में साइबर सुरक्षा को और बेहतर बनाने के लिए कुछ कदम उठाये जाने की आवश्यकता है।

कानून प्रवर्तन एजेंसियों का मजबूत प्रशिक्षण समय की मांग है।

सरकार को साइबर सुरक्षा और सुरक्षित इंटरनेट हैंडलिंग तकनीकों पर विशेष ध्यान देने वाली कानून प्रवर्तन एजेंसियों और व्यक्तियों को निरंतर, मजबूत और प्रभावी प्रशिक्षण प्रदान करना होगा।

बुनियादी ढांचे का विकास

इसमें अधिक साइबर सेल, साइबर कोर्ट और साइबर फोरेंसिक लैब बनाना शामिल होगा ताकि उल्लंघन करने वालों को विधिवत दंडित किया जाये।

डिजिटल साक्षरता पैदा करना

यह साइबर अपराधों के प्रति आमजनता में जागरुकता की कमजोरियों को दूर करके किया जा सकता है।

सेवा प्रदाताओं पर जिम्मेदारी

वेबसाइट के मालिकों को अपनी साइट पर ट्रैफिक के प्रति अधिक सतर्क रहना चाहिए और किसी भी अनियमितता की रिपोर्ट करनी चाहिए। यह साइबर हमलों पर बड़े पैमाने पर डेटा संग्रह सुनिश्चित करेगा। इन डेटा का उपयोग भविष्य में एक नई साइबर सुरक्षा रणनीति बनाने के लिए किया जा सकता है।

सूचना प्रौद्योगिकी अधिनियम में संशोधन

नियमित साइबर सुरक्षा ऑडिट करने के लिए कंपनियों पर कानूनी जिम्मेदारी डालने की आवश्यकता है।

उसके लिए, स्वतंत्र एजेंसियों द्वारा अनिवार्य साइबर सुरक्षा ऑडिट को शामिल करने के लिए आईटी अधिनियम में संशोधन किया जा सकता है जैसा कि अभी पिछले साल 2021 में हुआ था लेकिन अभी इससे भी अधिक कठोर नियम की जरूरत है।

निष्कर्ष

हम सभी सक्रिय रूप से लड़ रहे हैं और अपने नेटवर्क और सूचनाओं की सुरक्षा के लिए विभिन्न ढांचे या प्रौद्योगिकियों को प्रस्तुत कर रहे हैं लेकिन ये सभी केवल अल्पावधि के लिए सुरक्षा प्रदान करते हैं। हालांकि, बेहतर सुरक्षा समझ और उपयुक्त रणनीतियां हमें बौद्धिक संपदा और व्यापार रहस्यों की रक्षा करने और वित्तीय और प्रतिष्ठा के नुकसान को कम करने में मदद कर सकती हैं। केंद्रऔर राज्य सरकारों द्वारा बड़ी मात्रा में डेटा और गोपनीय रिकॉर्ड डिजिटल रूप में ऑनलाइन रखती हैं जो साइबर हमले का प्राथमिक लक्ष्य बन जाता है। अनुचित बुनियादी ढांचे, जागरूकता की कमी और पर्याप्त धन के कारण अधिकांश समय सरकारों को कठिनाइयों का सामना करना पड़ता है।

सरकारी निकायों/एजनसियों के लिए यह महत्वपूर्ण है कि वे समाज को विश्वसनीय सेवाएं प्रदान करें, स्वस्थ नागरिक–से–सरकार संचार बनाए रखें और गोपनीय जानकारी की सुरक्षा करें।

संदर्भ सूचीः–

1. https://link.springer.com/book/10.1007/978-981-15-1675-7#bibliographic-information
2. https://d19k0hz679a7ts.cloudfront.net/value_added_material/Security-Sep19-Sep20-Hindi.pdf
3. https://www.latestcarernews.com/cyber-security-pdf/
4. https://rlsa.gov.in/publication/Cyber%20Crime%20and%20Cyber%20Security%20Booklet.pdf
5. https://www.amarujala.com/technology/tech-diary/cyber-crime-cases-increased-in-india-by-five-percent-in-2021-govt-data
6. https://cybercrime.gov.in/Hindi/Defaulthn.aspx
7. https://www.aajtak.in/crime/cyber-crime
8. https://www.tv9hindi.com/india/cyber-crime-increased-in-india-cases-recorded-a-five-fold-jump-in-last-three-years-says-government-1161687.html
9. https://www.jagran.com/technology/tech-news-cyber-crime-11-percent-jump-in-2020-in-india-according-ncrb-data-22457752.html
10. https://www.crpfindia.com/cyber-crime-in-hindi/
11. https://zeenews.india.com/hindi/business/cyber-crime-government-website-banking-fraud-tollfree-number/1310778
12. https://hi.wikipedia.org/wiki/
13. https://www.cybercrime.gov.in/Webform/Helpline.aspx