P: ISSN NO.: 2321-290X RNI : UPBIL/2013/55327 VOL-IV* ISSUE-III*November-2016
E: ISSN NO.: 2349-980X **Shrinkhla Ek Shodhparak Vaicharik Patrika**

भारत में साइबर अपराध : एक विश्लेषण

श्रमवीर सिंह कुशवाह
वरिष्ठ प्रवक्ता,
समाजशास्त्र विभाग,
आर0 बी0एस0 कॉलेज,
आगरा

सारांश

विगत वर्षों में भारत ने सूचना प्रौद्योगिकी के क्षेत्र में बहुत उन्नति की है। इसके साथ ही अपराधों में भी वृद्धि हुई है। साइबर अपराध भी आधुनिक प्रकार का अपराध है। वर्तमान में भारत में कई प्रकार के साइबर अपराध पाये जाते हैं। क्रेडिट कार्ड फ्रॉड, दस्तावेजों में हेरफेर, ई–मेल थ्रेट, पासवर्ड चोरी, वायरस, हैकिंग, सॉफ्टवेयर पायरेसी, साइबर स्टाकिंग, पोर्नोग्राफी, साइबर गेम्बलिंग, फिशिंग, डाटा डिडलिंग, सलामी अटैक, साइबर आतंकवाद जैसे कई अपराध आम हैं। सरकार ने इन साइबर अपराधों पर नियंत्रण करने के लिये सूचना प्रौद्योगिक अधिनियम 2000 एवं अन्य कानून बनाये हैं। वर्तमान में साइबर अपराधों के आँकड़ों को नेशनल क्राइम रिकॉर्ड ब्यूरो एकत्रित करता है। साइबर अपराधों को कानून के साथ स्वयं की जागरूकता एवं ज्ञान से रोका जा सकता है।

मुख्य शब्द : अपराध, साइबर अपराध, सूचना प्रौद्योगिकी, इंटरनेट, कम्प्यूटर, क्रेडिट कार्ड, हैकिंग, पायरेसी, पोर्नोग्राफी, ई–मेल, पासवर्ड

प्रस्तावना

समाज सामाजिक संबंधों से निर्मित व्यवस्था है। समाज में व्यवस्था बनी रहे ऐसा प्रयास सदैव से समाज करता रहा है। लेकिन फिर भी सामाजिक व्यवस्था को सदैव से चुनौतियों का सामना करना पड़ता रहा है। अपराध भी एक चुनौती है। कोई भी समाज इससे अछूता नहीं है। न्यूनाधिक सभी समाजों में अपराध पाया जाता है। समय के साथ अपराधों के स्वरूपों में परिवर्तन आता रहा है। सामाजिक उद्विकास के साथ–साथ नए–नए तरीके के आपराधिक कृत्य सामने आते रहे हैं। वर्तमान युग सूचना प्रौद्योगिकी का युग है। सूचना–प्रौद्योगिकी मानव विकास के रास्ते में एक बहुत बड़ी सहायिका के रूप में कार्यरत है। इसके अनेक लाभ स्पष्ट दिखाई दे रहे हैं। परन्तु कुछ लोगों ने गैरकानूनी तरीके से इसका दुरुपयोग करना शुरू कर दिया है। सूचना–प्रौद्योगिकी का उपयोग कर अनेक प्रकार के अपराधों को कारित किया जा रहा है। सूचना–प्रौद्योगिकी का दुरुपयोग कर अपराधों को कारित करना ही साइबर अपराध है।

उद्देश्य

भारत में साइबर अपराधों का विश्लेषण करना।

साइबर अपराध की अवधारणा

सूचना प्रौद्योगिकी, संचार क्रांति एवं वैश्वीकरण के इस युग में जहाँ एक ओर समाज में जागरूकता में वृद्धि हुई है एवं विभिन्न देशों के बीच दूरी घटी है वहीं अनेक प्रकार के अपराधों ने भी जन्म लिया। साइबर अपराध भी उनमें से एक है।[1] इंटरनेट शब्द इंटरनेशनल नेटवर्किंग का ही संक्षिप्त रूप है। यह कम्प्यूटरों का विश्वव्यापी जाल है जो विभिन्न संचार माध्यमों द्वारा जुड़कर सूचनाओं का आदान–प्रदान करता है। प्रो0 जे0सी0 लिक्लाइडर को इंटरनेट का जनक माना जाता है। इंटरनेट की शुरूआत 1969 में अमेरिकन रक्षा विभाग द्वारा 'एडवांस्ड रिसर्च प्रोजेक्ट एजेंसी नेट' के विकास के लिए किया गया। 1989 में इंटरनेट को सामान्य जनता के लिए खोल दिये जाने के कारण इसमें व्यापकता आयी। वर्ष 1990 में टिम बर्नर ली द्वारा 'वर्ल्ड वाइड वेब' के आविष्कार ने इंटरनेट को नई दिशा एवं आयाम दिये हैं।[2] सूचना प्रौद्योगिकी के तीव्र विकास ने न केवल दुनिया को एक वैश्विक ग्राम का रूप प्रदान किया बल्कि आम आदमी को भी गतिशील बना दिया है।[3]

विज्ञान गल्प लिखने वाले विलियम गिब्सन ने वर्ष 1948 में अपनी पुस्तक 'न्यूरान एन्सर' में साइबर स्पेस शब्द का प्रयोग किया। जिसमें इसका अर्थ छवियों के कम्प्यूटर द्वारा उसका त्रि–आयामी रेखाचित्र के रूप में वर्णन से है। लेकिन वर्तमान में इसके मायने बदल गये हैं। आज साइबर स्पेस का अर्थ इंटरनेट के रूप में समझे जाने वाले अंर्तसम्बन्धी वैश्विक कम्प्यूटर तंत्र से है।[4]

साइबर क्राइम का अर्थ कम्प्यूटर जनित अपराध से लिया जाता है। संयुक्त राष्ट्र के कम्प्यूटर क्राइम कंट्रोल एवं प्रिवेंशन मेनुअल के अनुसार जालसाजी, ठगी और अनाधिकृत प्रवेश को साइबर अपराध के अन्तर्गत परिभाषित करते हैं। यह वह अवैधानिक कार्य है जिसमें कम्प्यूटर या तो औज़ार की तरह या लक्ष्य की तरह प्रयोग होता है अथवा दोनों ही तरीके से प्रयुक्त हो सकता है।[5] वेवोपीडिया कम्प्यूटर डिक्शनरी के अनुसार साइबर अपराध कम्प्यूटर तथा नेटवर्क से संबंधित कोई भी आपराधिक कृत्य है। साथ ही इसमें इन्टरनेट द्वारा संचालित परम्परागत अपराध आते हैं। उदाहरण के लिए घृणाकारी अपराध, टेलीमार्केटिंग एवं इन्टरनेट फ्रॉड, पहचान चोरी, क्रेडिट कार्ड एकाउण्ट चोरी भी साइबर अपराध माने जाते हैं, यदि अवैध क्रियाकलाप कम्प्यूटर एवं इन्टरनेट के प्रयोग द्वारा सम्पन्न किए गए हों।[6]

सैद्धांतिक रूप से साइबर अपराध को तीन श्रेणियों में बाँटा गया है[7]–

1. **किसी व्यक्ति विशेष के विरूद्ध अपराध**
   इसमें उस व्यक्ति के साइबर स्पेस पर निगरानी रखना एवं उसकी सूचनाऐं चुराकर व्यक्ति को हानि पहुँचाना।
2. **सरकार के विरूद्ध अपराध**
   जैसे साइबर आतंकवाद जिसमें इंटरनेट के माध्यम से राजनीतिक, धार्मिक, साम्प्रदायिक और इस तरह की दूसरी विचारधाराओं के माध्यम से लोगों में आतंक एवं अफवाह फैलाना।
3. **सम्पत्ति के विरूद्ध अपराध**
   जिसमें गोपनीय सूचनाओं, वित्तीय लेन–देन, बैंक एकाउण्ट, पासवर्ड या क्रेडिट कार्ड से जुड़ी महत्वपूर्ण जानकारियों को प्राप्त करना।

तकनीकि दृष्टि से साइबर अपराध को निम्न दो भागों में बांटा जा सकता है।[8]

1. इसके अंतर्गत कम्प्यूटरों को एक लक्ष्य के रूप में अन्य कम्प्यूटरों पर आक्रमण करने के लिए प्रयोग किया जाता है। जैसे हैकिंग, वायरस, वर्मस, डोस आक्रमण। इसमें दूसरे कम्प्यूटरों को हैक कर या उनमें वायरस डालकर उन्हें बाधित किया जाता है।
2. इसके अंतर्गत कम्प्यूटरों को एक शस्त्र या हथियार के रूप में उपयोग लाया जाता है जैसे साइबर आतंकवाद, बौद्धिक सम्पदा अधिकारों का उल्लंघन, क्रेडिट कार्ड धोखाधड़ी, ब्लैकमेलिंग, अश्लील सामग्री का प्रकाशन एवं पारेषण, इत्यादि। इसमें साइबर स्पेस का उपयोग कुत्सित स्वार्थों जैसे आतंकी घटनाओं को अंजाम देना, किसी का एकाउण्ट या क्रेडिट कार्ड के साथ फर्जीवाड़ा करना, किसी दूसरे के डाटा या सूचनाओं के साथ छेड़छाड़ करना, अश्लील असामाजिक तथा उन्माद फैलाने वाली सामग्री का प्रसारण करना, दुष्प्रचार कर ब्लैकमेलिंग करना।

प्रमुख साइबर अपराध

1. हैकिंग से मतलब किसी कम्प्यूटर या नेटवर्क में संरक्षित सूचनाओं को अनाधिकृत रूप से प्रवेश कर प्राप्त कर लेना या उपयोग करना है।[9] वर्तमान में हैकर्स का एक बड़ा संगठन पेशेवर तरीके से हैकिंग के अपराध में लिप्त है। साइबर अपराध के करीब 50–60 प्रतिशत अपराध हैकिंग श्रेणी के होते हैं। सम्पूर्ण विश्व को हैकिंग की समस्या का सामना करना पड़ रहा है। वर्ष 2007 के प्रारम्भिक पाँच महीनों में ही हैकिंग के 2344 मामले प्रकाश में आये थे। हैकिंग के माध्यम से आर्थिक गतिविधियों को प्रभावित करना चिंता का विषय है।[10]
2. सॉफ्टवेयर पायरेसी भी एक साइबर अपराध की श्रेणी में आता है। इसके अन्तर्गत सॉफ्टवेयर बनाने वाली कंपनियों को भुगतान किये बगैर या उनकी बिना आज्ञा के सॉफ्टवेयर की नकली कापियाँ बनाना और उपयोग करना आता है। भारत में एक अनुमान के अनुसार 60 प्रतिशत सॉफ्टवेयर पायरेटिड है। सॉफ्टवेयर की पायरेसी से भारतीय सॉफ्टवेयर कम्पनियों को करीब 900 करोड़ रूपये की वार्षिक हानि होती है।[11]
3. साइबर स्टाकिंग परेशान करने का एक तरीका है। इसमें व्यक्ति को अवांछित या अयाचित सूचनायें भेजकर परेशान किया जाता है। इन्टरनेट के माध्यम से साइबर अपराधी स्वयं को छिपाकर पीड़ित को बार–बार धमकी देता है। आमतौर पर इसके अपराधी पुरूष होते हैं एवं पीड़ित महिलायें होती हैं।[12]
4. वायरस एक प्रकार का साफ्टवेयर प्रोग्राम होता है जो कम्प्यूटरों को हानि पहुँचाता है। इस समय इंटरनेट की दुनिया में हजारों प्रकार के वायरस उपस्थित हैं। एंटीवायरस बनाने वाली प्रसिद्ध कम्पनी नेटवर्क एसोसिएट्स के एक सर्वे के अनुसार इंटरनेट के दुनिया में 60000 से अधिक वायरस हैं। विश्व में पहला कम्प्यूटर वायरस अमेरिकी छात्र फ्रेड कोहेन ने बनाया था।[13]
5. साइबर गेम्बलिंग साइबर अपराध का एक नया आयाम है। इसमें इंटरनेट के द्वारा ऑन लाइन गेम्बलिंग की जाती है। नेट पर ही कैसिनों चल रहे हैं। क्रिश्चियन कैपिटल एडवाइसर्स नामक संस्था के एक सर्वे के अनुसार 2009 तक ऑन लाइन जुआ उद्योग लगभग 3.5 बिलियन डालर का हो गया है।[14]
6. इंटरनेट के माध्यम से पोर्नोग्राफी तेजी से बढ़ता अपराध है। इसमें इंटरनेट के द्वारा बच्चों, महिलाओं एवं पुरूषों की अश्लील तस्वीरों को विभिन्न साइटों पर उपलब्ध करा दी जाती है। अपरिपक्व बच्चों एवं किशोरों पर इसका नकारात्मक प्रभाव पड़ता है। इन्टरनेट के माध्यम से साइबर अपराधी आसानी से उपभोक्ता पर पहुँच जाता है। साइबर वॉचडॉग के अनुसार इंटरनेट अय्याशी का सबसे बड़ा केन्द्र है। रिपोर्ट के अनुसार इंटरनेट उपस्थित कुल साइट्स में एक तिहाई से अधिक पोर्न साइट्स हैं।[15]
7. किसी भी व्यक्ति को मिथ्या ईमेल इस प्रकार भेजा जाता है कि प्राप्तकर्ता उसे वास्तविक एन्टरप्राइज समझकर अपनी व्यक्तिगत सूचनायें फर्जी भेजने वाले को दे दे। इसे साइबर दुनियाँ में फिशिंग कहा जाता है। इस प्रकार की कोशिश व्यक्तिगत पहचान की

चोरी करने के लिए की जाती हैं। अक्सर पासवर्ड, क्रेडिट या बैंक एकाउण्ट के नम्बर इसके द्वारा पूछे जाते हैं।[16]

8. क्रेडिट कार्ड फ्रॉड की घटनाएँ भी आजकल बढ़ गई है। इसके अन्तर्गत किसी व्यक्ति के क्रेडिट कार्ड को अनाधिकृत एवं अवैध रूप से अन्य व्यक्ति उपयोग कर लेता है एवं वास्तविक धारक को हानि पहुँचाता है।[17]
9. किसी कम्प्यूटर के प्रविष्ट के समय अथवा उससे पहले डाटा परिवर्तित करना अर्थात् मिथ्या आँकड़े प्रवेश करा देना डाटा डिडलिंग कहलाता है।[18]
10. लॉजिक बम्ब ऐसे प्रोग्राम होते हैं जो विशेष निर्देश पर सक्रिय होकर कम्प्यूटर प्रोग्राम या डाटा को क्षतिग्रस्त कर देते हैं।[19]
11. सलामी अटैक के अन्तर्गत साइबर अपराधी इतनी सावधानीपूर्वक अपराध करता है या हेराफेरी करता है कि क्षति पा रहे व्यक्ति को इसका आभास तक नहीं होता।[20]
12. ट्रोजन अटैक एक प्रकार का अनाधिकृत प्रोग्राम है जो आंतरिक रूप से क्रियाशील होकर अधिकृत प्रोग्राम की तरह दिखता है। इसमें उपयोगकर्ता के साथ धोखाधड़ी की जाती है।[21]
13. जब कोई उपयोगकर्ता कुछ गोपनीय पत्र लिखकर चला जाता है तो ऐसे में दूसरा व्यक्ति उसकी वही फाइल खोलकर पढ़ लेता है और पढ़ने के बाद फाइल बंद कर चला जाता है। इस साइबर अपराध को स्नूपिंग कहा जाता है।[22]
14. ई–मेल के माध्यम से धमकी देने की घटनाएँ बहुत बढ़ रही हैं। जिसे साइबर थ्रेट कहा जाता है।[23]
15. विख्यात कम्पनियों के नाम से पंजीयन इस उद्देश्य से कराना कि उन्हें भविष्य में अच्छे दामों में विक्रय कर लाभ अर्जित किया जायेगा। साइबर स्क्वेटिंग कहलाता है। जानी मानी साइटों के नाम में थोड़ा परिवर्तन कर ग्राहकों को गुमराह करना टाइपों स्क्वेटिंग कहलाता है।[24]
16. कम्प्यूटर पर काम करने वाला व्यक्ति अपनी निजी एवं गोपनीय जानकारी को सुरक्षित रखना चाहता है इसलिए वह अपनी जानकारियों को सुरक्षित रखने के लिये पासवर्ड इस्तेमाल करता है। साइबर अपराधी उसके पासवर्ड को तोड़कर डाटा चुरा लेता है।[25]
17. प्रौद्योगिकी न तो अच्छी होती है और न बुरी। हमारे द्वारा उसका अनुप्रयोग ही उसे अच्छा या बुरा बनाता है। आतंकवादियों द्वारा भी इंटरनेट का उपयोग करके बड़े पैमाने पर राष्ट्र को प्रभावित करने की कोशिश की जाती है।[26]

सूचना प्रौद्योगिकी अधिनियम, 2000

सूचना प्रौद्योगिकी बिल को संसद में दिसम्बर 1999 में पेश किया गया, संसद ने इसे मई 2000 में पारित किया और 9 जून 2000 को इस पर राष्ट्रपति ने हस्ताक्षर किये। यह अधिनियम 23 अक्टूबर, 2000 से लागू है। इस अधिनियम में 13 अध्याय, 94 अनुभाग और चार अनुसूचियाँ थीं। सूचना प्रौद्योगिकी अधिनियम का प्रभाव उसके सम्पूर्ण भारत में और कुछ स्थितियों में भारत की सीमा के बाहर भी है। इस अधिनियम में कुछ कमियाँ रह गयी थीं। जिसके फलस्वरूप इसमें संशोधन अपरिहार्य हो गया। सूचना प्रौद्योगिकी संशोधन बिल 2006 का प्रारूप 15 दिसम्बर 2006 को संसद के निम्न सदन में पेश किया गया। संशोधन को साकार रूप लेने में लगभग दो वर्ष लग गये। सूचना प्रौद्योगिकी (संशोधन) बिल, 2006 को प्रौद्योगिकी (संशोधन) बिल, 2008 द्वारा पुनः संशोधित किया गया। 22 दिसम्बर, 2008 को निम्न सदन द्वारा एवं 23 दिसम्बर 2008 को उच्च सदन द्वारा इसे पारित कर दिया गया। राष्ट्रपति जी द्वारा इस पर 5 फरवरी 2009 को हस्ताक्षर कर दिये गये।[27]

नेशनल क्राइम रिकॉर्ड ब्यूरों द्वारा निम्न तीन मुख्य शीर्षकों के अन्तर्गत समंकों को एकत्रित किया जाता है।

1. सूचना प्रौद्योगिकी अधिनियम 2000 के अन्तर्गत पंजीकृत अपराध।
2. भारतीय दण्ड संहिता के अन्तर्गत पंजीकृत अपराध।
3. विशेष एवं स्थानीय नियमों के अन्तर्गत पंजीकृत अपराध।

नेशनल क्राइम रिकॉर्ड ब्यूरों की क्राइम इन इंडिया 2015 के अनुसार वर्ष 2015 में कुल 11592 प्रकरण (सूचना–प्रौद्योगिकी अधिनियम 2000, भारतीय दंड संहिता एवं विशेष एवं स्थानीय कानून के अन्तर्गत) दर्ज हुए, जबकि 2014 में 9622 प्रकरण दर्ज हुए। इससे स्पष्ट होता है कि वर्ष 2014 की तुलना में वर्ष 2015 में अपराधों में 20 प्रतिशत की वृद्धि हुई। उत्तर प्रदेश में सर्वाधिक 2208 मामले दर्ज हुए। दूसरा स्थान महाराष्ट्र का रहा जहाँ 2195 प्रकरण दर्ज हुए। अखिल भारतीय स्तर पर वर्ष 2015 में 8121 व्यक्ति गिरफ्तार हुए। जबकि वर्ष 2014 में 5752 व्यक्ति गिरफ्तार हुए थे । इस तरह से वर्ष 2014 एवं 2015 के दौरान गिरफ्तार व्यक्तियों में 41.2 प्रतिशत की वृद्धि हुई।

नेशनल क्राइम रिकॉर्ड ब्यूरो के क्राइम इन इंडिया 2015 के अनुसार सूचना प्रौद्योगिकी अधिनियम 2000 के अंतर्गत वर्ष 2013, 2014 एवं 2015 में क्रमशः 4356, 7201 एवं 8045 आपराधिक प्रकरण दर्ज हुए। वर्ष 2014 की तुलना में वर्ष 2015 में पंजीकृत प्रकरणों में 11.7 प्रतिशत की वृद्धि देखी गयी। वर्ष 2014 में सबसे पहले साइबर आतंकवाद से संबंधित आँकड़ों को एकत्रित किया गया। वर्ष 2014 में 5 और वर्ष 2015 में साइबर आतंकवाद के 13 मामले दर्ज हुए। अश्लीलता के इलैक्ट्रानिक प्रकाशन एवं पारेषण और लैंगिक प्रदर्शन कार्य (धारा 67 से 67C आई0टी0 एक्ट) के अन्तर्गत वर्ष 2013, 2014 एवं 2015 में क्रमशः 1203, 758 एवं 816 मामले दर्ज हुए। कम्प्यूटर से सम्बन्धित अपराधों (धारा 66 से 66E, आई0 टी0 एक्ट) के अन्तर्गत वर्ष 2013, 2014 एवं 2015 में क्रमशः 2516, 5548 एवं 6567 मामले दर्ज हुए।

नेशनल क्राइम रिकॉर्ड ब्यूरो के क्राइम इन इंडिया 2015 के अनुसार सूचना प्रौद्योगिकी अधिनियम, 2000 के अंतर्गत वर्ष 2013, 2014 एवं 2015 में क्रमशः 2098, 4246 एवं 5102 व्यक्ति गिरफ्तार किये गये। वर्ष 2014 की तुलना में वर्ष 2015 में गिरफ्तार व्यक्तियों की संख्या में 20.2 प्रतिशत की वृद्धि देखी गयी। कम्प्यूटर से

सम्बन्धित अपराधों (धारा 66 से 66E आई0टी0 एक्ट) के अन्तर्गत गिरफ्तार व्यक्तियों की संख्या वर्ष 2013, 2014 एवं 2015 के क्रमशः 1011, 3131 एवं 4217 रही।

नेशनल क्राइम रिकॉर्ड ब्यूरो के क्राइम इन इंडिया 2015 के अनुसार सूचना प्रौद्योगिकी अधिनियम 2000 के अन्तर्गत गिरफ्तर व्यक्तियों में 62.5 प्रतिशत व्यक्ति (5102 व्यक्तियों में से 3188 व्यक्ति) 18 वर्ष से अधिक एवं 30 वर्ष से कम आयु के थे। 30.8 प्रतिशत व्यक्ति (5102 में से 1573 व्यक्ति) 30 वर्ष से 45 वर्ष तक के हैं। वर्ष 2015 में 18 वर्ष से कम आयु के 98 नाबालिकों पर केस दर्ज हुए।

नेशनल क्राइम रिकॉर्ड ब्यूरो के क्राइम इन इंडिया 2015 में भारतीय दण्ड संहिता के अंतर्गत साइबर अपराध के 3422 प्रकरण दर्ज हुए। जबकि इसी शीर्षक के अन्तर्गत वर्ष 2013 एवं 2014 में क्रमशः 1337 एवं 2272 प्रकरण दर्ज हुए। वर्ष 2014 की तुलना में वर्ष 2015 में दर्ज हुए अपराधों में 50.6 प्रतिशत की वृद्धि हुई। वर्ष 2015 में चीटिंग के सबसे अधिक 2255 प्रकरण दर्ज हुए। जो कुल अपराधों के 65.9 प्रतिशत थे। भारतीय दण्ड संहिता के अन्तर्गत साइबर अपराधों के मामलों में वर्ष 2013, 2014 एवं 2015 में क्रमशः 1203, 1224 एवं 2867 व्यक्ति गिरफ्तार किये गये।

नेशनल क्राइम रिकॉर्ड ब्यूरो के क्राइम इन इंडिया 2015 के अनुसार विशेष एवं स्थानीय कानूनों के अन्तर्गत वर्ष 2015 में 125 प्रकरण दर्ज किये गये।

साइबर अपराध को नियंत्रित और रोकथाम करने के उपाय

कहा जाता है कि अपराध घटित हो उससे अच्छा है कि हम पहले से ही सचेत रहें। साइबर दुनिया में काम करने वालों को जागरूक रहना चाहिए। सामान्य तौर पर साइबर अपराधों से बचने के लिये दो तरह के उपाय किए जा सकते हैं –

अपराध घटित होने से पूर्व उपाय[28]

1. ई ब्लास्टर नामक सॉफ्टवेयर का प्रयोग जो उपयोगकर्ता की सभी गतिविधियों को रिकॉर्ड करता है एवं ई–मेल रिपोर्ट को भी प्रेषित करता है। यह पोर्नोग्राफी को रोकने में मददगार है।
2. विन गार्जियन की मदद से माता–पिता अपने बच्चों पर नियंत्रण रख उन्हें अवांछित साइटों से दूर रख सकते हैं।
3. फैमिली कनेक्ट सॉफ्टवेयर एक फिल्टर की तरह काम करता है जो अवांछित साइट्स पर रोक लगा देता है।
4. उपायोगकर्ता को सदैव अपना पासवर्ड स्ट्राँग बनाना चाहिए।
5. क्रेडिट कार्ड की जानकारी किसी अपरिचित से शेयर नहीं करनी चाहिए। क्रेडिट एवं डेबिट कार्ड के उपयोग करते समय सावधानी बरतना चाहिए।
6. वायरस से सुरक्षा के लिए एंटीवायरस का उपयोग करना चाहिए साथ ही समय–समय पर इसे अपडेट करते रहना चाहिए।
7. स्कैम एवं फिसिंग जैसे आक्रमणों से बचने के लिए संदेहास्पद ई–मेल के पते की प्रामाणिकता की जानकारी प्राप्त कर लेना चाहिए। किसी भी अपरिचित ई–मेल संदेश के आधार पर अपनी व्यक्तिगत जानकारी शेयर नहीं करना चाहिए।
8. ऑनलाइन खरीददारी करते समय विशेष सावधानी बरतनी चाहिए। पूर्णरूप से संतुष्ट होने के बाद ही आर्डर करना चाहिए। भुगतान क्रेडिट कार्ड से करना चाहिए। भुगतान कम से कम धन वाले क्रेडिट कार्ड से करना चाहिए।
9. हैकिंग से बचाव हेतु फायरवाल सॉफ्टवेयर का उपयोग करना चाहिए। यह अनाधिकृत उपयोगकर्ता को निजी नेटवर्क के उपयोग से रोकता है। यदि आवश्यकता पड़ने पर कोई सॉफ्टवेयर डाउनलोड करना है तो उसे विश्वसनीय वेबसाइट से डाउनलोड करना चाहिए।

अपराध के घटित होने के बाद उपाय[29]

1. सिस्टम को डिस्टर्ब नहीं करना चाहिए एवं कम्प्यूटर को तुरन्त बंद करना चाहिए।
2. पुलिस को तत्काल सूचित करना चाहिए।
3. अवांछित व्यक्ति की सर्विस प्रोवाइडर से तलाश करवाना चाहिए।
4. जाँच दल का सहयोग करना चाहिए।

निष्कर्ष

साइबर अपराध निरन्तर एक बड़ी समस्या बनता जा रहा है। साइबर अपराध के नित नए स्वरूप सामने उपस्थित होते जा रहे हैं। साइबर अपराध में अपराधी प्रायः छिपे रहते हैं उन्हें पकड़ना भी मुश्किल होता है। हालांकि सूचना प्रौद्योगिकी अधिनियम एवं दूसरे कानूनों के प्रभाव से साइबर अपराध पर कुछ हद तक नियंत्रण हुआ है पर इस सम्बन्ध में और भी सख्त कानून बनाकर एवं उचित तरीके से लागू किये जाने की आवश्यकता है। इन अपराधों से बचने के लिये उपयोगकर्ता को भी सावधानीपूर्वक एवं जागरूक रहकर साइबर दुनिया में व्यवहार करना चाहिए।

सन्दर्भ ग्रन्थ सूची

1. बघेल, डॉ0 डी0एस0 (2015) 'अपराधशास्त्र' विवेक प्रकाशन, दिल्ली, पृ0 2
2. अग्रवाल, अनिल (संपादक) (2013–14) 'इंटरनेट : खूबियाँ और खामियाँ' परीक्षा मंथन निबंध श्रृंखला–भाग 5, मंथन प्रकाशन, इलाहाबाद, पृ0 40
3. तिवारी, शंकर प्रसाद (विनय) (2012) 'साइबर क्राइम की प्रकृति तथा सुरक्षात्मक उपाय' प्रतियोगिता दर्पण, आगरा, मार्च, पृ0 1488–1491
4. पाठक,अरूणकुमार (2014) 'साइबर क्राइम एवं साइबर लॉज' पुस्तक सदन प्रकाशन, इलाहाबाद, पृ0 53
5. वही, पृ0 54–55
6. चौहान, एम0एस0 (2012) 'अपराध शास्त्र, दण्ड प्रशासन एवं पीड़ित शास्त्र' सेन्ट्रल लॉ एजेन्सी, इलाहाबाद, पृ0 113
7. तिवारी, शंकर प्रसाद (विनय) (2012) 'साइबर क्राइम की प्रकृति तथा सुरक्षात्मक उपाय' प्रतियोगिता दर्पण, आगरा, मार्च, पृ0 1489
8. वही

9. पाठक, अरूण कुमार (2014) 'साइबर क्राइम एवं साइबर लॉज' पुस्तक सदन प्रकाशन, इलाहाबाद, पृ0 63
10. वही, पृ0 64–66
11. वही, पृ0 66
12. वही, पृ0 69
13. वही, पृ0 68–69
14. वही, पृ0 70
15. वही, पृ0 71–72
16. चौहान, एम0एस0 (2012), 'अपराधशास्त्र, दण्ड प्रशासन एवं पीड़ित शास्त्र' सेन्ट्रल लॉ एजेन्सी, इलाहाबाद, पृ0 115
17. वही
18. वही
19. वही
20. पाठक, अरूण कुमार (2014) 'साइबर क्राइम एवं साइबर लॉज' पुस्तक सदन प्रकाशन, इलाहाबाद, पृ0 77
21. वही, पृ0 78
22. वही, पृ0 79
23. वही
24. वही, पृ0 74
25. वही
26. मिश्रा, डॉ0 जय प्रकाश (2014) 'साइबर विधि एक परिचय' सेन्ट्रल लॉ पब्लिकेशन्स, इलाहाबाद पृ0 172
27. वही, पृ0 14 – 15
28. पाठक, अरूण कुमार (2014) 'साइबर क्राइम एवं साइबर लॉज' पुस्तक सदन प्रकाशन, इलाहाबाद, पृ0 121–124
29. वही, पृ0 126