साइबर फॉरेंसिक

डॉ. राकेश प्रकाश

पुलिस अनुसंधान एवं विकास ब्यूरो
गृह मंत्रालय, भारत सरकार, नई दिल्ली

साइबर फॉरेंसिक

डॉ. राकेश प्रकाश
एम ए, एम फिल, पी एच डी मीडिया प्रबंधन

पुलिस अनुसंधान एवं विकास ब्यूरो
गृह मंत्रालय, भारत सरकार, नई दिल्ली
वर्ष 2021

भारत सरकार, गृह मंत्रालय की हिन्दी सलाहकार समिति द्वारा दिनांक 23 मई, 1979 को आयोजित बैठक में निर्णय लिया गया था कि पुलिस, अपराध, कारागार एवं न्यायालयिक विज्ञान तथा पुलिस प्रशासन आदि विषयों पर हिन्दी में मौलिक पुस्तकें उपलब्ध कराने के लिए पं. गोविन्द वल्लभ पंत पुरस्कार योजना प्रतिस्थापित की जाए। तदनुसार 22 मार्च, 1980 को गृह मंत्रालय अपर सचिव की अध्यक्षता में हुई बैठक में निर्धारित मापदंडो के अनुसार इस योजना को अंतिम रूप दिया गया। इस योजना के भाग 1 के अंतर्गत प्रकाशित मौलिक पुस्तकों को पुरस्कृत किया जाता है तथा भाग 2 के अंतर्गत दिए गए विषयों पर पुस्तक लेखन कार्य कराया जाता है। इसी के तहत यह पुस्तक प्रकाशित की जा रही है।

इस पुस्तक में दिए गए विचार लेखक के निजी हैं
इनसे पुलिस अनुसंधान एवं विकास ब्यूरो,
गृह मंत्रालय, भारत सरकार, नई दिल्ली की
सहमति आवश्यक नहीं है।

प्रकाशक	-	पुलिस अनुसंधान एवं विकास ब्यूरो गृह मंत्रालय, एन.एच-8, महिपालपुर, नई दिल्ली-110037
संपादक	-	विजय कुमार
संपादन सहयोग	-	सतीश चन्द्र डबराल, वरिष्ठ अनुवादक
प्रथम संस्करण	-	2021
मुद्रक	-	स्मैट फॉर्मस, 3588, जी.टी.रोड़, दिल्ली-110007

आमुख

भारत की पुलिस व्यवस्था को सुदृढ़ बनाने के लिए पुलिस अनुसंधान एवं विकास ब्यूरो, गृह मंत्रालय, भारत सरकार द्वारा वर्ष 1982 से पुलिस, कारागार प्रशासन, अपराध शास्त्र तथा न्यायालयिक विज्ञान इत्यादि से संबंधित विभिन्न विषयों पर हिंदी में पुस्तक लेखन को बढ़ावा देने के लिए पंडित गोविंद वल्लभ पंत पुरस्कार योजना चलाई जा रही है । इस योजना के भाग एक के अंतर्गत इन विषयों पर वर्ष भर में हिंदी में प्रकाशित पांच उत्कृष्ट पुस्तकों को पुरस्कृत किया जाता है। साथ ही योजना के भाग दो के अंतर्गत ब्यूरो द्वारा पुस्तक लेखन हेतु विषय देकर रुपरेखाएं आमंत्रित की जाती हैं। मूल्यांकन समिति द्वारा इन रुपरेखाओं को प्रकाशन योग्य पाए जाने पर पुलिस अनुसंधान एवं विकास ब्यूरो द्वारा इनका प्रकाशन किया जाता है। इस योजना के भाग एक के अंतर्गत ब्यूरो द्वारा अब तक उपर्युक्त विषयों की हिंदी में प्रकाशित 151 पुस्तकों को पुरस्कृत किया जा चुका है । भाग दो के अंतर्गत अब तक ब्यूरो द्वारा 40 पुस्तकों का प्रकाशन किया जा चुका है।

पुलिस अनुसंधान एवं विकास ब्यूरो द्वारा वर्ष 2019 में साइबर फोरेंसिक विषय पर रुपरेखा आमंत्रित की गई थी । वर्ष 2020 के दौरान योजना की समिति द्वारा की गई सिफारिशों के आधार पर "साइबर फॉरेंसिक" पुस्तक जिसके लेखक डॉ राकेश प्रकाश है का प्रकाशन कार्य किया गया है। साइबर फॉरेंसिक के क्षेत्र में हिंदी में जानकारी साझा करना अपने आप में चुनौतीपूर्ण कार्य है। इस पुस्तक में साइबर फॉरेंसिक के अलग-अलग पहलुओं के मामलों को शामिल किया गया है। साइबर अपराध से जुड़ी अतीत की घटनाओं का विश्लेषण करने के साथ-साथ वर्तमान में हो रही साइबर अपराध की घटनाओं से निपटने के तरीके और भविष्य की संभावित चुनौतियों को रेखांकित करने की कोशिश की गई है। पुस्तक में मुख्य रूप से साइबर फॉरेंसिक से जुड़ी समस्या, कारण, निवारण, जानकारों की राय

और इनसे संबंधित आंकड़ों का समावेश किया गया है। इंटरनेट और साइबर फॉरेंसिक से जुड़े मामले बेहद जटिल होते हैं, खासकर तब जब साइबर अपराधी दुनिया के किसी तीसरे देश में बैठकर आपके कंप्यूटर नेटवर्क को पूरी तरह से अपने कब्जे में ले लेता है।

इस पुस्तक में साइबर क्राइम की नवीन चुनौतियों की व्यापक रूप से जानकारी देने के साथ-साथ विभिन्न प्रकार की साइबर समस्याओं, फेक न्यूज़, हैकिंग, पायरेसी, वायरस, स्पाइवेयर, पोर्नोग्राफी इत्यादि पर प्रकाश डाला गया है । पुस्तक में वैश्विक स्तर पर बदल रहे फॉरेंसिक साइंस के स्वरूप, साइबर अटैक से बचने के लिए क्या करें क्या न करें, इंटरनेट के फायदे और नकारात्मक प्रभाव, साइबर सुरक्षा की जरूरत, साइबर फॉरेंसिक टूल और डिजिटल प्रौद्योगिकी, राष्ट्रीय साइबर फॉरेंसिक प्रयोगशाला, सरकार द्वारा इन गुनाहों को रोकने के लिए उठाए गए मुख्य कदम, इनसे निपटने की मौजूदा स्थिति, प्रभावी कानून, सूचना प्रौद्योगिकी अधिनियम इत्यादि की जानकारी के साथ-साथ वर्तमान कानून एवं नए कानूनों की आवश्यकता, फॉरेंसिक लैब, कंप्यूटर फॉरेंसिक, नेटवर्क फॉरेंसिक इत्यादि की महत्वपूर्ण जानकारी दी गई है।

देश में साइबर अपराध की वास्तविकता को सही मायने में लोगों के सामने रखने के लिए पुस्तक में विभिन्न आंकड़ों को शामिल किया गया है। इस पुस्तक में सरल भाषा के प्रयोग का विशेष ध्यान रखा गया है ताकि लोगों को विषय वस्तु समझने में किसी प्रकार की कठिनाई का सामना न करना पड़े। आने वाले समय में साइबर फॉरेंसिक न सिर्फ साइबर अपराध बल्कि कई दूसरे तरीके के अपराधों को सुलझाने में भी कारगर भूमिका निभाएगा। आशा है कि यह पुस्तक साइबर फॉरेंसिक से जुड़े विभिन्न जटिल पहुलओं को लोगों के सामने सरल और सहज रूप में प्रस्तुत करने में सफल रहेगी और इस क्षेत्र से जुड़े सभी लोगों के अध्ययन और शोध के काम में भी उपयोगी साबित होगी।

संपादक

लेखक परिचय

डॉ. राकेश प्रकाश, एमिटी विश्वविद्यालय, नोएडा में असिस्टेंट प्रोफेसर के पद पर कार्यरत हैं। पिछले 20 वर्षों से ये पत्रकारिता के विभिन्न माध्यमों समाचार पत्रों, इंटरनेट, रेडियो, टेलीविजन, पुस्तक लेखन और अध्यापन के क्षेत्र में सक्रिय हैं। वर्ष 2000 में दैनिक अमर उजाला, हिंदी समाचार पत्र के साथ पत्रकारिता में करिअर की शुरुआत के बाद दैनिक जागरण समाचार पत्र के इंटरनेट संस्करण www.jagran.com से जुड़े। नवंबर 2001 से दिसंबर 2002 के बीच ईटीवी में कॉपी एडिटर के पद पर कार्य किया और वर्ष 2002 से 2017 तक ज़ी न्यूज़, नोएडा में प्रोड्यूसर के पद पर रहे। आकाशवाणी (All India Radio), नई दिल्ली के समाचार सेवा प्रभाग में संवाददाता के रुप में और डीडी न्यूज़, नई दिल्ली में बतौर असिस्टेंट एडिटर कार्य किया। इसके पश्चात भारतीय कृषि अनुसंधान परिषद, नई दिल्ली और प्रकाशन निदेशालय, गोविंद बल्लभ पंत विश्वविद्यालय, उत्तराखंड में संपादक के रुप में काम किया। तत्पश्चात शोध पत्रिका संचार विमर्श में संपादकीय सलाहकार की भूमिका का निर्वहन किया। नाट्य कला एवं फिल्म अध्ययन विभाग, महात्मा गांधी अंतरराष्ट्रीय हिंदी विश्वविद्यालय, वर्धा से पी.एचडी. की पढ़ाई पूरी करने के बाद इन्होंने विभाग के अध्ययन मंडल के सदस्य के रुप में अपनी सेवाएं दी। प्रेस सूचना ब्यूरो, नई दिल्ली और भारतीय अंतर्देशीय जलमार्ग प्राधिकरण, नोएडा में अनुवादक के तौर पर कार्य किया। वर्ष 2010 में इन्हें पुलिस अनुसंधान एवं विकास ब्यूरों, गृह मंत्रालय, भारत सरकार द्वारा पं० गोविंद वल्लभ पंत पुरस्कार योजना के अंतर्गत सम्मानित किया गया। इसी वर्ष वैध समस्याओं के निदान हेतु हिंसा की बढ़ती प्रवृति नाम से इनकी पुस्तक प्रकाशित हुई। गुरु गोविंद सिंह इंद्रप्रस्थ विश्वविधायलय, दिल्ली, गुरु जंभेश्वर विज्ञान एवं प्रौद्योगिकी विश्वविद्यालय, हिसार, से संबंद्ध विभिन्न

संस्थानों में अथिति व्याख्याता के तौर पर आमंत्रित हुए। वर्तमान में डॉ राकेश प्रकाश एमिटी विश्वविद्यालय नोएडा में असिस्टेंट प्रोफेसर (ग्रेड-3) के पद पर कार्यरत हैं। इनसे rakesh.prakash@gmail.com या rprakash1@amity.edu पर संपर्क किया जा सकता है।

अनुक्रमणिका

भाग 1
साइबर फॉरेंसिक – चुनौती और संभावनाएं

चौथा अध्याय

भाग 3
साइबर फॉरेंसिक – नई प्रौद्योगिकी नई संभावनाएं

भाग 1

साइबर फॉरेंसिक – चुनौती और संभावनाएं

प्रथम अध्याय

साइबर फॉरेंसिक क्राइम से जुड़ी चुनौतियां और पुलिस की तैयारी

साइबर फॉरेंसिक

साइबर फॉरेंसिक की दुनिया में हर दिन एक नई चुनौती उभरकर सामने आ रही है। चुनौती जितनी जटिल होती है, उसका सकारात्मक या नाकारात्मक परिणाम उतना ही गंभीर और दूरगामी होता है। साइबर फॉरेंसिक का सीधा संबंध इंटरनेट से है और मौजूदा दौर में इंटरनेट का महत्व दिन-प्रतिदिन बढ़ता जा रहा है। शहर से लेकर गांव तक और गहरे समुद्र से लेकर अंतरिक्ष की अनंत रहस्यमयी दुनिया तक, कम्प्यूटर की मदद के बिना किसी बड़े काम की कल्पना करना भी मुश्किल है। लेकिन तकनीक का इस्तेमाल गलत इरादों की खातिर किया जाने लगे तो समस्याएं पैदा होने लगती हैं। आजकल अपराधी भी तकनीक का सहारा लेकर हाईटेक होते जा रहे हैं। अपराधियों का गिरोह गुनाह के लिए कम्प्यूटर, इंटरनेट, डिजिटल उपकरण और वर्ल्ड वाइड वेब इत्यादि का प्रयोग कर रहे हैं। ऑनलाइन ठगी या चोरी भी इसी कैटगरी का खतरनाक अपराध होता है। किसी भी वेबसाइट को हैक या सिस्टम से डेटा की चोरी करना, इस तरह के सभी अपराध साइबर फॉरेंसिक या साइबर क्राइम की श्रेणी में आते हैं और ऐसे अपराधियों की नकेल कसने के लिए साइबर फॉरेंसिक की तकनीक एक कारगर हथियार है क्योंकि साइबर क्राइम, दुनिया भर में सुरक्षा और जांच एजेंसियां के लिए परेशानी का सबब बन चुकी है।

यही वजह है कि ऑनलाइन आतंकवाद एवं चरमपंथ से निपटने और इंटरनेट को सुरक्षित रखने की बड़ी पहल वैश्विक स्तर पर शुरु हो चुकी है। साइबर

अपराध को लेकर वैश्विक नियमन पर सहमति भले ही न बन रही हो लेकिन एक वैश्विक समझ बनाने की जरूरत है ताकि यह सुनिश्चित हो कि साइबर क्षेत्र सुरक्षित बना रहे। डिजिटल क्षेत्र में चरमपंथी और आतंकवादी ताकतों को घुसने से रोकने के लिए सभी देशों को द्विपक्षीय या बहुपक्षीय ढंग से समन्वित कार्य करने की आवश्कता है। श्री एस. जयशंकर ने साइबर जगत के संचालन से जुड़े सवालों पर पेरिस शांति मंच पर कहा कि महत्त्वपूर्ण ढांचों पर साइबर हमलों के साथ ही खास तरह के सुरक्षा खतरों से निपटने के लिए देशों को तेज कार्रवाई और साइबर हमलों को कम करने की व्यवस्था पर विचार करना चाहिए। यह इसलिए ताकि संपूर्ण डिजिटल जगत हमारी सुरक्षा को जोखिम में डाले बिना हमारे समाज एवं अर्थव्यवस्थाओं को आगे ले जाने में काम आए। ऑनलाइन आतंकवाद एवं चरमपंथ से निपटने और इंटरनेट को सुरक्षित रखने की बड़ी पहल शुरु करने में भारत फ्रांस, न्यूजीलैंड, कनाडा और कई अन्य देशों के साथ शामिल हुआ है। 'क्राइस्टचर्च कॉल टू एक्शन' पहल का नाम न्यूजीलैंड के शहर पर रखा गया है, जहां मस्जिदों पर हुए हमले में 51 लोगों की मौत हो गई थी। विदेश मंत्री श्री एस. जयशंकर ने कहा कि वैश्विक नियमन पर सहमति भले ही न बन रही हो लेकिन एक वैश्विक समझ बनाने की जरूरत है ताकि यह सुनिश्चित हो कि साइबर क्षेत्र बिना किसी रोकटोक के और सुरक्षित बना रहे। उन्होंने कहा कि इसके लिए बहुपक्षवाद पहले से कहीं ज्यादा जरूरी हो गया है। साइबर क्षेत्र एवं डिजिटल प्रौद्योगिकियां आर्थिक, सामाजिक, राजनीतिक, औद्योगिक और यहां तक कि व्यावहारिक परिवर्तन में भी अहम भूमिका निभाती हैं। उन्होंने कहा, ये राष्ट्रीय सीमाओं में संचालित होते हैं लेकिन इनकी प्रकृति किसी सीमा से बंधी नहीं होने की है। भारत जैसे बड़े विकासशील देश ने विश्व के सबसे बड़े डिजिटल प्रौद्योगिकी कार्यक्रम 'डिजिटल इंडिया' की शुरुआत की थी जिसका मकसद सभी नागरिकों तक डिजिटल अवसंरचना को पहुंचाना है। भारत डिजिटल अवसरों को लेकर उत्साहित है लेकिन साइबर क्षेत्र के खतरों के प्रति बेहद चिंतित भी है। चिंता की असली वजह साइबर क्राइम

के बढ़ते आंकड़े हैं।

साइबर अपराध क्या है?

साइबर अपराध एक ऐसा अपराध है जिसमें कंप्यूटर एवं नेटवर्क शामिल होता है। किसी की भी निजी जानकारी कंप्यूटर से निकाल लेना या चोरी कर लेना भी साइबर अपराध है। साइबर अपराध कई प्रकार के हैं जैसे कि स्पैम ईमेल, हैकिंग, फिशिंग, वायरस को डालना, किसी की जानकारी को ऑनलाइन प्राप्त करना या किसी पर हर समय नजर रखना साइबर अपराध है। साइबर अपराध कानून प्रवर्तन अधिकारियों हेतु अद्वितीय चुनौतियों भरा हैं और ऐसे अपराध जटिल हैं और पहचान के लिए कुछ विशेष कौशल और खासकर फोरेंसिक कौशल की आवश्यकता होती है।

किसी अपराध की जांच के लिए वैज्ञानिक सिद्धांतों और तौर-तरीकों का उपयोग फॉरेंसिक साइंस कहलाता है। इस फील्ड में काम करने वाले प्रोफेशनल फॉरेंसिक साइंस साइंटिस्ट कहलाते हैं। ये प्रोफेशनल नई तकनीकों का इस्तेमाल कर सबूतों की जांच करते हैं और अपराधियों को पकड़ने में मदद करते हैं। ये क्राइम लेबोरेटरी आधारित जॉब है, जिसमें सबूतों की समीक्षा (Analysis) करना होता है।

फॉरेंसिक साइंस अपराध से जुड़ा विज्ञान है। इसके अंतगर्त अपराध का पता लगाने के लिए शरीर के तरल पदार्थो की जांच की जाती है। फॉरेंसिक रिपोर्ट को अदालत भी अहम प्रमाण मानती है। देश-विदेश में बढ़ रही आतंकी घटनाओं ने फॉरेंसिक विशेषज्ञों की मांग बढ़ा दी है। आपराधिक वारदातों के सूत्रधारों की धर-पकड़ के लिए प्रशिक्षित सुरक्षा बलों की जरूरत आज समाज और समय की मांग है।

इस साइंस को जानकर अपराध से जुडे लोगों को पकड़वाने में काफी मददगार साबित होता है। अपराधियों या आतंकवादी का स्कैच तैयार

कराने में फॉरेंसिक साइंस एक्सपर्ट काफी सहायक होते हैं। अदालत भी इस विज्ञान की मदद लेकर जांच को आगे बढ़ाती है। आतंकवादी गुत्थियां हों या रहस्यमय मौत, इसे सुलझाने में फॉरेंसिक साइंस की अहम भूमिका होती है। फॉरेंसिक साइंटिस्ट से प्राप्त इनपुट को लेकर ही इंवेस्टिगेटिंग ऑफिसर अदालत के समक्ष हाजिर होता है। जरूरत पड़ने पर फॉरेंसिक एक्सपर्ट घटना स्थल का निरीक्षण करता है।

राष्ट्रीय अपराध रिकॉर्ड ब्यूरो (एनसीआरबी) के आंकड़ों में साइबर क्राइम

साल 2015 - 17 के दौरान देश के अलग-अलग हिस्सों में 45,705 साइबर क्राइम के मामले दर्ज किए गए हैं। साल 2015 में देश में 11,331, वर्ष 2016 में 12,187 और साल 2017 में 21,593 साइबर अपराध के मामले दर्ज किए गए। पिछले तीन सालों में साइबर क्राइम में 1.7 प्रतिशत की दर से बढ़ोत्तरी हुई है। साल 2015 में सबसे अधिक साइबर अपराध की घटनाएं उत्तर प्रदेश में दर्ज हुई हैं, जिनकी संख्या 2208 है। दूसरी ओर 2017 में यूपी में सबसे ज्यादा 4971 साइबर क्राइम की घटनाएं हुई हैं। 2015-17 तक साइबर क्राइम में सबसे ज्यादा यानी 5 फीसदी की बढ़ोत्तरी कर्नाटक में दर्ज की गई है। इन तीन सालों में सबसे कम साइबर क्राइम के मामले पूर्वोत्तर भारत के नागालैंड में दर्ज किए गए हैं, यहां साइबर अपराध के सिर्फ 2 मामले ही दर्ज किए गए हैं। दूसरी ओर केंद्र शासित प्रदेश दिल्ली में साइबर क्राइम की 874 घटनाएं दर्ज की गई हैं। एनसीआरबी के आंकड़ों पर यकीन किया जाए तो केंद्र शासित प्रदेशों में से एक लक्षद्वीप में साल 2015-17 के बीच साइबर अपराध का एक भी मामला सामने नहीं आया है। एक अनुमान के मुताबिक किसी भी अपराध से जुड़े सारे मामले पुलिस के पास नहीं पहुंच पाते हैं। लिहाजा साइबर अपराध या धोखाधड़ी के छोटे-मोटे मामले में भी ऐसा हो सकता है।

न्यूक्लियर पावर प्लांट पर साइबर अटैक

मौजूदा दौर में साइबर फॉरेंसिक का महत्व इस बात से समझा जा सकता है कि कुछ दिन पहले ही न्यूक्लियर पावर कॉर्पोरेशन ऑफ इंडिया (एनपीसीआईएल) ने पुष्टि की है कि तमिलनाडु में स्थित कुडनकुलम प्लांट के सिस्टम पर साइबर अटैक हुआ था और यह खबर सही है। लेकिन, एनपीसीआईएल ने यह भी साफ किया है कि साइबर अटैक से सिस्टम को कोई नुकसान नहीं पहुंचा है। इससे पहले न्यूक्लियर प्लांट के अधिकारियों ने दावा किया था कि उनके सिस्टम पर साइबर अटैक करना नामुमकिन है। परमाणु ऊर्जा विभाग के तहत लोक उपक्रम न्यूक्लियर पावर कॉरपोरेशन ऑफ इंडिया (एनपीसीआईएल) के अनुसार साइबर अटैक से संयंत्र की कंप्यूटरीकृत कार्यप्रणाली पर असर नहीं हुआ है। एनपीसीआईएल की माने तो 'साइबर अटैक के बारे में 4 सितंबर 2019 को पता लगने पर इस मामले को सीईआरटी-इन (कंप्यूटर आपात कार्रवाई टीम) द्वारा सूचित किया गया था। परमाणु ऊर्जा विभाग के विशेषज्ञों ने तुरंत मामले की छानबीन के काम को पूरा कर लिया। जांच में पता चला कि प्रभावित कंप्यूटर एक यूज़र का था, जोकि प्रशासनिक उद्देश्यों के लिए इस्तेमाल होने वाले इंटरनेट नेटवर्क से जुड़ा था।

आतंक का अड्डा न बने साइबर स्पेस : प्रधानमंत्री

प्रधानमंत्री नरेंद्र मोदी ने 23 सितंबर 2017 को दिल्ली में साइबर स्पेस पर 5वें वैश्विक सम्मेलन का उद्घाटन करते हुए कहा था कि साइबर स्पेस की सुरक्षा के बगैर डिजिटल इंडिया सफल नहीं होगा। उन्होंने साइबर आतंक से लेकर सभी तरीके के साइबर अपराध पर दुनिया के नेताओं से रोक लगाने की अपील की थी । इससे साफ है कि भारत के विकास में फॉरेंसिक साइंस की भूमिका काफी अहम है। प्रधानमंत्री मोदी ने कहा था कि पिछले दो दशकों में साइबर स्पेस ने कैसे पूरी दुनिया को बदल कर रख दिया है, हम

70 के दशक के बड़े-बड़े आकार के कंप्यूटर याद करते हैं और अब भारत की प्रतिस्पर्धा इस मामले में विकसित देशों से है। उन्होंने कहा कि मोबाइल फोन अब डाटा स्टोरेज और कम्यूनिकेशन का सबसे बड़ा टूल है। डिजिटल दुनिया में बड़े बदलाव अब और तेज हो रहे हैं, ये दुनिया के साथ भारत में भी नजर आ रहा है। भारत के आईटी टैलेंट को दुनिया में पहचान मिली है भारतीय आईटी कंपनी ने भी दुनिया में अपना नाम कमाया है, आज डिजिटल टेक्नॉलॉजी एक बड़ा उद्योग बन चुका है। इसलिए इससे जुड़े सुरक्षा के विभिन्न पहलुओं के अध्ययन और खतरों को दूर करने के लिए साइबर फॉरेंसिक की महत्ता काफी बढ़ गई है।

डिजिटल एक्सेस से लोगों को सशक्त करने की कोशिश

डिजिटल एक्सेस की मदद से लोगों को सशक्त बनाने की कोशिश लगातार जारी है। मोबाइल पॉवर का इस्तेमाल और असर दूर-दराज के क्षेत्रों में भी हो रहा है। डिजिटल क्रांति की मदद से आज एक किसान कई तरह की सुविधाओं का इस्तेमाल कर सकता है। उदाहरण के लिए मृदा परीक्षण, विशेषज्ञों की राय और बेहतर कीमत, डिजिटल क्रांति उन्हें बेहतर आमदनी में मदद कर रही है। इस काम में भी साइबर फॉरेंसिक तकनीक की अहम भूमिका है।

ई-गवर्नेंस को देगा नई दिशा

भारत में लोग अब कैशलेस ट्रांजेक्शन कर रहे हैं। साइबर अपराधी लोगों की कमाई को गलत तरीके से हड़प न लें, इसके लिए साइबर फॉरेंसिक तकनीक के लाभ आमलोगों तक पहुंचाना है। क्योंकि पहले डिजिटल तकनीक का आमलोग उस तरीके से उपयोग नहीं करते थे, जितना वह आज कर रहे हैं। आज ज्यादातर सेवाओं को ऑनलाइन तकनीक से जोड़ा जा रहा है।

साइबर स्पेस महत्वपूर्ण क्षेत्र

साइबर स्पेस नए-नए प्रयोग के लिए एक महत्वपूर्ण क्षेत्र है। स्टार्टअप्स के जरिए रोजाना की दिक्कतों का समाधान करने और जीवन स्तर सुधारने की कोशिश में लगे हैं। इंटरनेट युवाओं के लिए एक बेहतर माध्यम है। यहां वह अपना हुनर दिखा सकते हैं। लिहाजा साइबर स्पेस की सुरक्षा के लिए साइबर फॉरेंसिक की भूमिका काफी महत्वपूर्ण हो गई है। आने वाले दिनों में साइबर फॉरेंसिक काफी अहम भूमिका निभाएगा।

साइबर-सुरक्षा के मुद्दे पर समाधान की जरूरत

विश्व समुदाय को साइबर-सुरक्षा के मुद्दे पर आत्मविश्वास के साथ एक समाधान और समान दृष्टिकोण की जरूरत है। साइबर स्पेस तकनीक लोगों की ज़रुरतों को मजबूती प्रदान करने वाली होनी चाहिए। सभी देशों को यह सुनिश्चित करने की जिम्मेदारी लेनी होगी कि डिजिटल स्पेस आतंकवाद और कट्टरता के लिए एक खेल का मैदान बनकर ना रह जाए। इस प्रौद्योगिकी का उपयोग मानव एवं विश्व के कल्याण और विकास के लिए होना चाहिए। साइबर फॉरेंसिक की भूमिका के बिना इस लक्ष्य को पूरा नहीं किया जा सकता है। यह जानकर आपको हैरानी होगी कि साइबर अपराध की वजह से सिर्फ भारत ही नहीं पूरी दुनिया परेशान है। इसकी वजह से दिनोंदिन बढ़ते संकट का अनुमान हम इस बात से लगा सकते हैं कि साइबर अपराधों और अपराधियों पर रोक लगाने के लिए पूरी दुनिया परेशान है। साइबर फॉरेंसिक का दायरा अब काफी बड़ा हो चुका है। तकनीक के जरिए विकास जितनी तेजी से गांव-गांव और शहर-शहर में पांव पसार रहा है इसी के साथ इंटरनेट-कंप्यूटर नेटवर्क का जाल भी उसी तेजी से आगे बढ़ता जा रहा है।

गृह मंत्रालय ने साइबर फ्रॉड और साइबर क्राइम को रोकने के लिए साइबर एंड इंफॉर्मेशन सिक्योरिटी ब्रांच का गठन किया है। यह इस बात की ओर

साफ इशारा करता है कि केंद्र सरकार अब साइबर क्राइम को रोकने के लिए कठोर कदम उठाने के मूड में है। गृह मंत्रालय सभी राज्यों को निर्देश दे चुकी है कि वह अपने-अपने राजधानी और महत्वपूर्ण स्थानों पर साइबर क्राइम और बैंक फ्रॉड की जांच को मजबूती प्रदान करने के लिए 'फॉरेंसिक लैब' में सभी अत्याधुनिक सुविधाएं उपलब्ध कराएं। बैंक फ्रॉड और साइबर अपराध की वजह से लोगों को बहुत मुसीबतों का सामना करना पड़ता है। साइबर अपराध के कारण आम जनता की मेहनत की कमाई एक झटके में गायब हो जाती है। इसलिए मामले की गंभीरता को देखते हुए सभी राज्य साइबर क्राइम की फॉरेंसिक जांच और उसके तकनीक पहलुओं पर ज्यादा जोर दे रहे हैं। जितनी तेजी से देश में इंटरनेट के इस्तेमाल करने वालों की संख्या में दिनोंदिन इजाफा हो रहा है, ठीक उसी रफ्तार से पूरी दुनिया में साइबर अपराध के खतरे भी बढ़ते जा रहे हैं।

आम लोगों के पर्सनल अकाउंट को हैक करने से लेकर साइबर स्टॉकिंग, साइबर टेररिज्म जैसी वारदात अब आम बात हो गई हैं। इन तमाम खतरों से बैंकों, मल्टीनेशनल कंपनियों के कामकाज पर काफी असर पड़ता है। इतना ही नहीं आम लोग अपनी गाढ़ी कमाई का बड़ा हिस्सा बैंकों में रखते हैं, उनकी मेहनत की कमाई भी साइबर अपराध और साइबर फ्रॉड का शिकार हो जाती है, इन सभी पर लगाम लगाने के लिए और ऐसे जालसाजी से बचाने के लिए गृह मंत्रालय योजनाबद्ध तरीके से काम कर रही है। एक अनुमान के मुताबिक दुनिया भर में साइबर हमलों से करीब सवा तीन लाख से भी अधिक कंप्यूटर प्रभावित हुए हैं। जिस तरीके से लोगों की दिनचर्या और उनके कामकाज के तरीके बदल रहे हैं, कुछ इसी अंदाज में अलग अलग तरह की धोखाधड़ी की वारदाते भी बढ़ती जा रही है। सभी के हाथों में स्मार्टफोन है, कंप्यूटर हैं, लैपटॉप हैं। लोग जाने अनजाने अपनी हर जानकारी चाहे वह पर्सनल हो या प्रोफेशनल साझा करने से बाज नहीं आते हैं। इसी बात का फायदा हैकर उठाते हैं और पलक झपकते ही हैकिंग की वारदात को अंजाम दे डालते हैं। कन्याकुमारी से लेकर कश्मीर तक साइबर अपराध

और अपराधियों से निपटने के लिए व्यापक स्तर पर निगरानी की जा रही है। जम्मू कश्मीर में फोरेंसिक साइंस लैबोरेटरी (एफएसएल) ने क्राइम से जुड़े मुद्दों पर गहन जांच के लिए श्रीनगर में डीएनए टेस्ट के लिए लैब भी स्थापित की है। इसके अलावा साथ ही कंप्यूटर फोरेंसिक लैब भी बनाई गई है। इसका मकसद मोबाइल और कंप्यूटर से साइबर अपराध के मामलों की पड़ताल कर उन्हें सुलझाना है।

डीएनए टेस्टिंग लैब में सभी जरूरी उपकरण लगाए गए हैं। लैब में किसी केस से जुड़े व्यक्ति के ब्लड सैंपल के माध्यम से डीएनए टेस्ट की प्रक्रिया पूरी की जाएगी। इसका मुख्य उद्देश्य किसी व्यक्ति के खून के निशान की बदौलत अपराधी के खून का मिलान कर सही अपराधी की पहचान करना है। कंप्यूटर या मोबाइल से हुए आनलाइन फ्राड या यूं कहें कि साइबर क्राइम के जांच में भी यह तरीका बेहद कारगर साबित हुआ है। दुनिया भर में साइबर अपराधियों से निपटने के लिए साइबर फॉरेंसिक साइंस के क्षेत्र में नए-नए प्रयोग और अविष्कार का दौर जारी है। अमेरिका के वाशिंगटन में वैज्ञानिकों ने एक अल्गोरिद्म (Algorithm) का विकास किया है, जो डेटा चोरी के इरादे से किये गए हमलों के समय हार्डवेयर की सुरक्षा करता है। हमलों में हैकर इलेक्ट्रॉनिक उपकरणों के हार्डवेयर में ऊर्जा और विद्युत चुम्बकीय विकिरण की विविधताओं के बारे में जानकारी हासिल करते हैं और उस जानकारी का प्रयोग करके एक कोड में परिवर्तित सूचना या डेटा (एंक्रिप्टेड जानकारी) को चुरा लेते हैं।

अमेरिका में यूनिवर्सिटी ऑफ़ व्योमिंग में सहायक प्रोफेसर माइक बोरोविज़क के मुताबिक भले ही आप सॉफ़्टवेयर को कितना भी सुरक्षित बना सकते हैं लेकिन अगर हार्डवेयर जानकारी लीक करता है, तो आप मूल रूप से उन सभी सुरक्षा तंत्रों को नाकारा साबित कर सकते हैं। हर तरीके के हालात को ध्यान में रखकर शोधकर्ताओं ने डिजाइन और कोड उपकरणों को इस तरह से पुनर्गठित करने का तरीका विकसित करने की ठानी है, जो किसी भी

जानकारी को लीक नहीं करता है। ऐसा करने के लिए, उन्होंने एक अल्गोरिद्म विकसित किया है जो अधिक सुरक्षित हार्डवेयर प्रदान करने का काम करता है।

व्हाट्सऐप में साइबर अपराधियों ने लगाई सेंध

साइबर फॉरेंसिक की दुनिया में व्हाट्सऐप से जुड़े एक नए खुलासे ने सबको हिलाकर रख दिया। इज़राइली टेक्नोलॉजी कंपनी NSO ने 2019 में हुए आम चुनाव के दौरान व्हाट्सऐप में सेंध लगाकर पत्रकारों, वकीलों और मानवाधिकार कार्यकर्ताओं की जासूसी की। इस मामले में अभी अंतिम सच निकलकर सामने आना बाकी है। इज़राइली कंपनी NSO की माने तो सरकार या सरकारी एजेंसियां ही पेगासस सॉफ़्टवेयर के माध्यम से जासूसी कर सकती हैं। इससे पहले कैंब्रिज एनालिटिका मामले में भी फ़ेसबुक से जवाब मांगा गया था। इस बार भी फेसबुक को ही जवाब देना होगा क्योंकि व्हाट्सऐप का भी मालिकाना हक फेसबुक के पास ही है। जानकारों की माने तो व्हाट्सऐप में सेंध लगाने का यह गोरखधंधा कई सालों से चल रहा था। लेकिन अब कैलिफ़ोर्निया की अदालत में व्हाट्सऐप द्वारा मुकदमा दायर करने के पीछे आखिर क्या रणनीति है? इसके बारे में अभी कुछ कहना जल्दबाजी होगी। फिलहाल तो यही जानकारी निकल कर सामने आ रही है कि व्हाट्सऐप ने इजरायली कंपनी एनएसओ और उसकी सहयोगी कंपनी Q साइबर टेक्नोलॉजीज़ लिमिटेड के ख़िलाफ़ मुकदमा दायर किया है। 2018 में फ़ेसबुक ने यह माना था कि उनके ग्रुप द्वारा व्हाट्सऐप और इंस्टाग्राम के डाटा को इन्टेग्रेट करके उसका व्यवसायिक इस्तेमाल किया जा रहा है साथ ही यह बात भी कही थी कि उसके प्लेटफ़ॉर्म में अनेक ऐप के माध्यम से डाटा माइनिंग का कारोबार होता है। कैंब्रिज एनालिटिका ने भी फेसबुक और सोशल मीडिया का इस्तेमाल करके भारत समेत कई देशों में लोकतांत्रिक प्रक्रिया को प्रभावित करने की कोशिश की। इन सबके बाद भी व्हाट्सऐप दावा कर रहा है कि उसके जरिए की गई कॉल, वीडियो कॉल, चैट, ग्रुप

चैट, इमेज, वीडियो, वॉइस मैसेज और फ़ाइल ट्रांसफ़र इंक्रिप्टेड होते हैं और पूरी तरह सुरक्षित भी होते हैं। कैलिफ़ोर्निया की कोर्ट में दाखिल केस के मुताबिक इज़रायली कंपनी ने मोबाइल फ़ोन के माध्यम से व्हाट्सऐप के सिस्टम को भी हैक कर लिया। इस सॉफ़्टवेयर के इस्तेमाल में एक मिस्ड कॉल के ज़रिए स्मार्ट फ़ोन के भीतर वायरस प्रवेश कर सभी जानकारी इकट्ठा कर लेता है। फ़ोन में लगा कैमरा इस बात की जानकारी देता है कि संबंधित व्यक्ति कहां जा रहा है किससे मिल रहा है और क्या बातें हो रही हैं?। इस तरह के क्राइम को सुलझाने का सिर्फ एक तरीका है, जिसका नाम है साइबर फॉरेंसिक।

शुरुआती जानकारी के मुताबिक एयरटेल, एमटीएनएल सहित देश के 8 मोबाइल नेटवर्क का खुफियागिरी के लिए प्रयोग किया गया। कोर्ट में दर्ज केस के मुताबिक इज़रायली कंपनी ने जनवरी 2018 से मई 2019 के बीच भारत समेत अनेक देशों के लोगों की जासूसी के काम को अंजाम दिया। लेकिन सबसे बड़ा सवाल है कि साइबर क्राइम के इस नए अपराध के तरीके पर कैसे रोक लगाई जाए। कैसे बिना जानकारी के आमलोगों के मोबाइल फोन में हो रही सेंधमारी को रोका जाए। साइबर सुरक्षा के क्षेत्र में काम कर रहे लोगों के लिए यह एक नई चुनौती किसी चक्रव्यूह के समान है, जिसे भेदना बेहद ज़रुरी है। न्यूज़ पेपर रिपोर्ट की माने तो NSO इज़रायली कंपनी है लेकिन इस पर मालिकाना हक यूरोप की एक प्राइवेट इक्विटी फ़र्म नोवाल्पिना कैपिटल एलएलपी ने फरवरी में ही हासिल कर लिया था। उसने NSO को करीब 100 करोड़ डॉलर में ख़रीद लिया था। बिज़नेस इन्साइडर की बैकी पीटरसन की रिपोर्ट के अनुसार एनएसओ ने पिछले साल 125 मिलियन डॉलर का लाभ कमाया था। अगर यह छोटी सी कंपनी अरबों का मुनाफा कमा रही है तो फेसबुक जैसी कंपनी डेटा बेचकर कितना कमा सकती है इसका महज अंदाजा ही लगाया जा सकता है। जिस काम में अरबों-खरबों का नफा-नुकसान जुड़ा हो वहां साइबर अपराध पर लगाम लगाना किसी चुनौती से कम नहीं है। अगर देश में खुफियागिरी के इस काम

को विदेशी या निजी कंपनी के जरिए किया गया है तो यह देश की सुरक्षा के लिए किसी गंभीर खतरे से कम नहीं है। कनाडा की यूनिवर्सिटी ऑफ़ टोरंटो की सिटीज़न लैब ने सितंबर, 2018 में ही व्हाट्सऐप में सेंधमारी की बात कही थी। यूनिवर्सिटी ऑफ़ टोरंटो की सिटीज़न लैब के मुताबिक 45 देशों में NSO के माध्यम से व्हाट्सऐप में सेंधमारी की गई।

साइबर जासूसी पर लगाम ज़रुरी

हमारे देश में 40 करोड़ से ज्यादा व्हाट्सऐप यूज़र हैं। साइबर क्राइम कितना खतरनाक है, इसका अंदाजा इस बात से लगा सकते हैं कि इज़राइली सॉफ्टवेर के माध्यम से फ़ोन को ट्रैक करके इस्तांबुल में सऊदी अरब के दूतावास में वाशिंगटन पोस्ट के पत्रकार जमाल खशोज्जी की हत्या कर दी गयी थी। दुनिया भर में दर्जनों कंपनिया डिजिटल या साइबर क्षेत्र में जासूसी का काम करती है। फ़ेसबुक जैसी कंपनियां अनेक एप्स और डाटा ब्रोकर्स के माध्यम से डेटा की खरीद-बिक्री और जासूसी जैसे जानलेवा काम को बढ़ावा देती हैं। देश में सोशल मीडिया कंपनियों के नियमन के लिए आईटी एक्ट में साल 2008 में व्यापक परिवर्तन किए गए हैं। साल 2009 और 2011 में अनेक इंटरमीडिटीयरी कंपनियों और डाटा सुरक्षा के लिए कई नियम बनाए गए। डिजिटल इंडिया के नाम पर कई इंटरनेट कंपनियां सही तरीके से नियम कायदों का पालन नहीं कर रही है। राष्ट्रीय सुरक्षा और अदालती हस्तक्षेप के बाद दिसंबर 2018 में इंटरमीडिटीयरी कंपनियों की जवाबदेही बढ़ाने के लिए ड्राफ़्ट नियम का मसौदा जारी किया। इन नियमों के लागू होने के साथ ही व्हाट्सऐप जैसी कंपनियों को हिंदुस्तान में अपना कार्यालय खोलने और नोडल अधिकारी को नियुक्त करने के साथ ही टैक्स भी चुकाना होगा।

केंद्रीय सूचना प्रौद्योगिकी मंत्रालय जनवरी 2020 से कुछ नए नियम जारी कर सकता है। इस नए नियम के दायरे में वह कंपनियां आएंगी, जो मैसेज भेजने के लिए लोगों को मंच मुहैय्या कराती है। इसमें सोशल मीडिया एप्स,

वेबसाइट्स और कई ई-कॉमर्स कंपनियां भी शामिल हैं। दरअसल इसका उद्देश्य सोशल मीडिया पर अफवाह या फ़ेक न्यूज़ पर लगाम लगाना है। सोशल मीडिया पर साल 2017 और 2018 के बीच 50 अफ़वाहें फैली और इसकी वजह से 40 से ज़्यादा लोगों को जान गंवानी पड़ी। साइबर फॉरेंसिक के जरिए फेक न्यूज़ फैलाने वालों की पहचान भी आसान हो जाती है। फेक न्यूज़ उसे कहते है, जो गलत तथ्यों, सूचना और जानकारियों पर आधारित होता है। इसका मकसद गलत सूचना के जरिए नफरत फैलाना होता है, जिसकी वजह से कई जगहों पर हिंसा भी भड़क उठती है। लिहाजा साइबर फॉरेंसिक आज के समय के लिए ज़रुरी ही नहीं बल्कि मजबूरी हो गई है।

पूरी दुनिया रियल से वर्चुअल वर्ल्ड की तरफ बढ़ती जा रही है। हर चीज अब ऑनलाइन होती जा रही है। ऑक्सीजन से लेकर बल्ड बैंक तक ऑनलाइन हो चुकी है। बैंकिंग, ई-कॉमर्स, ई-टिकट, ऑनलाइन परीक्षा से लेकर ऑनलाइन एजुकेशन तक सब कुछ इंटरनेट और कंप्यूटर पर आधारित हो चली है। लिहाजा साइबर फ्रॉड और ऑनलाइन क्राइम के मामले दिनोंदिन बढ़ते जा रहे हैं। वर्ष 2018 में तो एक सरकारी कर्मचारी ही भीड़ की हिंसा के शिकार हो गए थे, उन्हें सरकार ने गांवों में जाकर सोशल मीडिया पर फैलने वाली अफ़वाहों पर यक़ीन ना करने की घोषणा करने का काम दिया था। विगत दो साल के भीतर सोशल मीडिया से ग़लत जानकारी फैलने की वजह से भीड़ की हिंसा के 50 से अधिक मामले दर्ज हुए हैं। इन सोशल मीडिया एप्स में फ़ेसबुक, यूट्यूब, शेयरचैट और स्थानीय भाषाओं में चलने वाली अन्य एप्स शामिल हैं। लेकिन सबसे ज़्यादा फ़ेक न्यूज़ व्हाट्सऐप की वजह से फैली है। इस तरह के जितने भी मामले है उन सभी मामलों को सुलझाने में साइबर फॉरेंसिक विभाग की अहम भूमिका होती है।

व्हाट्सऐप की ओर से फेक न्यूज़ को लेकर उठाए गए कदम

- किसी मैसेज को फॉरवर्ड करने की लिमिट तय करना
- फॉरवर्ड मैसेज के ऊपर 'फॉरवर्ड' लिखकर बताना
- 20 लाख ऐसे अकाउंट्स को बैन किया है जो बल्क में मैसेज भेजते थे
- लोगों के लिए जागरुकता कार्यक्रम चलाना
- व्हाट्सऐप मैसेज या वीडियो के ओरिजनल सेंडर का पता लगाना (विचारार्थ)

सोशल मीडिया को लेकर अटर्नी जनरल ने सुप्रीम कोर्ट में कहा था, अगर ये सोशल मीडिया कंपनियां जांच एजेंसियों के साथ अपने डेटा को डीक्रिप्ट नहीं कर सकतीं, खासतौर पर तब जबकि वो मामले देशद्रोह, पोर्नोग्राफ़ी या अन्य अपराधों से जुड़ें हों तो इन्हें भारत में व्यापार करना ही नहीं चाहिए। उन्होंने यह भी बताया कि चीन में ऑनलाइन निगरानी का स्तर बहुत ज़्यादा है, वहां लोकप्रिय ऐप वीचैट पर कई बार वह शब्द अपने आप ग़ायब हो जाते हैं, जो प्रतिबंधित है। वर्ष 2011 से ही हिंदुस्तान के क़ानून ऑनलाइन प्लेटफॉर्म के लिए बेहद लचीले रहे हैं।

फ़ोन पर दो लोगों के बीच क्या बात हुई। इसके लिए किसी फ़ोन कंपनी को ज़िम्मेदार नहीं माना जाता। यहीं बात ई-मेल के मामले में लागू होती है। लेकिन सरकार के नए प्रस्तावित प्रावधान की वजह से कंपनियों को मुश्किलों का सामना करना पड़ सकता है। इसके अनुसार जिस भी प्लेटफ़ॉर्म पर देश में 50 लाख से ज़्यादा यूज़र्स होंगे, उन्हें भारत में दफ़्तर खोलना होगा। इसका मकसद उन्हें पहले से ज्यादा जिम्मेदार बनाना है। ऐसा करके सरकार सोशल मीडिया के अलावा दूसरे प्लेटफॉर्म को भी कड़ा संदेश देना चाह रही है।

साइबर हैकरों के तूफानी तेवर

प्राकृतिक आपदा से बचने के तरीकों के बारे में हर किसी को पता है। लेकिन इंटरनेट के जरिए तबाही फैलाने वाले साइबर तूफान से कैसे निपटा जाए, इसे लेकर साइबर फॉरेंसिक की दुनिया में उथल-पुथल मची हुई है। कुछ-कुछ दिनों पर साइबर तूफान दुनिया के किसी न किसी हिस्से में तबाही फैला रहे होते हैं। यह तूफान प्राकृतिक नहीं होता है। इसकी कमान साइबर हैकरों के हाथों में होती है। ऐसे ही एक तूफान का नाम है रीपर। यह मालवेयर अब तक पूरी दुनिया में करीब 20 लाख डिवाइस को अपना शिकार बना चुका है। यही नहीं यह रोजाना करीब 10 हजार डिवाइस को इनफेक्ट कर रहा है। इसकी वजह से महाराष्ट्र साइबर सेक्युरिटी को एडवाइजरी जारी कर लोगों को अपने डिवाइस वायरस से सुरक्षित कर लेने की सलाह देनी पड़ी। महाराष्ट्र सायबर सेक्युरिटी के आईजी बृजेश सिंह के मुताबिक ये अब तक का सबसे बड़े सायबर हमलों में से एक है। इसके पहले मिराई नाम का मालवेयर इसी तरह का हमला कर चुका है। आमलोगों की भाषा में कहें तो रीपर मालवेयर जोम्बी यानी किसी और के दिमाग से संचालित कंप्यूटर की ऐसी सेना तैयार कर रहा है जो कमांड मिलते ही हमला बोल देंगे। सायबर फॉरेंसिक की भाषा में इसे बोटनेट कहते हैं।

साइबर एक्सपर्ट प्रशांत माली के मुताबिक बोटनेट एक तरह का कंप्यूटर रोबोट है, जो अन्य सर्वर से जुड़े सीसीटीवी, डीवीआर और राउटर को अपने चपेट में लेकर चुपचाप पड़ा रहता है। इनफेक्टेड सभी उपकरण बिना किसी गड़बड़ी के पहले की तरह काम करते रहते हैं। लेकिन जैसे ही बोटनेट उन्हें कमांड देता है, वह आदेश के अनुसार निशाने पर दिए गए सिस्टम या सर्वर पर हमला कर देता है।

बोटनेट इस तरीके का साइबर हमला फिरौती के लिए या फिर सुपारी लेकर करता है। साइबर क्राइम का नेटवर्क अब लोकल नहीं ग्लोबल हो चुका है।

साइबर लुटेरे केवल पीसी या मोबाइल फोन को ही निशाना नहीं बना रहे हैं। दूर किसी तीसरे देश में बैठे साइबर लुटेरे सुरक्षा कैमरों और राउटर जैसे इंटरनेट से जुड़े डिवाइस को भी निशाना बना रहे हैं। इसकी वजह से इससे साइबर सुरक्षा से जुड़े जोखिम अब पहले से कहीं ज्यादा बढ़ गए हैं। एक अनुमान के मुताबिक दुनिया भर में रोजाना करीब 20 अरब छोटे-बड़े साइबर हमले होते रहते हैं।

इसके लिए अलग-अलग स्पाइवेयर और मालवेयर का इस्तेमाल किया जाता है। इन्हीं में से एक है पेगासस स्वाइवेयर, जिसका इस्तेमाल भारत में आम चुनाव के दौरान किया गया था। हलांकि वॉट्सऐप ने दावा किया कि उसने सभी संबंधित लोगों को सूचित कर दिया था कि उनके हैंडसेट की निगरानी की जा रही है। वॉट्सऐप का आरोप है कि इजरायली खुफिया समूह ने दुनिया भर में लगभग 1,400 वॉट्सऐप उपयोगकर्ताओं को निशाना बनाने के लिए 'पेगासस' स्पाइवेयर का इस्तेमाल किया। वॉट्सऐप के अनुसार 'पेगासस' सॉफ्टवेयर का इस्तेमाल आईओएस, एंड्रॉयड और ब्लैकबेरी ऑपरेटिंग सिस्टम पर चलने वाले स्मार्टफोन को हाईजैक करने के लिए किया गया था।

सोशल मीडिया की दिग्गज कंपनी वॉट्सऐप ने इस साल मई में अपने उपयोगकर्ताओं को ऐप को अपग्रेड करने के लिए कहा था, ताकि उस सुरक्षा संबंधी कमी को दूर किया जा सके जो ऐसे मालवेयर को स्मार्टफोन में प्रवेश करने देती है, जिसका इस्तेमाल जासूसी के लिए किया जा सकता है। बताया जा रहा है कि यह दुर्भावनापूर्ण कोड 29 अप्रैल से 10 मई तक वॉट्सऐप सर्वर के माध्यम से प्रसारित किया गया। पेगासस वॉट्सऐप पर मिस्ड वीडियो कॉल के जरिए भी स्मार्टफोन के भीतर घुसपैठ कर सकता है। यह बिना आपकी जानकारी के फोन खोल सकता है और स्पाइवेयर इंस्टॉल कर सकता है। पेगासस के जरिए हैकर पासवर्ड, संपर्क, कैलेंडर ईवेंट, टेक्स्ट संदेश और यहां तक कि मैसेजिंग ऐप्स पर वॉयस कॉल सहित

हर तरह के डेटा को एक्सेस कर सकता है। वॉट्सऐप भले ही अपने यूज़र्स को उनके मेसेजेस के पूरी तरह सुरक्षित होने का दावा करें लेकिन एंड-टू-एंड एनक्रिप्शन पूरी तरह नाकाम रहा। खासकर तब जब कोई व्यक्ति किसी के साथ बात ही नहीं कर रहा हो और एक मिस्ड कॉल के जरिए उसे निशाना बना लिया जाए, यह किसी भी स्तर पर बेहद खतरनाक है।

स्पाइवेयर ने कैसे निकाला तोड़?

ऐपल अपने यूज़र्स को ऑडियो और विडियो कॉल के लिए ऐसी ही फेसटाइम सर्विस देता है लेकिन वे कभी भी फेसटाइम कॉल्स को ऑफ कर सकते हैं। लेकिन वॉट्सऐप पर कॉल्स को डिसेबल करने का ऑप्शन नहीं है, जोकि बेहद खतरनाक है और मैलवेयर एवं स्पाइवेयर के लिए सेंध मारने के रास्ते खोल देता है। पेगासस मैलवेयर को बनाने वाली NSO ग्रुप लगभग नौ वर्ष पुरानी है, जो सर्विलांस टूल बनाती है। पेगासस भी इस कंपनी के सर्विलांस टूल्स में से एक है, जो आपके स्मार्टफोन को कंट्रोल कर सकता है। एनएसओ के मुताबिक यह टूल केवल सरकारी एजेंसियों के लिए बनाया गया है, जो अपराधियों व साइबर स्पेस पर आतंकियों को रोक सकता है। इस मैलवेयर के सामने आने के बाद वॉट्सऐप ने 13 मई को तुरंत अपडेट की घोषणा की थी। वॉट्सऐप के आरोप के अनुसार एनएसओ की वजह से उसकी प्रतिष्ठा को काफी नुकसान पहुंचा और उसे 75 हजार डॉलर, यानी करीब 54 लाख रुपये से अधिक का घाटा हुआ।

पड़ताल से हुआ खुलासा

जनवरी 2018 से मई 2019 के दौरान एनएसओ ने वॉट्सऐप पर यूज़र खाता खोला। अप्रैल और मई 2019 में उसने लक्ष्य किए गए मोबाइल नंबर वाले डिवाइस में मलिशस कोड भेजने के लिए यूज़र खाता का प्रयोग किया। वॉट्सऐप पर खाता खोलने के लिए अलग-अलग देशों में पंजीकृत नंबर का प्रयोग किया गया। उन देशों में साइप्रस, इजरायल, ब्राजील, इंडोनेशिया,

स्वीडन और नीदरलैंड का नाम शामिल हैं। पब्लिक रिपोर्ट के मुताबिक, एनएसओ के क्लाइंट्स में किंगडम ऑफ बहरीन, यूनाइटेड अरब अमीरात और मैक्सिको में सरकारी एजेंसियों समेत निजी संस्थाएं शामिल हैं। स्पाइवेयर तीन स्तर पर निगरानी करता है। इनिशल डेटा एक्ट्रैक्शन, पैसिव मॉनिटरिंग और ऐक्टिव कलेक्शन शामिल हैं। वॉट्सऐप के मुताबिक 'पेगासस को आईमेसेज, स्काइप, टेलिग्राम, वीचैट, फेसबुक मेसेंजर और वॉट्सऐप समेत अन्य पर होने वाले संदेशो के आदान-प्रदान को बाधित करने के लिए तैयार किया गया था। यह किसी भी हैंडसेट से भेजें और प्राप्त किए गए संदेशों पर नजर रखता था।

नहीं छोड़ता गुनाह के निशान

वॉट्सऐप का मानना है कि यह स्पाइवेयर निशाना बनाने वाले मोबाइल हैंडसेट पर कोई सबूत नहीं छोड़ता है। बैटरी, मेमोरी और डेटा की न्यूनतम खपत करता है और एक सेल्फ-डिस्ट्रक्ट ऑप्शन के साथ आता है, जिसे किसी भी समय प्रयोग किया जा सकता है। इसका उद्देश्य किसी भी तरह के सबूत को मिटाना होता है।

साइबर अपराध के प्रकार

प्रौद्योगिकी के नए आयाम की वजह से साइबर अपराध के अलग-अलग प्रकार देखने को मिल रहे हैं। उनमें से कुछ प्रमुख श्रेणी की सूची निम्नलिखित है।

निजी जानकारी चुराना या डेटा चोरी

इसे साधरण शब्दों में हैकिंग कहते हैं। इसके जरिये साइबर अपराधी आपके कंप्यूटर नेटवर्क में प्रवेश कर आपकी निजी जानकारी जैसे, नेट बैंकिंग पासवर्ड, क्रेडिट कार्ड की जानकारी चुरा लेते हैं। यह तरीका सबसे पुराना और साइबर अपराधियों के लिए कारगर है। किसी व्यक्ति, संस्थान या

संगठन आदि के किसी सिस्टम से निजी या गोपनीय डेटा या सूचनाओं की चोरी करना भी साइबर क्राइम है। अगर किसी संस्थान या संगठन के अंदरूनी डेटा तक आपकी पहुंच है, लेकिन आप अपनी उस जायज पहुंच का इस्तेमाल संगठन की इजाजत के बिना, उसके नाजायज दुरुपयोग की मंशा से करते हैं, तो वह भी इसी अपराध के दायरे में आएगा। कॉल सेंटरस् या लोगों की जानकारी रखने वाले संगठनों में इस तरह की चोरी के मामले सामने आते रहे हैं। ऐसे मामलों में आईटी (संशोधन) कानून 2008 की धारा 43 (बी), धारा 66 (ई), 67 (सी), आईपीसी की धारा 379, 405, 420 और कॉपीराइट कानून के तहत दोष साबित होने पर अपराध की गंभीरता के हिसाब से तीन साल तक की जेल या दो लाख रुपये तक जुर्माना हो सकता है।

हैकिंग

किसी कंप्यूटर, उपकरण, सूचना तंत्र या नेटवर्क में अनधिकृत तरीके से घुसपैठ करना और डेटा से छेड़छाड़ करना हैकिंग कहलाता है। यह हैकिंग उस सिस्टम की फिजिकल एक्सेस और रिमोट एक्सेस के जरिए भी हो सकती है। जरूरी नहीं कि ऐसी हैकिंग के दौरान उस सिस्टम को नुकसान पहुंचा ही हो, अगर कोई नुकसान नहीं भी हुआ है, तो भी घुसपैठ करना साइबर क्राइम के तहत आता है, जिसके लिए सजा का प्रावधान है। आईटी (संशोधन) एक्ट 2008 की धारा 43 (ए), धारा 66 - आईपीसी की धारा 379 और 406 के तहत अपराध साबित होने पर तीन साल तक की जेल या पांच लाख रुपये तक जुर्माना हो सकता है।

फिशिंग

यह शब्द साइबर क्राइम के जगत में काफी आम और मुख्य शब्द है। इसके जरिये आपको फर्जी मेल भेजकर ठगा जाता है। इसमें आपके पास कोई मेल आती है और आपसे कहा जाता है कि आपने यह इनाम जीता है इसके लिए बैंक से जुड़े डाटा भरे। इसके जरिये आदमी आनलाइन ठगी या फिसिंग का

शिकार होता है।

सॉफ्टवेयर पायरेसी

नकली साफ्टवेयर तैयार कर सस्ते दामों पर बेचना भी साइबर क्राइम में आता है। इसकी वजह से साफ्टवेयर कंपनियों को भारी नुकसान उठाना पड़ता है। पायरेसी का यह धंधा पूरी दुनिया को अपनी चपेट में ले चुका है।

सोशल साइट के जरिये अफवाह फैलाना

बहुत से लोग सोशल साइट पर सामाजिक, वैचारिक, धार्मिक और राजनीतिक अफवाह फैलाते हैं। इसको अन्य लोगों द्वारा फैलाया जाता है। इसी पर लगाम लगाने और संदिग्ध व्यक्ति के लिए भी साइबर फॉरेंसिक तकनीक का उपयोग किया जाता है। साइबर अपराध रोकने को लेकर सभी राज्यों की तरह झारखंड पुलिस भी काफी कोशिश कर रही है। साइबर अपराध से जुड़े मामलों में अनुसंधान के लिए अब हर जिले में साइबर फोरेंसिक लैब खोलने का प्रस्ताव विचाराधीन है। राज्य पुलिस का एकमात्र साइबर लैब वर्तमान में रांची के साइबर थाना परिसर में खोला गया है। राज्य पुलिस मुख्यालय को साइबर मामलों के नोडल अधिकारी आईजी नवीन कुमार सिंह ने सभी जिलों में साइबर फोरेंसिक लैब खोलने का प्रस्ताव तैयार कर भेजा था। राज्य में साइबर अपराध के अनुसंधान के लिए सभी जिलों में साइबर थाने खोलने की घोषणा डीजीपी डीके पांडेय ने भी की थी। वर्तमान में राज्य के छह जिलों में साइबर थाने चल रहे हैं। सभी साइबर फोरेंसिक लैब सीआईडी के अधीन होंगे। रांची की पहली अत्याधुनिक साइबर फोरेंसिक लैब के निर्माण पर 1.60 करोड़ खर्च किया गया है।

वायरस, स्पाईवेयर फैलाना

अक्सर कम्प्यूटर में आए वायरस और स्पाईवेयर को हटाने पर लोग ध्यान नहीं देते हैं। उनके सिस्टम से होते हुए ये वायरस दूसरों तक पहुंच जाते हैं।

हैकिंग, डाउनलोड, कंपनियों के अंदरूनी नेटवर्क, वाई-फाई कनेक्शनों और असुरक्षित फ्लैश ड्राइव, सीडी के जरिए भी वायरस फैल जाते हैं। वायरस बनाने वाले अपराधियों की पूरी एक इंडस्ट्री है, जिनके खिलाफ वक्त बेवक्त कड़ी कार्रवाई होती रही है। लेकिन आम लोग भी कानून के दायरे में आ सकते हैं। अगर उनकी लापरवाही से किसी के सिस्टम में कोई खतरनाक वायरस पहुंच जाए और बड़ा नुकसान कर दे। इस तरह के केस में आईटी (संशोधन) एक्ट 2008 की धारा 43 (सी), धारा 66, आईपीसी की धारा 268 और देश की सुरक्षा को खतरा पहुंचाने के लिए फैलाए गए वायरस पर साइबर आतंकवाद से जुड़ी धारा 66 (एफ) भी लगाई जाती है। दोष सिद्ध होने पर साइबर-वॉर और साइबर आतंकवाद से जुड़े मामलों में उम्र कैद का प्रावधान है। जबकि अन्य मामलों में तीन साल तक की जेल या जुर्माना हो सकता है।

पहचान की चोरी

किसी दूसरे शख्स की पहचान से जुड़े डेटा, गुप्त सूचनाओं वगैरह का इस्तेमाल करना भी साइबर अपराध है। यदि कोई इंसान दूसरों के क्रेडिट कार्ड नंबर, पासपोर्ट नंबर, आधार नंबर, डिजिटल आईडी कार्ड, ई-कॉमर्स ट्रांजैक्शन पासवर्ड, इलेक्ट्रॉनिक सिग्नेचर वगैरह का इस्तेमाल करके शॉपिंग या धन की निकासी करता है तो वह इस अपराध में शामिल हो जाता है। जब आप किसी दूसरे शख्स के नाम पर या उसकी पहचान का आभास देते हुए कोई जुर्म करते हैं, या उसका नाजायज फायदा उठाते हैं, तो यह जुर्म आइडेंटिटी थेफ्ट के दायरे में आता है। ऐसा करने वाले पर आईटी (संशोधन) एक्ट 2008 की धारा 43, 66 (सी), आईपीसी की धारा 419 लगाए जाने का प्रावधान है, जिसमे दोष साबित होने पर तीन साल तक की जेल या एक लाख रुपये तक जुर्माना हो सकता है।

ई-मेल स्पूफिंग और फ्रॉड

अक्सर आपके इनबॉक्स या स्पैम बॉक्स में कई तरह के इनाम देने वाले या बिजनेस पार्टनर बनाने वाले या फिर लॉटरी निकलने वाले मेल आते हैं। ये सभी मेल किसी दूसरे शख्स के ई-मेल या फर्जी ई-मेल आईडी के जरिए किए जाते हैं। किसी दूसरे के ई-मेल पते का इस्तेमाल करते हुए गलत मकसद से दूसरों को ई-मेल भेजना इसी अपराध की श्रेणी में आता है। हैकिंग, फिशिंग, स्पैम और वायरस, स्पाईवेयर फैलाने के लिए इस तरह के फर्जी ईमेल का इस्तेमाल अधिक होता है। ऐसा काम करने वाले अपराधियों का मकसद ई-मेल पाने वाले को धोखा देकर उसकी गोपनीय जानकारी हासिल करना होता है। ऐसी जानकारियों में बैंक खाता नंबर, क्रेडिट कार्ड नंबर, ई-कॉमर्स साइट का पासवर्ड वगैरह आ सकते हैं। इस तरह के मामलों में आईटी कानून 2000 की धारा 77 बी, आईटी (संशोधन) कानून 2008 की धारा 66 डी, आईपीसी की धारा 417, 419, 420 और 465 लगाए जाने का प्रावधान है। दोष साबित होने पर तीन साल तक की जेल या जुर्माना हो सकता है।

पोर्नोग्राफी

इंटरनेट के माध्यम से अश्लीलता का व्यापार भी खूब फलफूल रहा है। ऐसे में पोर्नोग्राफी एक बड़ा कारोबार बन गई है, जिसके दायरे में ऐसे फोटो, विडियो, टेक्स्ट, ऑडियो और सामग्री आती है, जो यौन, यौन कृत्यों और नग्नता पर आधारित हो। ऐसी सामग्री को इलेक्ट्रॉनिक ढंग से प्रकाशित करने, किसी को भेजने या किसी और के जरिए प्रकाशित करवाने या भिजवाने पर पोर्नोग्राफी निरोधक कानून लागू होता है। दूसरों के नग्न या अश्लील वीडियो तैयार करने वाले या ऐसा एमएमएस बनाने वाले या इलेक्ट्रॉनिक माध्यमों से इन्हे दूसरों तक पहुंचाने वाले और किसी को उसकी मर्जी के खिलाफ अश्लील संदेश भेजने वाले लोग इसी कानून के दायरे में आते हैं। पोर्नोग्राफी प्रकाशित करना और इलेक्ट्रॉनिक जरियों से दूसरों तक पहुंचाना अवैध है। लेकिन उसे

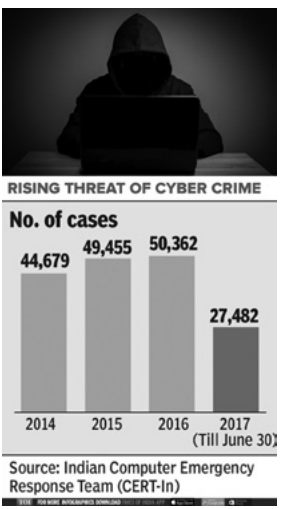
देखना, पढ़ना या सुनना अवैध नहीं माना जाता, जबकि चाइल्ड पोर्नोग्राफी देखना भी अवैध माना जाता है। इसके तहत आने वाले मामलों में आईटी (संशोधन) कानून 2008 की धारा 67 (ए), आईपीसी की धारा 292, 293, 294, 500, 506 और 509 के तहत सजा का प्रावधान है। जुर्म की गंभीरता के लिहाज से पहली गलती पर पांच साल तक की जेल या दस लाख रुपये तक जुर्माना हो सकता है लेकिन दूसरी बार गलती करने पर जेल की सजा 7 साल तक बढ़ सकती है।

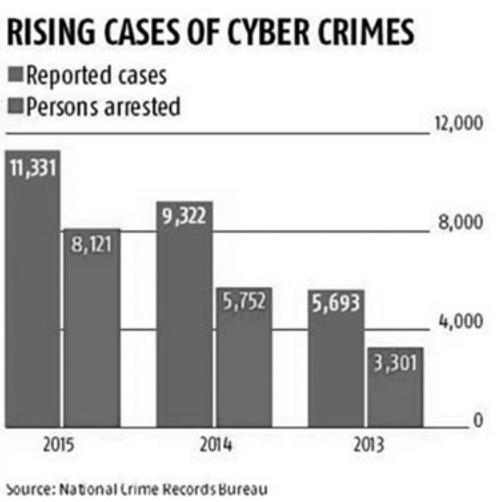
चाइल्ड पोर्नोग्राफी

बच्चों के साथ पेश आने वाले मामलों पर कानून और भी ज्यादा सख्त है। बच्चों को सेक्सुअल एक्ट में शामिल करना या नग्न दिखाना या इलेक्ट्रॉनिक फॉर्मेट में कोई सामग्री प्रकाशित करना या दूसरों को भेजना भी इसी कानून के तहत आता है। बल्कि भारतीय कानून के मुताबिक जो लोग बच्चों से जुड़ी अश्लील सामग्री तैयार करते हैं, इकट्ठी करते हैं, ढूंढते हैं, देखते हैं, डाउनलोड करते हैं, विज्ञापन देते हैं, प्रमोट करते हैं, दूसरों के साथ लेनदेन करते हैं या बांटते हैं तो वह भी गैरकानूनी माना जाता है। बच्चों को बहला-फुसलाकर ऑनलाइन संबंधों के लिए तैयार करना, फिर उनके साथ यौन संबंध बनाना या बच्चों से जुड़ी यौन गतिविधियों को रेकॉर्ड करना, एमएमएस बनाना, दूसरों को भेजना आदि भी इसी के तहत आते हैं। इस कानून में 18 साल से कम उम्र के लोगों को बच्चों की श्रेणी में माना जाता है। ऐसे मामलों में आईटी (संशोधन) कानून 2009 की धारा 67 (बी), आईपीसी की धाराएं 292, 293, 294, 500, 506 और 509 के तहत सजा का प्रावधान है। पहले अपराध पर पांच साल की जेल या दस लाख रुपये तक जुर्माना हो सकता है। लेकिन दूसरे अपराध पर सात साल तक की जेल या दस लाख रुपये तक जुर्माना हो सकता है।

बच्चों और महिलाओं को तंग करना

आज के दौर में सोशल नेटवर्किंग साइट्स की लोकप्रियता अपने चरम पर हैं। ऐसे में सोशल नेटवर्किंग वेबसाइटों, ई-मेल, चैट वगैरह के जरिए बच्चों या महिलाओं को तंग करने के मामले सामने आते रहते हैं। इन आधुनिक तरीकों से किसी को अश्लील या धमकाने वाले संदेश भेजना या किसी भी रूप में परेशान करना साइबर अपराध के दायरे में ही आता है। किसी के खिलाफ दुर्भावना से अफवाहें फैलाना, नफरत फैलाना या बदनाम करना भी इसी श्रेणी का अपराध है। इस तरह के केस में आईटी (संशोधन) कानून 2009 की धारा 66 (ए) के तहत सजा का प्रावधान है। दोष साबित होने पर 3 साल तक की जेल या जुर्माना हो सकता है।





साइबर अपराध के लिए कारगर कानून की ज़रुरत

हमारे देश में टेलीफ़ोन टैपिंग पर सख़्त क़ानून है लेकिन डिजिटल सेंधमारी या साइबर क्राइम को लेकर अभी और कठोर कानून बनाए जाने की ज़रुरत महसूस होने लगी है। हिंदुस्तान में टेलीग्राफ़ क़ानून के जरिए परंपरागत संचार

व्यवस्था को संचालित और नियंत्रित किया जाता है। सर्वोच्च न्यायालय ने भी PUCL मामले में अहम फ़ैसला देकर टेलीफ़ोन टैपिंग को लेकर कठोर कानूनी प्रावधान की व्यवस्था बनाई है। लेकिन व्हाट्सऐप में सेंधमारी केस के सामने आने के बाद मोबाइल और इंटरनेट की नई व्यवस्था में पुराने कानून अब कारगर नहीं रह गए हैं। सुप्रीम कोर्ट के 9 जजों की बेंच में पुट्टास्वामी मामले में निजता के अधिकार को संविधान के अनुच्छेद 21 के तहत जीवन का अधिकार माना गया। ऐसे में व्हाट्सऐप और फ़ेसबुक करोड़ों लोगों के निजी जानकारी से संबंधित डेटा को लेकर लापरवाही भरा कदम कैसे उठा सकती है। हाल के दिनों में सोशल मीडिया और साइबर अपराध के बढ़ते मामलों को देखते हुए सुप्रीम कोर्ट ने सोशल मीडिया कंपनियों के मामलों को एक जगह स्थानांतरित करके जनवरी, 2020 में सुनवाई करने का आदेश दिया है।

साइबर अपराध संबंधी कानून

दुनिया के दूसरे हिस्सों की तरह भारत में भी साइबर अपराध के मामलों में तेजी से बढ़ोतरी हो रही है। सरकार साइबर अपराध के बढ़ते मामलों को लेकर बेहद गंभीर है। देश में साइबर अपराध के मामलों में सूचना तकनीक कानून 2000 और सूचना तकनीक (संशोधन) कानून 2008 को लागू किया जाता है। लेकिन इसी कैटगरी के कई मामलों में भारतीय दंड संहिता (आईपीसी), कॉपीराइट कानून 1957, कंपनी कानून, सरकारी गोपनीयता कानून और यहां तक कि आतंकवाद निरोधक कानून के अंन्तर्गत भी कार्रवाई की जाती है या की जा सकती है।

कई मामलों में लागू होता है आईटी कानून

साइबर क्राइम के कुछ मामलों में आईटी विभाग की तरफ से जारी किए गए आईटी नियम 2011 के तहत भी कार्रवाई की जाती है। इस कानून में निर्दोष लोगों को साजिशों से बचाने के प्रावधान भी हैं। लेकिन कंप्यूटर, इंटरनेट

और दूरसंचार इस्तेमाल करने वालों को हमेशा सतर्क रहना चाहिए कि उनसे जाने-अनजाने में कोई साइबर क्राइम तो नहीं हो रहा है।

साइबर फॉरेंसिक क्राइम से जुड़ी चुनौतियां और पुलिस की तैयारी

इंटरनेट के बढ़ते प्रसार के साथ-साथ विश्व स्तर पर तकनीक पर बढ़ती निर्भरता के साथ-साथ साइबर अपराध का खतरा भी बढ़ गया है। इन साइबर खतरों से निपटने के लिए तैयारी के रूप में सूचना प्रौद्योगिकी विभाग ने ई.आर.नेट इंडिया को निधि उपलब्ध कराई, जिससे सी.बी.आई.एकेडमी में अपनी तरह का एक पहला साइबर फॉरेंसिक लैब स्थापित किया गया। इस प्रोजेक्ट के तहत सी.बी.आई. के अधिकारियों को उच्च गुणवत्ता वाली कंप्यूटर फॉरेंसिक ट्रेनिंग दी गई। इस फॉरेंसिक लैब में उन्नत फॉरेंसिक टूल्स लगाए गए हैं, जिसमें डिजिटल उपकरणों, जैसे कंप्यूटर, लैपटॉप, मोबाइल फोन, सैटेलाइट फोन और जीपीएस (ग्लोबल पोजिशनिंग सिस्टम) के सहारे ई-एविडेंस को एकत्र करने और घटनाओं की क्रमवार जानकारी जुटाने में काफी उपयोगी है। इससे जो जानकारी और सबूत उत्पन्न होंगे उनसे साइबर अपराधों की मॉनिटरिंग और ट्रेकिंग करने में सहायता मिल सकेगी। लैब में साइबर फॉरेंसिक विश्लेषण और प्रक्रिया पर प्रशिक्षण देने और साइबर अपराध गतिविधियों के बारे में तकनीक के माध्यम से साक्ष्य जुटाने की सुविधा भी है। इस प्रोजेक्ट का एक मुख्य उद्देश्य पूरे देश में आपराधिक जांच में लगे स्टाफ को प्रशिक्षण देना, उन्हें साइबर अपराध जांच के तरीकों से अवगत कराना भी है ताकि वे साइबर कानून और साइबर जांच और साक्ष्य की कड़ियों के प्रबंधन की जटिलताओं के बारे में जानकारी प्राप्त कर सकें। इस प्रोजेक्ट की सबसे बड़ी चुनौती न केवल साइबर फॉरेंसिक लैब स्थापित करना है बल्कि जांचकर्ताओं को फॉरेंसिक उपकरणों के प्रभावी उपयोग के लिए अपेक्षित कौशल प्रदान करना है।

क्या होती है फॉरेंसिक लैब?

साइबर फॉरेंसिक लैब में मोबाइल फोन फॉरेंसिक लैब होगी। इसके जरिए किसी भी मोबाइल से डिलीट किए गए डाटा, तस्वीर, चैट व तमाम चीजों को दोबारा इंस्टाल किया जा सकेगा। टू इमेजर मशीन के माध्यम से किसी भी घटनास्थल से जब्त डिस्क, मोबाइल या दूसरे उपकरण टू इमेज व सारी जानकारी ली जाएगी। डिस्क फॉरेंसिक उपकरण से किसी भी कंप्यूटर या लैपटाप की डिस्क से डिलीट डाटा इंस्टाल किया जा सकता है। इसके अलावा डीवीआर एनेलाइजर मशीन के माध्यम से धुंधली तस्वीर या गाड़ियों के नंबर प्लेट को साफ कर चिन्हित किया जाएगा। किसी भी पासवर्ड को तोड़ने के लिए पासवर्ड क्रैकिंग टूल जैसे उपकरण लैब में रहेंगे। एफएसएल (फारेंसिक साइंस लेबोरेट्री) में रक्त, बंदूक आदि की जांच की जाती है, ठीक उसी तरह साइबर फारेंसिक लैब भी काम करेगा। साइबर अपराध से जुड़ी हर तरह की जांच अब फारेंसिक लैब में होगी।

पहले अपराधियों द्वारा प्रयोग किए जाने वाले मोबाइल, लैपटाप या पैनकार्ड का डिलीट रिपोर्ट को निकालने के लिए बाहर भेजा जाता था। फारेंसिक लैब बनने से इस तरह के काम में आसानी होगी। केंद्रीय कार्मिक राज्य मंत्री जितेंद्र सिंह ने कहा कि साइबर अपराध का अध्ययन भारत के लिए बहुत ही महत्वपूर्ण है, क्योंकि यह बड़ी आबादी वाला देश है तथा यहां विश्व में दूसरे स्थान पर सबसे ज्यादा इंटरनेट उपभोक्ता हैं। विश्वभर में फिलहाल साइबर अपराध की घटनाएं बढ़ती जा रही हैं। राज्यों में महिला और बच्चों के खिलाफ 'साइबर अपराध रोकथाम प्रोजेक्ट' के तहत साइबर फॉरेंसिक लैबोरेट्री और साइबर फॉरेंसिक प्रशिक्षण सुविधाएं उपलब्ध कराई गई है। अरुणाचल प्रदेश, हिमाचल प्रदेश, मध्य प्रदेश, तेलंगाना और उत्तराखंड समेत पांच राज्यों में साइबर फॉरेंसिक लैबोरेट्री पहले से बनी हुई हैं। प्रोजेक्ट के अंतर्गत 410 सरकारी अभियोजकों समेत 3664 कर्मचारियों को प्रशिक्षण दिया गया है। आपको बता दें कि यह कार्य महिला सुरक्षा सुधारने के

मकसद से निर्भया फंड के तहत हो रहा है। इस प्रोजेक्ट की समीक्षा और निगरानी का जिम्मा एक एम्पावर्ड समिति के पास है। राष्ट्रीय अपराध रिकॉर्ड ब्यूरो के मुताबिक 2016 में 12,187 साइबर अपराध दर्ज हुए थे, यह आंकड़ा 2015 से 6.3 फीसदी ज्यादा था, जबकि 2015 में 2014 के मुकाबले साढ़े 20 फीसदी की बढ़ोतरी हुई थी। देश के अलग अलग फॉरेंसिक लैब में उन्नत फॉरेंसिक टूल्स लगाए गए हैं, जिसमें डिजिटल उपकरणों, जैसे कंप्यूटर, लैपटॉप, मोबाइल फोन, सैटेलाइट फोन और जीपीएस (ग्लोबल पोजिशनिंग सिस्टम) के सहारे ई-एविडेंस को एकत्र करने और घटनाओं की क्रमवार जानकारी जुटाने में उपयोगी होंगे। इससे जो जानकारी और सबूत उत्पन्न होंगे उनसे साइबर अपराधों की मॉनिटरिंग और ट्रेकिंग करने में सहायता मिल सकेगी। लैब में साइबर फॉरेंसिक विश्लेषण और प्रक्रिया पर प्रशिक्षण देने और साइबर अपराध गतिविधियों के बारे में तकनीक के माध्यम से साक्ष्य जुटाने की सुविधा भी है। इस प्रोजेक्ट का एक मुख्य उद्देश्य पूरे देश में आपराधिक जांच में लगे स्टाफ को प्रशिक्षण देना, उन्हें साइबर अपराध जांच के तरीकों से अवगत कराना भी है ताकि वे साइबर कानून और साइबर जांच और साक्ष्य की कड़ियों के प्रबंधन की जटिलताओं के बारे में जानकारी प्राप्त कर सकें। इस प्रोजेक्ट की सबसे बड़ी चुनौती न केवल साइबर फॉरेंसिक लैब स्थापित करना है बल्कि जांचकर्ताओं को फॉरेंसिक उपकरणों के प्रभावी उपयोग के लिए अपेक्षित कौशल प्रदान करना है।

साइबर फॉरेंसिक लैब की संरचना

साइबर फोरेंसिक लैब संचालन के लिए फोरेंसिक कंसल्टेंट की बहाली होगी। एक चीफ टेक्निकल अफसर, एक टेक्निकल अफसर की भी बहाली होगी। हर राज्य के साइबर फोरेंसिक लैब में काम करने के लिए ज़रुरत के हिसाब से करीब 400 सिपाहियों का चयन किया जाएगा। ये सिपाही टेक्निकल बैकग्राउंड के होंगे। अधिकारियों के मुताबिक, रोटेशन के तहत इन पुलिसकर्मियों को साइबर फोरेंसिक लैब में ड्यूटी पर लगाया जाएगा।

लैब में क्या कुछ नया होगा

मोबाइल फोन फोरेंसिक मशीन लैब में होगा। इसके जरिए किसी भी मोबाइल से डिलीट किए डाटा, तस्वीर, चैट व तमाम चीजों को दुबारा इंस्टॉल किया जा सकेगा। डिस्क फोरेंसिक उपकरण के जरिए किसी कंप्यूटर या लैपटॉप के डिस्क से डिलीट किए गए डाटा को इंस्टॉल किया जा सकेगा। ट्रू इमेजर मशीन की खरीद भी होगी। इस मशीन से किसी भी घटनास्थल से जब्त डिस्क, मोबाइल या दूसरे उपकरण की ट्रू इमेज व सारी जानकारी ली जाएगी। हाई एंड फोरेंसिक सर्वर तकरीबन 128 आरएएम का कंप्यूटर होगा, जिसपर लैब की गतिविधियां ऑपरेट होंगी। डीवीआर एनेलाइजर के जरिए धुंधली तस्वीर या गाड़ियों के नंबर प्लेट को साफ कर चिह्नित किया जाएगा। किसी भी पासवर्ड को तोड़ने के लिए पासवर्ड क्रैकिंग टूल की खरीद होगी। साइबर क्राइम से लड़ने के लिए लेकर विभिन्न तकनीकी कॉलेजों में साइबर क्राइम पर छात्रों को अपग्रेड किया जा रहा है। छात्रों के बीच लगातार विशेषज्ञों को बुलाया जा रहा है, जो उन्हें साइबर क्राइम के शिकार होने से बचने के तरह-तरह के टिप्स बता रहे हैं। साइबर सुरक्षा को लेकर बीआईटी, सीयूजे, एक्सआईएसएस से लेकर अन्य विश्वविद्यालयों में कार्यशाला का आयोजन किया जा रहा है।

साइबर फॉरेंसिक में एक जांच के तकनीकी पहलू को कई उप शाखाओं में बांटा गया है। जैसे की कंप्यूटर फॉरेंसिक, नेटवर्क फॉरेंसिक, फोरेंसिक डेटा विश्लेषण और मोबाइल यंत्र फोरेंसिक। फोरेंसिक प्रक्रिया में जब्ती, फॉरेंसिक इमेजिंग (अधिग्रहण) और डिजिटल मीडिया का विश्लेषण और एकत्र साक्ष्य में एक रिपोर्ट का उत्पादन शामिल हैं।

कंप्यूटर फॉरेंसिक

कंप्यूटर फॉरेंसिक मे जो कंप्यूटर मे जानकारी जमा है उसका विश्लेषण करना या कंप्यूटर से जुड़ा कोई भी अपराध हुआ हो। कंप्यूटर की चोरी होना या

उसमे जानकारी की चोरी होना कंप्यूटर फॉरेंसिक मै आता है।

नेटवर्क फॉरेंसिक

नेटवर्क फॉरेंसिक या साइबर फॉरेंसिक जो अपराध नेटवर्क या इन्टरनेट से किया हो। इतना ही नही नेटवर्क से ओरों पर निगरानी भी रखी जा सकती है।

फॉरेंसिक डेटा विश्लेषण

यह खोजने के लिए और धोखाधड़ी, वित्तीय अपराध से उत्पन्न गतिविधियों के पैटर्न का विश्लेषण करने के उद्देश्य से संरचित डेटा की परख होती है।

मोबाइल यंत्र फॉरेंसिक

किसी भी अपराधिक स्थान पर पाये गए मोबाइल से जानकारी प्राप्त हो सकती है की वह किसका मोबाइल है और उसके भीतर क्या जानकारी जमा करके रखी गई है। मोबाइल से यह भी मालूम किया जा सकता है कि इस नंबर से किस समय पर किन-किन लोगों से संपर्क किया गया और किन लोगों ने उस नंबर पर फोन किया और कितने देर तक बात की। इसके अलावा फॉरेंसिक साइंस के जरिए मोबाइल से डिलिट किए संदेशों के बारे में भी पता किया जा सकता है।

पुलिस बताएगी कैसे बचें साइबर ठग से

साइबर सुरक्षा को लेकर विशेषज्ञ साइबर ठगी के बारे में बताएंगे। साथ ही डेबिट और क्रेडिट कार्ड के सही तरीके के इस्तमाल के बारे में बताएंगे। इसके अलावा कार्ड क्लोनिंग को लेकर भी लोगों को जागरुक किया जाएगा। हाल ही में हुई कार्ड क्लोनिंग की कई घटनाओं को लेकर विशेषज्ञ अपनी राय देंगे। साथ ही यह बताएंगे कि कैसे कार्ड स्वैप करने से पहले हर चीजों की बारीकी से जांच करनी चाहिए।

फिल्म 'ए वेडनेसडे' में आम आदमी का किरदार निभा रहे नसीरुद्दीन शाह मुंबई पुलिस कमिश्नर प्रकाश राठौर (अनुपम खेर) को फोन कर धमकी देते हैं। ये फोन कहां से और किस नंबर से किया गया, इसका पता पुलिस महकमे की साइबर विंग लाख कोशिश करने के बाद भी नहीं लगा पाती है। इसी काम को एक सोलह साल का लड़का पलक झपकते कर देता है। डिजिटल इंडिया की ओर बढ़ता देश अब ऐसी ही स्थिति से बचने के लिए हर मुमकिन कोशिश करने में जुटा है। मौजूदा दौर में मेट्रो ट्रेन से लेकर एयरपोर्ट, न्यूक्लियर पावर प्लांट, बैंकिंग और ट्रांसपोर्ट, ये सभी सेक्टर इंटरनेट या डिजिटल तरीके से संचालित किए जा रहे हैं। इनका सर्वर हैक कर बड़ी वारदात को अंजाम दिया जा सकता है। ऐसे ही हैकर्स को मात देने के लिए सरकार अपने हैकर्स की टीम बनाने की तैयारी में है। एथिकल हैकर्स की ये टीम सरकार को बताएगी कि उनके सर्वर को हैकर्स तबाही मचाने के इरादे से किन-किन तरीकों से हैक कर सकते हैं। इसी के आधार पर असली सर्वर को और सुरक्षित बनाया जाएगा। इस काम की जिम्मेदारी नेशनल क्रिटिकल इन्फॉर्मेशन इन्फ्रास्ट्रक्चर प्रोटेक्शन सेंटर (NCIIPC) के कंधों पर है।

भारत समेत दुनिया भर में कई साइबर अटैक हुए। 'वानाक्राई रैनसमवेयर' जैसे वायरस ने दुनिया को अपनी चपेट में ले लिया। इस साइबर अटैक के चलते भारत के सबसे बड़े मुंबई स्थित कंटेनर पोर्ट जवाहर लाल नेहरू पोर्ट ट्रस्ट (JNPT) समेत दुनिया की 20 बड़ी कंपनियों का कामकाज ठप हो गया। ऐसे साइबर हमलों से कैसे बचा जाए। आइए एक नज़र डालते हैं।

1. यह वायरस घर पर कंप्यूटर का इस्तेमाल करने वालों पर इसका असर कम ही होगा। वानाक्राई ने बिना अपटेड किए गए विंडोज़ के ज़रिए बिज़नेस नेटवर्क को अपना निशाना बनाया। घर में विंडोज़ इस्तेमाल करने वालों के लिए इसका ख़तरा नहीं होगा।

2. ऑफिस या इंस्टीट्यूट जो भी इस रैनसमवेयर की चपेट में आए हैं और

जिनके पास अनलॉक की गई फाइलों का बैकअप कंप्यूटर से अलग किसी ड्राइव में नहीं है तो दुर्भाग्य से अब वो उन्हें खो चुके है। इसीलिए फाइलों का किसी अलग ड्राइव या मशीन में बैकअप होना जरुरी होता है। अगर वानाक्राई आपके कंप्यूटर में है तो इसे हटाना संभव है। हालांकि प्रक्रिया सरल नहीं है।

3. एक टेक्निकल सपोर्ट वेबसाइट ब्लीपिंग कंप्यूटर के अनुसार, कंप्यूटर से इस वायरस को साफ करने के लिए कुछ प्रोग्राम डाउनलोड करने पड़ते हैं।

4. इंटरनेट पर गिफ्ट, ऑफर, सेक्स वीडियो, गेमिंग आदि के लिंक के जरिए हैकर्स इस वायरस को कंप्यूटर में डालकर सिस्टम को हैक कर लेते हैं। एक बार हैकिंग के बाद इससे छुटकारा पाना संभव नहीं है।

5. इस अटैक से बचने के लिए अपने ऑनलाइन अकाउंट के लिए ऐसे पासवर्ड बनाए जिन्हें डिकोड करना मुश्किल हो।

6. अगर आप पुराने विडोंज ऑपरेटिंग सिस्टम जैसे XP, 8 या विस्टा का उपयोग कर रहे हों तो उसे अपडेट कर लें। माइक्रोसाफ्ट ने विशेष सिक्योंरिटी पैच जारी किए हैं।

7. सुरक्षा विशेषज्ञों का कहना है कि किसी भी तरह के मेल के साथ आने वाले रार, जीप या इस तरह के कंप्रेश फाइल को खोलने से पहले सुनिश्चित कर लें कि यह सही हैं। अनजाने मेल या लॉटरी से संबंधित मेल को किसी भी तरह खोलने की कोशिश न करें।

8. अपने सिस्टम में एंटी वायरस, एंटी फिशिंग, एंटी मालवेयर को तत्काल अपडेट कर लें। अंतिम सुझाव फिर से कि किसी भी अनजाने मेल या किसी वेबसाइट के अनजाने लिंक को खोलने से पहले सौ बार सोचें।

9. जिस कंप्यूटर पर एक से ज्यादा यूज़र बैठते हैं, उसका इस्तेमाल ना करें। इसके अलावा पब्लिक वाई-फाई का इस्तेमाल भी ना करें, तो बेहतर होगा।

10. आमतौर पर कई मालवेयर, जिन्हें हम अक्सर वायरस कहते हैं, आपके कंप्यूटर में गलत तरीके से घुस जाते हैं। अक्सर इनका उद्देश्य या तो आपके कंप्यूटर के डाटा को चुराना होता है या फिर उसे मिटाना होता है। लेकिन रैनसमवेयर आपके सिस्टम में आकर आपके डाटा को 'इनक्रिप्ट' यानी लॉक कर देता है. यूज़र तब तक इसमें मौजूद डेटा तक नहीं पहुंच पाता जब तक कि वह इसे 'अनलॉक' करने के लिए रैनसम यानी फिरौती नहीं देता। ये मालवेयर ईमेल के जरिए फैलता है।

पुलिस ट्विटर व अन्य सोशल मीडिया के माध्यम से लोगों को जागरुक कर रही है कि वे अपना बैंक अकाउंट नंबर, आधार कार्ड, पैन कार्ड की डिटेल किसी अनजान को न दें। इसके अलावा पुलिस ने साइबर हेल्प लाइन नंबर 9820810007 भी जारी किया हुआ है।

साइबर अटैक का सबसे ज्यादा असर यूक्रेन में हुआ, जहां सरकारी मंत्रालयों, बिजली कंपनियों और बैंक के कंप्यूटर सिस्टम में बड़ी खराबी आई। दुनिया भर में साइबर हमले की चपेट में आई कंपनी एपी मॉलर-मैर्स्क (AP Moller-Maersk) ही भारत में JNPT पर गेटवे टर्मिनल्स इंडिया (GTI) का संचालन करती है, जिसकी क्षमता 18 लाख स्टैंडर्ड कन्टेनर यूनिट की है। यूक्रेन का सेंट्रल बैंक, सरकारी बिजली वितरक कंपनी, विमान निर्माता कंपनी एंतोनोव और डाक सेवाएं बुरी तरह प्रभावित हुई थी। यूक्रेन की राजधानी कीव की मेट्रो में पेमेंट कार्ड काम नहीं कर रहे थे।

फॉरेंसिक साइंस का क्रेज

फॉरेंसिक साइंस अब विदेश में ही नहीं, देश में भी लोकप्रिय हुई है। इस

क्षेत्र में बढ़ती नौकरियों ने स्टूडेंट्स को फॉरेंसिक साइंस का कोर्स करने के लिए विवश कर दिया है। इसकी पढ़ाई करने वालों के लिए जॉब के कई विकल्प हैं। यही कारण है कि अपराध का पता लगाने वाले इस विज्ञान का क्रेज बढ़ता जा रहा है। इस फील्ड के लोग ब्लड सहित शरीर के अन्य तरल पदार्थों की जांच कर अपराधियों तक पहुंचने में मददगार साबित होते हैं।

विश्लेषणात्मक आवश्यकताओं के अनुसार किसी मामले के साक्ष्यों को प्रयोगशालाओं के एक या अधिक खंडों में जांचा जाता है। विभिन्न खंडों में किस तरह की प्रकृति की जाँचें की जा सकती हैं वह इस प्रकार हैं :

भौतिकी खंड : पेंट, शीशे, मिट्टी, रस्सी, धागे, बिजली के तार, कपड़े, लॉटरी टिकट, मुहर इत्यादि की भौतिक जांच; औजारों के निशान की तुलना, मिटाये गए पहचान नंबर / अंकों को पूर्व की अवस्था में लाना, दुर्घटनावश टूटे टुकड़ों को जोड़ कर स्रोत का पता करना, प्रहार की दिशा पता करने के लिए शीशे के टूटे टुकड़ों की जांच, नकली नोटों की जांच, तुलना के लिए तत्वों का पता लगाने का विश्लेषण और साक्ष्यों की शिनाख्त।

दस्तावेज़ खंड : प्रामाणिकता या जाल-साजी को सिद्ध करने के लिए ज्ञात मानकों पर सवालिया लेखन, टाइपराइटिंग, मुद्रित सामग्री, हस्ताक्षर की तुलना; मिटाने, परिवर्तन, बदलाव, गुप्त लेखन के लिए दस्तावेजों की जांच; गोपनीय बीजलेख वाचन; लेखन / कागज की परस्पर उम्र प्रमाणित करना; जले हुये दस्तावेजों की जांच आदि।

अस्त्र-विज्ञान खंड: आग्नेयास्त्रों की सक्षमता पता लगाने के लिए उनकी जांच। चलायी गई गोलियों, कारतूसों, छर्रों से पता करना कि क्या वह आग्नेयास्त्र शस्त्र कानून के अधीन आता है, वह कैसा और किस प्रकार का आग्नेयास्त्र है। पता करना कि क्या दो या अधिक कारतूस / कारतूस के खोल एक ही या अलग –अलग आग्नेयास्त्र से दागे गए हैं, किसी खास आग्नेयास्त्र से कारतूस/कारतूस के खोल का संबंध स्थापित करना, आग्नेयास्त्र का

प्रकार स्थापित करने के मद्देनजर पोस्टमार्टम रिपोर्ट / जख्म रिपोर्ट / एक्स रे प्लेट / कपड़े की जांच करना, गोलीबारी का साक्ष्य पता करने के लिए आग्नेयास्त्र की जांच, दुर्घटनावश गोली चलने की संभावना का पता करने के लिये आग्नेयास्त्र की जांच, गोलीबारी कितनी दूर से हुयी इसका आकलन, गोलीबारी से हुये अवशिष्ठ का पता करके गोली चलाने वाले या कारतूस से हुये छेद की पहचान, गोलीबारी के स्थल के पुनर्निर्माण के लिए सामान्य जांच आदि।

रसायनशास्त्र खंड : अफीम और इसके क्षार, हेरोइन, गाँजा, भांग, चरस और अन्य नशीले द्रव्य का परीक्षण; अवैध शराब, वार्निश, पेट्रोल, डीजल, केरोसिन आदि का परीक्षण; आगजनी के संदिग्ध मामलों में ज्वलनशील तरल व ठोस पदार्थों का परीक्षण; अलकोहलयुक्त औषधियों आदि का परीक्षण; डाई, स्याही, दाग-धब्बे और अन्य जैविक व अजैविक रसायनों का परीक्षण।

विषविज्ञान खंड: वनस्पति मूल के विष (धतूरा, कनेर, अफीम, मदार ईकोनाइट, नक्स वामिका आदि), अजैविक लवण (संखिया,कॉपर सल्फेट, साइनाइड आदि), तेजाब, औषधियाँ, क्षार तत्व, कीटनाशक (डीडीटी, बीएचसी पैराथीआन, मैलाथीआन, अल्ड्रिन, ज़िंक फॉस्फेट, एल्युमिनियम फॉसफाइड आदि), एल्कोहल (मीथाइल व ईथाइल अल्कोहल आदि) तथा शीशे के पाउडर समेत अन्य सभी प्रकार के विष की जांच के लिए विसरा, पेट के द्रव, उल्टी, मूत्र व रक्त का परीक्षण।

जीव विज्ञान खंड : जैविक द्रव (वीर्य, लार, पसीना, मूत्र, मल आदि) का परीक्षण; मानव / पशु मूल के ऊतकों का परीक्षण; बाल, ऊन और रेशों का परीक्षण; उत्पत्ति, आयु, लिंग, शारीरिक बनावट स्थापित करने के लिए हड्डियों, दांतों आदि का परीक्षण; कागज के गूदे का परीक्षण; बीज, पत्तों के टुकड़े, फूल, पराग कण, लकड़ी, छाल, टहनी आदि पौधे के हिस्सों की

पहचान की जांच; डायटम और अन्य सूक्ष्म जीवों फफूंद, काई, भुकड़ी जैसे अत्यंत सूक्ष्म वनस्पति तत्वों की पहचान।

सीरम विज्ञान खंड : रक्त की रसायनिक, माइक्रोस्कोपिक और स्पेक्ट्रोस्कोपिक जांच, रक्त के धब्बों व अन्य जैविक धब्बों की पहचान व ग्रुपिंग के लिए इनकी सीरम विज्ञानी जांच, रक्त के धब्बों से लिंग की पहचान, रक्त धब्बों की एंजाइम ग्रुपिंग।

विस्फोटक खंड : विस्फोटक पदार्थों का परीक्षण और विस्फोट के उपरांत विस्फोटक यंत्र के अवशेषों का परीक्षण तथा विस्फोट स्थल का परीक्षण।

चिकित्सा-विधिक खंड : पीड़ित / संदिग्ध व्यक्ति के जख्मों की जांच, शस्त्र व विषविज्ञान खंडों में विशेषज्ञों को उपयुक्त जानकारी व पोस्टमोर्टम रिपोर्ट की व्याख्या के जरिए सहायता प्रदान करना तथा चिकित्सा-विधि सलाह के लिए हड्डियों और ऊतकों का परीक्षण। यह खंड अभी स्थापना की प्रक्रिया में है।

मिथ्या-अनुसंधान खंड : संदिग्ध अपराधियों और गवाहों से पूछताछ। यह खंड स्थापना की प्रक्रिया में है।

उपस्कर विश्लेषण खंड : प्रयोगशाला के विभिन्न खंडों की जरूरतों के अनुसार विश्लेषण के आधुनिक उपस्कर तरीकों के प्रयोग से नमूनों का परीक्षण। यह खंड स्थापना की प्रक्रिया में है।

अपराध विवेचना में विज्ञान का प्रयोग कानून प्रवर्तन एजेंसियों के साथ दिनो-दिन लोकप्रिय होता जा रहा है। विगत वर्षों में विधि विज्ञान प्रयोगशाला को संदर्भित मामलों की बढ़ती संख्या से यह एकदम स्पष्ट है। 1979 में जब उत्तर प्रदेश सरकार ने राज्य की जांच एजेंसियों को उपलब्ध वैज्ञानिक सुविधाओं के पुनर्गठन का फैसला किया था तब आगरा और लखनऊ की प्रयोगशालाओं को संदर्भित मामलों की संख्या मात्र 7,500 थी। आज इन

प्रयोगशालाओं को मिलने वाले मामलों की औसत संख्या करीब 24,000 है।

अंतर्राष्ट्रीय सहयोग

संयुक्त राष्ट्र विकास कार्यक्रम के यूएनएफएडीएसी परियोजना के तहत सुदृढीकरण के लिए विधि विज्ञान प्रयोगशाला, लखनऊ का चयन किया गया था और मादक व नशीले पदार्थों के विश्लेषण व पहचान के लिए 1990 में इसे एचपीएलसी, जीएलसी और टीएलसी जैसे आधुनिक विश्लेषणात्मक उपकरण प्रदान किए गए थे। इन उपकरणों का इस्तेमाल नियमित विश्लेषणात्मक कार्यों के लिए किया जा रहा है।

दूसरा अध्याय
डिजिटल इंडिया बनाम साइबर क्राइम का चक्रव्यूह

वैश्विक स्तर पर फॉरेंसिक साइंस का बदलता स्वरूप

वैश्विक स्तर पर फॉरेंसिक साइंस का उपयोग सिर्फ अपराध और अपराधियों पर नकेल कसने के लिए ही नहीं बल्कि दुश्मन देश के साइबर सिस्टम को तबाह करने के लिए भी किया जाता है। फॉरेंसिक साइंस के जरिए डिजिटल दुनिया में होने वाली हर तरह की हरकत की तह तक जाकर पड़ताल करने का काम किया जाता है। अमेरिका और ईरान के बीच पैदा हुए तनाव में भी यह बात देखने को मिली। अब मिसाइल के जरिए हमले के बजाए एक देश दूसरे देश को डिजिटली तबाह करने में जुटे हैं। दूसरे शब्दों में कहें तो पूरी दुनिया में जंग का मैदान बदल रहा है।

निगरानी ड्रोन को मार गिराए जाने के बाद अमेरिका ने ईरान पर साइबर अटैक किया था। इस हमले में ईरानी सेना और खुफिया एजेंसी को निशाना बनाया गया था। तत्कालीन यूएस के राष्ट्रपति डॉनल्ड ट्रंप ने ईरान के ऊपर मिसाइल हमले का आदेश देने के बाद इसे वापस ले लिया और उसके बदले तेहरान पर 'साइबर स्ट्राइक' का आदेश दिया था। अमेरिका ने गुपचुप तरीके से ईरान के सुरक्षा सिस्टम को निशाना बनाया। यह कुछ अलग किस्म की लड़ाई है। इसमें लड़ाई बड़े जोर-शोर से होती है, लेकिन किसी को कुछ पता नहीं चलता है। क्योंकि जंग का मैदान ज़मीन नहीं बल्कि साइबर सिस्टम होते हैं। इस लड़ाई से होने वाले नुकसान का अंदाजा सिर्फ साइबर फॉरेंसिक के जरिए ही लगाया जा सकता है।

अमेरिका ने ईरान के खिलाफ भविष्य के 'ब्रह्मास्त्र' का प्रयोग किया। इसके जरिए यूएस ने ईरानी सैन्य सिस्टम को तबाह करने का दावा किया। वह भी बिना खून का एक कतरा गिराए। ईरान ने भी पलटवार किया। लेकिन इस तरीके की लड़ाई में जिसमें बिना बम गिराए या गोली चलाए किसी भी देश के सिस्टम को जड़ से हिलाया जा सकता है। इस तरह की लड़ाई में होने वाले नफे-नुकसान का अंदाजा या दुश्मन के गुपचुप हमले के बारे में जानकारी हासिल करने में साइबर फॉरेंसिक विज्ञान कारगर भूमिका निभाती है।

अमेरिका और ईरान के बीच हुई साइबर वॉर भविष्य में होने वाली लड़ाई की एक झलक भर है। दुनिया मिसाइलों, टैंकों और तोपों से निकलकर साइबर वेपन की ओर बढ़ रही है और इस जंग में जीत के लिए सभी महारथियों ने अपनी तैयारियों को पुख्ता करना शुरु कर दिया है। 20 जून, 2019 को ईरान की ओर से ड्रोन को मार गिराए जाने के बाद अमेरिका ने साइबर अटैक करके ईरानी सेना के सैन्य कमांड और कंट्रोल सिस्टम को तबाह कर दिया था। इसके अलावा ईरान के उन खुफिया समूहों को निशाना बनाया गया जिन पर हाल के दिनों में तेल टैंकरों पर हमले का शक था। कई कंप्यूटर सिस्टमों को निशाना बनाया गया। इस अभियान से जुड़े एक अधिकारी के मुताबिक ईरान के मिसाइल लॉन्च करने वाले कंप्यूटर को भी साइबर हमले के जरिए शिकार बनाया गया। इस हमले में किसी व्यक्ति की मौत नहीं हुई। इससे पहले ट्रंप ने कहा था कि मिसाइल हमले में ईरान के आम नागरिक मारे जाते, इसलिए उन्होंने अपने फैसले को वापस ले लिया। दरअसल, ट्रंप अपने फैसले से पीछे नहीं हटे बल्कि अमेरिकी हमले का तरीका बदल दिया। उन्होंने मिसाइल की जगह पर ईरान पर साइबर अटैक कर दिया।

ईरान ने भी अमेरिका पर किया पलटवार

अमेरिकी साइबर हमले के बाद ईरान ने भी पलटवार किया। साइबर सिक्योरिटी कंपनी फायरआई के मुताबिक ईरान से जुड़े APT39, APT33,

APT34 हैकर समूहों ने अमेरिका की दूरसंचार और एयरोस्पेस कंपनियों को निशाना बनाया। हालांकि इसमें अमेरिका को कितना नुकसान हुआ है, इसकी पुष्टि नहीं हुई है। बताया जा रहा है कि ईरान हैकर समूह APT34 2014 से सक्रिय है और लगातार ईरान के पक्ष में साइबर हमले करता रहता है। ऐसा नहीं है कि अमेरिका ने इस तरह की डिजिटल स्ट्राइक पहली बार किया।

अमेरिका-इजरायल पहले भी कर चुके हैं ऐसा अटैक

इससे पहले भी अमेरिका और इजरायल ने ईरान के खिलाफ साइबर अटैक किया था। माना जाता है इस हमले में इस्तेमाल कंप्यूटर वायरस स्टक्सनेट को अमेरिका और इजरायल ने मिलकर बनाया था और उसने ईरान के पूरे डिजिटल सिस्टम को तबाह कर दिया था। पहली बार वर्ष 2010 में इस वायरस के बारे में पता चला था। इसके जवाब में ईरान ने भी अपनी साइबर आर्मी तैयार की है। ईरान ने अपने महत्वपूर्ण कंप्यूटरों को ऑफलाइन भी कर दिया । इससे पहले भी अमेरिका ने अपने मध्यावधि चुनाव के दौरान रूस के इंटरनेट रिसर्च एजेंसी को निशाना बनाया था। रूस पर अमेरिकी राष्ट्रपति चुनाव के दौरान साइबर हमले करने का आरोप लगा था। इसके बाद अमेरिका ने रूसी सिस्टम में अपने हथियार तैनात किए थे, ताकि जरूरत पड़ने पर उन्हें पंगु बनाया जा सके।

गेम चेंजर है साइबर अटैक

विशेषज्ञों के मुताबिक तेजी से डिजिटल होती दुनिया में साइबर अटैक आने वाले समय में गेम चेंजर साबित हो सकती है। सोचिए अगर किसी देश की मिसाइलें लॉन्च न हो पाएं, पनडुब्बियां आपके आदेश को न मानें और परमाणु हथियारों से जुड़े कंप्यूटर काम न करें। ऐसे में वह देश जंग के समय असहाय हो जाएगा और बिना लड़े ही घुटने टेक देगा। साइबर अटैक इसे

संभव बनाता है। सबसे महत्वपूर्ण बात यह है कि इस हमले में किसी जान या माल का नुकसान नहीं होता है। आने वाले समय में 5G तकनीक और आर्टिफिशल इंटेलिजेंस इस जंग को और तेज करेंगे।

साइबर युद्ध बनाम साइबर फॉरेंसिक

अमेरिकी खुफिया एजेंसी के मुताबिक हरेक देश अपनी साइबर वॉरफेयर तकनीक और साइबर डिफेंस क्षमता में निवेश कर रहा है। इसके अलावा 30 देश ऐसे हैं जो आक्रामक साइबर अटैक क्षमता पर काम कर रहे हैं। हालांकि ज्यादातर देश यह काम बेहद गोपनीय तरीके से कर रहे हैं। इस तरह से गोपनीय साइबर हथियारों की जंग पहले ही शुरू हो गई है। अमेरिका का मानना है कि रूस, चीन, ईरान और उत्तर कोरिया उसके लिए बड़ा खतरा हैं। अमेरिका ने चेतावनी दी है कि रूस के पास 'बेहद उन्नत आक्रामक साइबर प्रोग्राम' है। विशेषज्ञों के मुताबिक उत्तर कोरिया ने एक ऐसा हथियार बनाया है जो करोड़ों डॉलर चुरा सकता है। इससे दुनियाभर में गंभीर संकट पैदा हो सकता है।

अमेरिकी रक्षा मंत्रालय पेंटागन के मुताबिक चीन बहुत तेजी के साथ साइबर युद्ध की क्षमता को बढ़ा रहा है ताकि वह अमेरिका की बराबरी कर सके। चीन अमेरिकी रक्षा नेटवर्क में घुसकर डेटा इकट्ठा कर रहा है जिससे भविष्य में संकट पैदा हो सकता है। इन सबके बावजूद माना जाता है कि अमेरिका की साइबर डिफेंस और साइबर अटैक क्षमता सबसे अच्छी है। वर्ष 2016 में अमेरिकी राष्ट्रपति बराक ओबामा ने भी कहा था कि हमने रक्षा और साइबर अटैक करने की बेहतरीन क्षमता हासिल कर ली है। अमेरिका ने अपने साइबर कमान को एकीकृत युद्ध कमान में बदल दिया है। इसके अलावा कई बेहद घातक साइबर हथियार बनाए गए हैं। साथ ही साथ दुश्मन के बारे में डिजिटल दुनिया में जानकारी का पता लगाने के लिए साइबर फॉरेंसिक के क्षेत्र में भी सभी देश जोर-शोर से नए-नए प्रयोग करने में जुटे हैं।

भारत ने भी बनाई द डिफेंस साइबर एजेंसी

भारत भी बेहद गोपनीय तरीके से साइबर वॉरफेयर की तैयारी कर रहा है। हाल के दिनों में पाकिस्तानी साइबर अटैक काफी बढ़ गया है, इसे देखते हुए सरकार ने तैयारी तेज कर दी है। सेना, नौसेना और वायुसेना की एक संयुक्त एजेंसी द डिफेंस साइबर एजेंसी बनाई जा रही है, जो साइबर हमलों का मुकाबला करेगी। इसमें 1000 विशेषज्ञ होंगे जो सेना, नौसेना और एयरफोर्स को दिए जाएंगे। यह एजेंसी दुश्मनों पर हमले करेगी और भारतीय प्रतिष्ठानों का बचाव भी करेगी। आने वाले समय द डिफेंस साइबर एजेंसी की भूमिका काफी कारगर साबित होने वाली है, क्योंकि भविष्य की जंग मैदान में कम डिजिटल फील्ड में ज्यादा लड़ी जाएगी।

डिजिटल इंडिया बनाम साइबर क्राइम

गुरुग्राम में पहला साइबर थाना मार्च 2018 में खोला गया था। यहां साल 2018 में 4620 शिकायतें आईं तो साल 2019 में 8912 जबकि 2020 में अब तक 312 लोगों के साथ ठगी हो चुकी है। साइबर सिटी गुरुग्राम अब साइबर क्राइम सिटी बनता जा रहा है। डेढ़ साल में अब तक साइबर थाने में कुल 13844 शिकायतें आई हैं, जिसमें पुलिस ने 12 हजार से ज्यादा शिकायतों का निपटारा कर दिया है। वहीं, ठग अब तक 2 करोड़ से ज्यादा की ठगी कर चुके हैं। पुलिस आंकड़ों की मानें तो साल 2019 में हर दिन 30 लोग पुलिस के पास ठगी की शिकायत लेकर पहुंचे थे। किसी को जालसाजों ने ऑनलाइन ठगा तो किसी को लॉटरी या जॉब का लालच देकर शिकार बनाया गया। हालांकि पुलिस का दावा है कि करीब 7700 शिकायतों का निपटारा कर दिया गया है। 2019 में कुल 118 शिकायतें पुलिस ने आईटी एक्ट के तहत दर्ज की थी। इस दौरान लॉटरी और जॉब के नाम पर फर्जीवाड़े के करीब 350 मामले सामने आए। वहीं, साइट के जरिए ठगी के लगभग 500 मामले पुलिस को मिले। फर्जी वेबसाइट बनाने के 138, हैकिंग के

करीब 50, डेटा लीक के 80, पोर्न वीडियो और फोटो से छेड़छाड़ से जुड़ी करीब 100 से अधिक शिकायतें पुलिस को मिलीं थी। जब ठगी के मामले इतने ज्यादा सामने आ रहे हैं, तो ऐसे में बचाव के क्या रास्ते हो सकते हैं या हमें किस तरह की सावधानिया बरतनी चाहिए?

1. कोई ऐप तुरंत एडवांस पेमेंट करने को कहे तो सतर्क हो जाएं
2. अपने खाते या मोबाइल वॉलेट की जानकारी किसी को न दें
3. मोबाइल वॉलेट ऐप में सिक्युरिटी ऑप्शन को ऑन रखें
4. मोबाइल पर मेसेज से आए लिंक पर क्लिक न करें
5. मोबाइल पर कोई ऐप किसी के कहने पर न डाउनलोड करें

साइबर क्राइम के लिए नहीं कोई ट्रिब्यूनल

सूचना प्रोधौगिकी के इस युग में जहां साइबर क्राइम लगातार बढ़ रहा है और आप और हम में से स्मार्ट मोबाइल का इस्तेमाल करने वाला हर व्यक्ति इसका आसान शिकार है, पर 2006 में बनाई गई साइबर अपीलेट ट्रिब्यूनल को खत्म कर दिया। आपको ये जानकर हैरानी होगी कि दिल्ली NCR में साइबर क्राइम के हजारों मामले एक दिन में सामने आते हैं। लेकिन करीब 7 साल से चेयरमैन के ना होने से इस ट्रिब्यूनल में 2011 से एक भी मामले की सुनवाई नहीं हो सकी। यानि अगर बैंक एकाउंट से अचानक आपके लाखों रुपये निकल जाएं या फिर कंप्यूटर से किसी ने आपकी पर्सनल जानकारी चुरा ली हो, या आपका कंप्यूटर किसी ने हैक कर लिया हो तो उनकी सुनवाई और अपराधी को सजा दिलवाने के लिए आप कुछ नहीं कर पाएंगे। आपके पास हाथ मलने के अलावा कोई और विकल्प नहीं है। साइबर एक्सपर्ट पवन दुग्गल के मुताबिक क्राइम ब्यूरो के क्राइम रिकॉर्ड में सिर्फ वही केस रजिस्टर हो पाते हैं जिनमें एफआईआर दर्ज हो पाती है और जो टोटल साइबर

क्राइम होते हैं,वो करंट रियलिटी से बिल्कुल उलट हैं। हमने कुछ साल पहले एक सर्वे किया था कि भारत में किस तरह से अंडर रिपोर्टिंग होती है, साइबर क्राइम के मामलों में हमने पाया कि 500 में से 50 की ही शिकायत मिलती है और फिर 50 में से कितने मामले की एफआईआर दर्ज हो पाती है कहना मुश्किल है।

फिलहाल सरकार ने टीडी सेट यानी Telecom Disputes Settlement and Appellate Tribunal में साइबर ट्रिब्यूनल और एयरपोर्ट ट्रिब्यूनल का विलय कर दिया है, लेकिन ये सिर्फ रस्म अदायगी भर है क्योंकि टीडी सेट के पास पहले से ही डेढ़ हजार मामले पेंडिंग हैं और मामले सुनने के लिए सिर्फ एक बेंच है। बेंच में न कोई साइबर एक्सपर्ट है और न कोई जुडिशल बेंच का जुडिशल मेंबर, लिहाजा यहां कोई साइबर क्राइम से जुड़ी याचिका ही नहीं लगाता, क्योंकि बिना दूसरी बेंच के बने साइबर फ्रॉड से जुड़े मामलों की सुनवाई संभव ही नहीं है। सुप्रीम कोर्ट से रिटायर्ड जस्टिस शिवा कीर्ति सिंह, जोकि टीडी सेट के चेयरमैन हैं, वह खुद भी मानते हैं कि पहले से ही इतने मामले लंबित हैं, लिहाजा जब तक नई बेंच नहीं बनती, साइबर हो या एयरपोर्ट ट्रिब्यूनल, मामलों का जल्द निपटारा नहीं हो सकता। उन्होंने एक और नई बेंच ट्रिब्यूनल बनाए जाने की गुजारिश की है। टीडी सेट के चेयरमैन के मुताबिक यहां पहले से ही बहुत ज्यादा मामले लंबित हैं, लिहाजा नई बेंच बनाने की जरूरत है और इस बारे में संबंधित विभाग को लिख दिया गया है। लेकिन सरकार अलग अलग एजेंसी के जरिए साइबर अपराध को रोकने की भरपूर कोशिश कर रही है।

चाइल्ड पोर्नोग्राफी सर्च करना अपराध, उत्तराखंड में केस दर्ज

इंटरनेट जानकारी का खजाना है, इसका सही इस्तेमाल करने से आप सभी तरह के काम घर बैठे कर सकते हैं। लेकिन गलती से भी इंटरनेट पर चाइल्ड पोर्नोग्राफी सर्च न करें और न ही ऐसी कोई सामग्री किसी को भेजें, क्योंकि

ऐसा करते ही आपका मोबाइल या कंप्यूटर और लैपटॉप को खुफिया एजेंसी अपने रडार पर ले लेगा।

सरकार के इस कदम का उद्देश्य न केवल बच्चे बल्कि बच्चों के विषय पर इंटरनेट पर गलत सामग्री सर्च करने वाले व्यस्कों पर भी शिकंजा कसना है। गलत सामग्री यानी चाइल्ड पोर्नोग्राफी ढूढ़ने वाले 2 लोगों पर पहले ही शिकंजा कस चुका है। साइबर विभाग दूरदराज के इलाकों में कार्रवाई कर रहा है। साइबर क्राइम कंट्रोल ने तीसरा मुकदमा इस संदर्भ में देवभूमि उत्तराखंड के अल्मोड़ा जिले में पंजीकृत किया है। केंद्र सरकार ने चाइल्ड पोर्नोग्राफी पर रोक लगाने के लिए इसकी निगरानी की जिम्मेदारी एक एजेंसी नेशनल क्राइम फॉर मिसिंग एंड एक्सप्लोइटिड चिल्ड्रेन (एनसीएमईसी) को सौंपी है।

यह एजेंसी देश में कहीं भी ऐसी सामग्री, ब्राउज, डाउनलोड या साझा करने पर संबंधित व्यक्ति को चिन्हित करने में सक्षम है। इसी एजेंसी ने उत्तराखंड में भी एक व्यक्ति पर पोर्नोग्राफी का पहला मुकदमा दर्ज किया, जो अल्मोड़ा जिले का रहने वाला है।

उत्तराखंड स्टेट साइबर क्राइम पुलिस स्टेशन में चाइल्ड पोर्नोग्राफी का पहला मुकदमा दर्ज किया गया। साइबर क्राइम के पुलिस क्षेत्राधिकारी अंकुश मिश्रा के अनुसार नेशनल क्राइम फॉर मिसिंग एंड एक्सप्लोइटिड चिल्ड्रेन (एनसीएमईसी) देशभर में चाइल्ड पोर्नोग्राफी से संबंधित सामग्री के आदान-प्रदान पर नजर रखती है।

इस एजेंसी ने चाइल्ड पोर्नोग्राफी से संबंधित सामग्री के संबंध में एक रिपोर्ट नेशनल क्राइम रिकार्ड ब्यूरो (एनसीआरबी), नई दिल्ली को भेजी थी, जिसमें अल्मोड़ा निवासी किशन सिंह का भी जिक्र था।

एजेंसी की रिपोर्ट के अनुसार, उसने चाइल्ड पोर्नोग्राफी का वीडियो इंटरनेट

से डाउनलोड कर अपने साथियों को सोशल साइट पर भेजा था। इस पर एनसीआरबी ने देहरादून साइबर पुलिस स्टेशन को मामले की जांच कर आरोपित पर कार्रवाई के लिए निर्देशित किया था।

चाइल्ड पोर्नोग्राफी से संबंधित सामग्री डाउनलोड या शेयर करने पर आरोपित के खिलाफ आइटी एक्ट की धारा 67बी के तहत मुकदमा दर्ज किया जाता है। इसमें पांच साल तक का कारावास हो सकता है। इसी तरह अन्य पोर्नोग्राफी से संबंधित सामग्री डाउनलोड या शेयर करने पर आइटी एक्ट की धारा 67 के तहत मुकदमा दर्ज होता है। इसमें भी पांच साल की जेल हो सकती है। साइबर क्राइम पुलिस के मुताबिक कि चाइल्ड पोर्नोग्राफी अपराध की श्रेणी में आता है।

केंद्रीय गृह मंत्रालय ने देश के सभी साइबर क्राइम थानों को ऐसा कोई भी मामला सामने आने पर इसे गंभीरता से लेते हुए तत्काल मुकदमा दर्ज करने का आदेश दिया है। साथ ही एक एजेंसी को चाइल्ड पोर्नोग्राफी से संबंधित सामग्री का आदान-प्रदान और इस्तेमाल करने वालों को चिन्हित करने की जिम्मेदारी सौंपी है। यह एजेंसी अपनी रिपोर्ट सीधे गृह मंत्रालय को भेजती है, जहां से संबंधित राज्य को कार्रवाई के निर्देश दिए जाते हैं, ऐसे में छोटी-सी गलती आपको बड़ी मुश्किल में डाल सकती है।

डिजिटल इंडिया के फायदे बनाम साइबर क्राइम का गहराता संकट

आपको कैश की जरूरत होती है तो आप क्या करते हैं? जाहिर है करोड़ों लोगों की तरह आप भी नजदीकी एटीएम जाकर कैश निकालते होंगे। आजकल एटीएम जाकर अपने कार्ड से कैश निकालना जिंदगी का अहम हिस्सा बन चुका है। लेकिन क्या आपको पता है कि एटीएम जाकर कैश निकालने वालों पर कुछ ऐसे लोगों की भी नजरें बनी हुई है जो एटीएम कार्ड

की क्लोनिंग कर एटीएम कार्डधारक को लाखों का चूना लगा रहे हैं।

ऐसे ही एक विदेशी मूल के शातिर अपराधी को भोपाल पुलिस की साइबर क्राइम टीम ने बैंगलुरु से गिरफ्तार किया। इसने भोपाल निवासी एक शख्स का एटीएम कार्ड क्लोन कर उसके खाते से रकम निकाल ली थी। पुलिस के अनुसार मामला 12 नवंबर, 2019 का है, जब फरियादी ने एफआईआर दर्ज करवाई थी कि उसके बैंक खाते से अज्ञात व्यक्ति ने रुपये निकाले हैं। पुलिस ने जांच में पाया कि कुछ दिन पहले फरियादी कैश निकालने के लिए भोपाल के कटारा हिल्स स्थित अमलतास के स्टेट बैंक ऑफ इंडिया एटीएम गया था। वहां एटीएम मशीन में स्किमर लगा हुआ था। जिससे फरियादी का एटीएम कार्ड क्लोन हुआ था। साइबर पुलिस को इस दौरान दो विदेशी नागरिकों की जानकारी मिली, जिन्होंने इस घटना को अंजाम दिया था।

सर्विलांस से पकड़ में आए अपराधी

साइबर पुलिस ने आरोपियों पर सर्विलांस के जरिए नजर रखनी शुरु की। पुलिस ने पाया कि अपराधी बेहद शातिर किस्म के हैं जो बेहद हाईटेक तरीके से वारदात को अंजाम देते हैं और लगातार अपनी लोकेशन अलग-अलग राज्यों में बदलते रहते हैं। पुलिस ने इन पर नजर रखनी शुरु की और आखिरकार इनको बैंगलुरु में चिन्हित कर लिया गया। 13 जनवरी, 2020 को साइबर क्राइम टीम ने बैंगलुरु से युगांडा निवासी मुकासा एंड्रू को गिरफ्तार कर लिया। इसके पास से 3 मोबाइल, भोपाल में क्लोन किए गए कार्ड वाले खाते की चेकबुक और एक लैपटॉप जब्त किया। आरोपी ने पुलिस पूछताछ में बताया कि उसने बैंगलुरु से भोपाल आकर एटीएम कार्ड क्लोन किया और वापस बैंगलुरु चला आया था। आरोपी ने कबूल किया है कि एटीएम कार्ड क्लोन करने के बाद वो मशीन को तोड़ देता था ताकि पकड़ा न जा सके। इसके अलावा डुप्लीकेट कार्ड से पैसे निकालने के बाद वो उसे भी तोड़ देता था। साइबर क्राइम ब्रांच ने आरोपी को भोपाल लाकर कोर्ट

में पेश किया, जहां से उसे पुलिस रिमांड पर भेज दिया गया।

साइबर अपराध का ग्लोबल नेटवर्क (वैश्विक एवं स्थानीय गठजोड़)

देश में ऑनलाइन फूड की डिलिवरी करने वाली कंपनी जोमेटो (Zomato) पर बड़ा साइबर हमला हुआ। इस संबंध में कंपनी ने ब्लॉग के जरिए जानकारी दी। ब्लॉग में 1.7 करोड़ यूजर्स के डाटा के चोरी होने की बात कही गई है। हालांकि कंपनी का कहना है कि यूज़र्स के पेमेंट से संबंधित कोई डाटा चोरी नहीं हुआ है। Zomato के मुताबिक डेटाबेस से लगभग 1.7 करोड़ कस्टमर्स के डेटा चोरी किए जा चुके हैं। इनमें ईमेल और पासवर्ड शामिल हैं। कंपनी ने अपने आधिकारिक ब्लॉग पोस्ट में बताया है कि डेटा यूज़र्स के डेटा चोरी किए गए हैं। हालांकि, कंपनी ने सभी प्रभावित यूज़र्स के पासवर्ड रीसेट कर दिए हैं और Zomato का कहना है कि क्रेडिट कार्ड की जानकारियां पूरी तरह सिक्योर हैं। लेकिन देश में ऑनलाइन काम करने वाली फूड की डिलिवरी करने वाली कंपनी जोमेटो (Zomato) एक अंतरराष्ट्रीय कंपनी है और इस साइबर हमले में वैश्विक के साथ स्थानीय लोगों का भी हाथ होने से इनकार नहीं किया जा सकता है।

हैकरीड के मुताबिक Zomato के डेटाबेस में यूजर्स के ईमेल पासवर्ड हैशेस शामिल हैं। जिन्हें डार्क वेब में पैकेज के तौर पर लगभग 1000 डॉलर (करीब 64064 रुपए) में बेचा जा रहा है। जो वेंडर्स इन डेटा को बेच रहे हैं वो इसका सैंपल भी दे रहे हैं कि यह डेटा सही है और इन्हें इस्तेमाल किया जा सकता है। कंपनी का कहना है कि चोरी किए गए पासवर्ड हैश के तौर पर हैं, इसलिए इन्हें हैकर्स प्लेन टेक्स्ट में कनवर्ट नहीं कर सकते हैं। Zomato ने कहा है कंपनी सिक्योरिटी में बढ़ोतरी करेगी और कस्टमर्स को हरसंभव मदद मुहैय्या कराएगी। कंपनी इसे ह्यूमन एरर कह कर भले ही टाल दे, लेकिन यह मामला गंभीर है और इसके साथ यूज़र्स कि सिक्योरिटी जुड़ी हैं।

क्योंकि इससे न सिर्फ यूज़र्स के जोमैटो अकाउंट प्रभावित होंगे बल्कि इससे दूसरी आईडी भी हैक हो सकती हैं।

साइबर फॉरेंसिक अपराध को लेकर लोगों में जागरुकता की कमी

भारतीय रिजर्व बैंक (RBI) ने मौजूदा और आगे की टेक्नोलॉजी में साइबर सुरक्षा के खतरों की समीक्षा के लिए विभिन्न विधाओं के जानकारों की एक स्थायी समिति का गठन किया है। इस स्थायी समिति के काम के निम्नलिखित कार्य होंगे।

यह 11 सदस्यीय समिति विभिन्न सुरक्षा मानकों, प्रोटोकॉल, इंटरफेस पर अंशधारकों से विचार-विमर्श करेगी।

समिति साइबर सुरक्षा को मजबूत करने और उसमें लचीलापन लाने के लिए उचित नीतिगत सुझाव भी देगी।

RBI की कार्यकारी निदेशक की अगुवाई वाली समिति आगे चलकर और अधिक विशेषज्ञों की सेवाएं ले सकती हैं और यह विशेष प्रकार के मुद्दों को देखने के लिए उप-समितियों की व्यवस्था के जरिए काम कर सकती है।

साइबर सुरक्षा और सूचना प्रौद्योगिकी परीक्षण पर विशेषज्ञ समिति की सिफारिशों के आधार पर RBI ने पिछले साल जून में बैंकों को दिशानिर्देश जारी कर साइबर सुरक्षा की तैयारियां करने को कहा था।

RBI ने कहा कि बैंकों ने अपनी सुरक्षा को मजबूत करने के लिए कई कदम उठाए हैं, लेकिन साइबर हमलों में विविधता को देखते हुए मौजूदा साइबर सुरक्षा पृष्ठभूमि की समीक्षा करने की जरूरत है।

साइबर हमले के बाद साइबर फॉरेंसिक ही एक मात्र उपाय

डिजिटल दुनिया के इस दौर में हर काम ऑनलाइन हो रहा है। सरकारें लोगों

को डिजिटल लेन-देन के लिए प्रोत्साहित करती हैं। मेट्रो टैक्सी में सफ़र करें या हवाई जहाज़ से उड़ान भरें, ऑनलाइन टिकट ख़रीदने का चलन बढ़ता जा रहा है। नौकरियों से लेकर शादियां तक ऑनलाइन ढूंढी जा रही हैं। ऐसे में एक दिन ऐसा हो, जब सारे कंप्यूटर बंद हो जाएं, तो क्या होगा? ठीक वैसा ही होगा, जैसा अमरीका के अलास्का राज्य के एक शहर मटानुस्का-सुसिन्ना में हुआ था। वहां के बाशिदों को अब तक पता नहीं कि क्या हुआ था। लेकिन, जब ऐसी घटना हुई, तो मैट्सू की सारी व्यवस्था चरमरा गई थी, बल्कि ढेर हो गई थी। असल में एक वायरस ने मटानुस्का-सुसिन्ना के कंप्यूटर नेटवर्क पर हमला किया था। इससे शहर की पूरी व्यवस्था चौपट हो गई थी। डिजिटल होती दुनिया जब पटरी से उतरती है, तो क्या होता है, ये बात मटानुस्का-सुसिन्ना पर हुए साइबर हमले से साफ़ हो गई थी। जब एक वायरस ने मटानुस्का-सुसिन्ना के कंप्यूटरों को ठप किया, तो सैकड़ों सरकारी कर्मचारियों के सिस्टम अचानक बंद हो गए। स्थानीय पुस्तकालयों में लगातार फोन आने लगे कि वो अपने कंप्यूटर फौरन बंद कर दें। यहां तक कि जानवरों को रखने के ठिकानों में दर्ज दवाओं के आंकड़े कंप्यूटर वायरस के ऐसे क़ैदी बने कि वहां के कर्मचारियों को समझ ही नहीं आ रहा था कि वो बीमार जानवरों को कौन सी दवां दे। बात सिर्फ़ यहीं तक नहीं रुकी। तैराकी सीखने के ऑनलाइन रजिस्ट्रेशन की व्यवस्था ठप हो गई। नतीजा ये हुआ कि तैराकी सीखने की चाहत रखने वालों को बुकिंग के लिए क़तार में खड़े होना पड़ा। शहर के एक सरकारी दफ़्तर को तो काम चलाने के लिए पुराने टाइपराइटर निकालने पड़े, ताकि सरकारी अर्ज़ियां निपटाई जा सकें।

मटानुस्का-सुसिन्ना शहर को मैट-सू के नाम से ज़्यादा जाना जाता है। अमरीका के उत्तरी राज्य अलास्का का ये शहर आज भी उस साइबर हमले से उबरने की कोशिश कर रहा है, जबकि साइबर अटैक को हुए लंबा समय बीत चुका है।

मैट-सू के कंप्यूटरों पर वायरस का हमला जुलाई, 2018 में हुआ था। जब इस साइबर हमले के पहले संकेत मिले, तो किसी को भी ये अंदाज़ा नहीं था

कि बात इतनी गंभीर हो जाएगी। शहर के आईटी कर्मचारियों को इस हमले से हुए नुक़सान की सफ़ाई के लिए 20-20 घंटे काम करना पड़ा था, ताकि क़रीब 150 सर्वरों से खुरच-खुरच कर वायरस हमले के अवशेष निकाले जा सकें। मैट-सू एक ग्रामीण बस्ती है। यहां की आबादी केवल एक लाख है। ऐसे में इस शहर पर साइबर हमला होना अचरज की बात थी। लेकिन साइबर फॉरेंसिक की टीम ने तोड़ निकाल लिया। पिछले साल 23 जुलाई, 2018 को मैट-सू के छोटे से मुहल्ले पामर के कर्मचारी रोज़ाना की तरह काम के लिए दफ़्तर पहुंचे। कुछ ही घंटों में उन्हें पता चल गया कि सिस्टम में कोई वायरस घुस आया है। शहर के आईटी निदेशक एरिक वाइट ने साइबर फॉरेंसिक की टीम को इस मामले की पड़ताल के लिए कहा। उन्होंने वायरस से जुड़ी कुछ फ़ाइलें पाईं, तो उन्हें डिलीट कर दिया और सभी कर्मचारियों को अपना लॉग इन और पासवर्ड बदलने को कहा। साथ ही सिस्टम की सफ़ाई का भी काम शुरू कर दिया गया। लेकिन, जैसे ही कंप्यूटर सिस्टम की हिफ़ाज़त की ये व्यवस्था लागू की गई, तो इसके उल्टे ही नतीजे देखने को मिले। एरिक वाइट बताते हैं कि एक के बाद एक कंप्यूटर ठप होने लगे। ऐसा लगा कि इस साइबर हमले का दूसरा स्टेज एक्टिव हो गया था। शायद किसी की निगाह, मैट-सू के आईटी विभाग की साइबर सुरक्षा के क़दमों पर थी। कई कंप्यूटरों पर तो बहुत अहम फ़ाइलें, इस हमले की शिकार हो गईं। हमलावर हैकरों ने सिस्टम से वायरस हटाने के लिए फ़िरौती मांगनी शुरू कर दी। ऐसे वायरस को रैनसमवेयर कहते हैं, जिसके ज़रिए लोगों के सिस्टम पर हमला किया जाता है। फिर उनके डेटा को रिस्टोर करने के लिए फ़िरौती वसूली जाती है।

कंप्यूटर बंद हुआ और काम हुआ ठप

हाल के बरसों में रैनसमवेयर के हमले की वजह से कई शहरों में अस्पतालों, बंदरगाहों और दफ़्तरों में काम-काज ठप हो चुका है। इन हमलों की वजह से कुछ देर के लिए पूरी तरह से अराजकता का माहौल हो जाता है। डिजिटल तरीक़े से काम निपटाने के हम इतने आदी हो चुके हैं कि आज हम समझ ही

नहीं पाते कि अचानक डिजिटल दुनिया के पहिए ठहर गए, तो क्या होगा? जानकार कहते हैं कि रैनसमवेयर के हमले से हर साल अरबों डॉलर का नुक़सान होता है। लेकिन, एरिक वाइट के लिए अपने शहर के सिस्टम पर हुआ ये वायरस अटैक चौंकाने वाला था। उन्होंने इतना बड़ा साइबर हमला, अपने फौजी दिनों में देखा था। एरिक वाइट अमरीकी एय़रफ़ोर्स में आईटी अफ़सर थे, वो रक्षा क्षेत्र के सरकारी ठेकेदारों के साथ काम कर रहे थे। एरिक बताते हैं कि, "मेरे पास आईटी सेक्टर में काम करने का 35 साल का तजुर्बा है, मैंने ऐसे कई हमले देखे हैं। लेकिन मैट-सू पर हुआ साइबर अटैक मेरी नज़र में सबसे बड़ा हमला था। जब एरिक को लगा कि इस साइबर हमले से भारी नुक़सान होगा, तो उन्होंने शहर के प्रमुख मैनेजर जॉन मूसी को इसकी ख़बर की दोनों ने बातचीत के बाद ये तय किया कि इससे निपटने में एफबीआई की मदद ली जानी चाहिए। इसके बाद मैट-सू के सारे कंप्यूटर ऑफलाइन कर दिए गए। साइबर फॉरेंसिक और आईटी विशेषज्ञ की टीम, कंप्यूटरों में सेव डेटा को फिर से रिस्टोर करने में जुट गए। शहर के सरकारी दफ़्तरों के क़रीब 700 कंप्यूटरों को एक-एक कर के बारीक़ी से चेक करना था। यानी जांच पूरी होने तक वहां के किसी कंप्टूटर में काम करना ख़तरे से ख़ाली नहीं था। शहर के ख़रीदारी विभाग के कर्मचारियों को पर्चे काग़ज़ क़लम से भरने पड़े। उन्होंने दफ़्तर में पड़े पुराने टाइपराइटर निकालकर अपना काम चलाया। उनका ऐसा करना पूरी दुनिया में सुर्ख़ियां बना था।

जब सारे सिस्टम ऑफ़लाइन हो गए, तो कर्मचारियों को फ़ोन और वेबमेल से काम चलाना पड़ा। नतीजा ये हुआ कि काम होने की प्रक्रिया एकदम धीमी हो गई। क्रेडिट कार्ड पेमेंट से लेकर कचरा उठाने तक का काम धीमा हो गया था। मैट-सू के सार्वजनिक पुस्तकालय की लाइब्रेरियन पेगी ओबर्ग ने कहा कि ये साइबर हमला बेहद डरावना था। मैट-सू की बिग लेक लाइब्रेरी में एक हफ़्ते में 1200 से 1500 लोग आते हैं।

इनमें से ज़्यादातर को इंटरनेट और कंप्यूटर सेवाओं की ज़रूरत होती है। पेगी

ओबर्ग कहती हैं कि आईटी डिपार्टमेंट ने सभी कंप्यूटरों को ऑफ़लाइन करा दिया था। उनके प्लग तक निकलवा दिए गए थे। पेगी ओबर्ग कहती हैं कि उन्होंने अपने बीस साल के करियर में ऐसा साइबर हमला पहले कभी नहीं देखा था।

स्कूल, कॉलेज जाने वाले क्यों करने लगते हैं हैकिंग?

हैकर, डेटा लीक, ये सुनते ही जो छवि दिमाग़ में उतरती है, वो अक्सर अंधेरे में हुड से सिर ढँक कर कंप्यूटर के सामने बैठे एक युवा की होती है। ऐसा शायद इसलिए क्योंकि डेटा लीक से जुड़े अधिकतर मामले चोरी-छिपे किए जाते हैं और ऐसे मामलों में जो ख़बरें हमारे सामने आती हैं उनमें किसी किशोर या युवा का नाम होता है। क्या ये कोई पैटर्न है या फिर युवा ही ऐसा करने के लिए अधिक आकर्षित होते हैं? ऐसा क्यों है? एथिकल हैकर साई कृष्णा कोटपल्ली जब इंजीनियरिंग की पहले साल की पढ़ाई कर रहे थे, तब उनके दोस्त ने उन्हें हैकिंग के बारे में बताया था. वो कहते हैं कि दो तीन साल लगातार उन्होंने केवल जिज्ञासा के कारण हैकिंग की।

जो किशोर होते हैं उनके पास काफी समय होता है और नया जानने की इच्छा भी अधिक होती है। उनके लिए ये रोमांच होता है कि वो अपने दोस्त का फ़ेसबुक हैक कर उनके सभी मैसेज पढ़ सकते हैं। या फिर किसी चीज़ पर 10 फीसदी डिस्काउंट को 90 फीसदी कर सकते हैं। आनंद प्रकाश एथिकल हैकर हैं और अब ऐपसिक्योर नाम की कंपनी के सीईओ हैं। आनंद प्रकाश कम उम्र में फेसबुक, ऊबर और ट्विटर जैसी कंपनियों के सॉफ्टवेयर में गड़बड़ी तलाश कर बग बाउंटी के रूप में काम करने के लिए जाने जाते हैं। 21 साल की उम्र में आनंद प्रकाश ने सबसे पहले हैकिंग की तो उन्होंने फेसबुक बग बाउंटी में हिस्सा लिया। वो कहते हैं, "हैकिंग के ज़रिए जब आप बग बाउंटी का काम करते हैं तो आपको ईनाम का पैसा तो मिलता है, पहचान भी मिलती है और साथ में आपका करियर भी बन जाता है। ये

युवाओं के लिए काफ़ी अच्छा साबित होता है। इन सबके अलावा जिज्ञासा भी होती है क्योंकि डेवेलपर तो हर कोई होता है लेकिन हैकर कम ही लोग होते हैं। हैकर अक्सर साइबर फॉरेंसिक की टीम के लिए सहायक का भी काम करते हैं।

एथिकल हैकर राहुल कुमार सिंह ने 9-10 साल की उम्र में जब पहली बार हैकिंग की थी, तब वो किसी और के कंप्यूटर में बिना उसकी जानकारी के घुसने के तरीक़े सीख रहे थे। लेकिन बाद में उन्होंने सॉफ्टवेयर कंपनी भी खोली और अब वो साइबर फॉरेंसिक जांचकर्ता के तौर पर काम कर रहे हैं। अब वो केवल अपने हुनर को बनाए रखने के लिए हैकिंग करते हैं।

साइबर अटैक के कुछ चौंकाने वाले तथ्य

जर्मनी की चांसलर एंगेला मर्केल समेत सैकड़ों राजनेताओं का निजी डेटा एक हैकर ने सोशल मीडिया पर लीक कर दिया था। ये हैकर 20 साल का एक स्कूली छात्र था जो सरकार से नाराज़ था।

15 साल के एक किशोर ने खुद को सीआईए प्रमुख जॉन ब्रेनन के तौर पर पेश कर अफ़ग़ानिस्तान और इटली में सीआईए के ख़ुफिया अभियानों से जुड़े कंप्यूटर में घुसने की कोशिश की।

2012 में 22 साल के एक युवक ने 60 लाख कंप्यूटर्स में वायरस डालकर लोगों के बैंक अकाउंट डीटेल निकाल लिए। इसके ज़रिए उसने 15 करोड़ रूसी रूबल की चोरी की।

एक जांच के तहत 2012 में ही एक हैकिंग ग्रुप से जुड़े 25 लोगों को इंटरपोल ने गिरफ्तार किया था। इंटरपोल 17 से 40 की उम्र के हैकर्स को आर्थिक मदद देने वालों की पड़ताल कर रहा था। गिरफ्तारियों के बाद इंटरपोल की वेबसाइट डाउन हो गई।

ब्रिटेन में 2012 में लूल्ज़सेक हैकिंग ग्रुप के दो सदस्यों को वेबसाइट हैंकिंग के आरोप में सज़ा सुनाई गई थी। ये दोनों 18 और 19 साल के थे।

जाने-माने हैकर जेरेमी हैमन्ड ने 18 साल की आयु में हैक दिस साइट नाम से एक वेबसाइट बना ली थी। उन्हें 2012 में 27 साल की उम्र में स्ट्रैटेजिक फोरकास्टिंग नाम की निजी खुफ़िया कंपनी से डेटा चुराने के आरोप में 10 साल की सज़ा सुनाई गई।

दुनिया के कई देशों में दहशत फैलाने वाले ब्लू व्हेल गेम को रूस में रहने वाले 21 साल के फिलिप बुडकिन ने बनाया था। ये खेल बच्चों के दिमाग़ को इस तरह अपने काबू में कर लेता था कि गेम की वजह से कई आत्महत्या की कोशिश के मामले सामने आए।

युवाओं को कैसे ग़लत दिशा में जाने से रोका जाए?

आनंद प्रकाश ने पुलिस के साइबर सेल के साथ इंटर्नशिप की थी, जहां उन्हें एथिकल और नॉन एथिकल हैकिंग के बारे में बताया जाता था। वो कहते हैं, "मेरे लिए वो काफ़ी महत्वपूर्ण था। ऐसा कुछ दूसरे हैकर्स के साथ हो और नॉर्मल एजुकेशन में हम साइबर सिक्योरिटी डालने लगें तो अच्छा हो जाएगा। जैसे मेरे साथ हुआ वैसा सबके साथ हो जाएगा." वहीं राहुल कुमार सिंह कहते हैं, "मैंने अपनी खुद की ज़िंदगी से यही जाना कि मैंने किसी का पेट मारा तो मेरा भी सारा धन चला जाएगा। बुरे काम का कोई भविष्य नहीं है। बुरा काम कर के आप एक लाख कमाएंगे, एक करोड़ कमाएंगे लेकिन जिस दिन अंदर जाएंगे उस दिन आपका पूरा परिवार इससे प्रभावित होगा।

हाल ही में हुईं कुछ आपराधिक घटनाओं ने महिलाओं के लिए सोशल साइट्स पर सुरक्षा को लेकर सवाल खड़ा किया है। बेंगलुरु में एक महिला के नाम पर नकली फ़ेसबुक अकाउंट बनाया गया और उसे एस्कॉर्ट सर्विस देने वाली वेबसाइट पर डाल दिया गया। इसके बाद से महिला के पास

फ़ोन आने लगे। ट्विटर पर 'पाकिस्तान डिफ़ेंस' नाम के एक अकाउंट ने दिल्ली की एक लड़की की तस्वीर के साथ छेड़छाड़ की थी। ऐसे ही मामले अक्सर सामने आते रहते हैं जिनमें लड़कियों की तस्वीरों और निजी जानकारियों का ग़लत इस्तेमाल या उन्हें ट्रोल किया जाता है। इस तरह के सभी मामलों में साइबर फॉरेंसिक की जांच काफी कारगर भूमिका निभाती है। ज्यादातर मामलों में युवाओं का नाम ही सामने आता है। लिहाजा ऐसे मामले में खास ध्यान देने की ज़रुरत है।

सोशल मीडिया पर बरतें सावधानी

अपराधों से निपटने के लिए कई कानून बनाये गए हैं लेकिन अपनी तरफ से भी कुछ सावधानियां बरतकर महिलाएं इन समस्याओं से बच सकती हैं और बिना किसी चिंता के सोशल मीडिया पर एक्टिव रह सकती हैं। इस बारे में साइबर सुरक्षा विशेषज्ञ जितेन जैन ने निम्नलिखित सुझाव दिए हैं।

क्या करें, क्या न करें?

सबसे पहले तो सोशल मीडिया पर अपनी निजी तस्वीरें डालने से बचें। उनका कोई भी इस्तेमाल कर सकता है।

अगर फिर भी आप तस्वीरें डालना चाहते हैं तो अपने फ़ेसबुक अकाउंट पर अपनी प्राइवेसी सेटिंग्स को पब्लिक न करें।

सेटिंग्स ऐसे रखें कि आपकी फ़ोटो आपके दोस्त या आपसे जुड़े हुए लोग ही देख पाएं। अनजान लोग उन तक न पहुंचे।

अपने नाम के बारे में गूगल पर हमेशा सर्च करते रहें ताकि आपको पता रहे कि आपका नाम कहां पर और किस-किस वेबसाइट पर आ रहा है।

अगर किसी ग़लत जगह पर या ऐसी जगह पर आपको नाम दिखाई देता है

जिसकी अनुमति आपने नहीं दी है, तो उसे तुरंत हटाने के लिए कह सकते हैं।

अनजान लोगों को फ़ेसबुक पर न जोड़ें. कई बार ऐसा करने से नुकसान भी हो सकता है।

प्रोफेशनल लोगों को लिंकडइन पर जोड़ें, फ़ेसबुक पर उनके साथ न जुड़ें, वहीं, ट्विटर के ऊपर बिल्कुल भी निजी तस्वीरें न डालें। यह एक सोशल नेटवर्किंग साइट नहीं है, यह एक ट्विटिंग प्लेटफॉर्म है।

ट्विटर पर ऐसी सेटिंग्स की जा सकती हैं कि आपकी अनुमति के बिना लोग आपको फॉलो न कर सकें। लेकिन, अमूमन लोग ऐसा करते नहीं हैं। सेटिंग्स को ज़्यादा निजी करके आपका अकाउंट ज़्यादा सुरक्षित रह सकता है।

आप कई बार किसी का अकाउंट ब्लॉक कर देते हैं या उसकी रिपोर्ट कर देते हैं। इसके बाद ब्लॉक किया हुआ शख़्स आपके अकाउंट तक नहीं पहुंच सकता लेकिन ध्यान रखें कि वो दूसरे अकाउंट से आप तक पहुंच सकता है।

ऐसे में किसी दूसरे अनजान प्रोफ़ाइल की फ्रेंड रिक्वेस्ट स्वीकारने से पहले इस बात को दिमाग में रखें। अगर आप किसी समस्या में फंस भी जाते हैं तो घबराएं नहीं बल्कि पुलिस को इसकी जानकारी दें।

कैसे पता करें नकली अकाउंट

अक्सर ऐसा भी होता है कि किसी फ़ेसबुक अकाउंट में लड़की की तस्वीर लगी होती है लेकिन वो अकाउंट किसी लड़के ने बनाया होता है। इसी तरह नकली नाम और तस्वीर के साथ भी फ़ेसबुक अकाउंट बना होता है।

ऐसे अकाउंट का पता लगाने के लिए कुछ बातों पर ध्यान देना ज़रूरी है। किसी भी फ्रेंड रिक्वेस्ट को स्वीकार करने से पहले सामने वाले का अकाउंट अच्छी तरह देख लें।

ऐसे नकली अकाउंट में अक्सर सारी फ़ोटो उसी दिन डली हुई होती हैं। वो सिर्फ तीन-चार ग्रुप्स से जुड़ा होता है और 10-15 दोस्त होते हैं। कई बार ऐसे अकाउंट में अलग-अलग लड़कियों की तस्वीरें होती हैं।

ऐसा भी होता है कि प्रोफ़ाइल पिक किसी लड़की की होती है लेकिन गैलरी में उसकी एक भी तस्वीर नहीं होती और न कोई पोस्ट होता है। इस तरह के अकाउंट से बचना चाहिए।

लाइक्स की चाह

क्रिमिनल साइकोलॉजिस्ट अनुजा त्रेहन कपूर के अनुसार महिलाओं को जब असल ज़िंदगी में उम्मीद के मुताबिक महत्व नहीं मिलता तो उसका झुकाव वचुर्अल की दुनिया की ओर ज़्यादा होता है, जहां उनकी तारीफ़ करते लोग थकते नहीं हैं। सेल्फी की ही बात करें तो इसने हमें ऐसी जगह ला दिया है कि वर्चुअल दुनिया में तो आपको लाइक मिलेंगे लेकिन असल दुनिया में आपको कोई पूछेगा भी नहीं।

अनुजा कपूर की माने तो लाइक्स और प्रशंसा की यही चाह लोगों को तस्वीरें डालने के प्रोत्साहित करती हैं और आप अपनी निजी जानकारियां व तस्वीरें डालने का सिलसिला बढ़ा देते हैं। महिलाओं के साथ यही स्थिति होती है। उस वक्त वो ये नहीं सोच पाती हैं कि इनका दुरुपयोग भी किया जा सकता है। लड़कियों के साथ हो रही घटनाएं साइबर क्राइम बढ़ने का भी हिस्सा हैं। साइबर क्राइम आपको पहचान छुपाने का मौका देता है। ये लोगों के लिए अपराध करना और आसान बना देता है। वहीं, अक्सर लोग सार्वजनिक रुप से अपनी दिनचर्या बता देते हैं। घर कहां है, कहां गए हैं और कहां जाने वाले हैं ये सब बता देते हैं। ये सामने वाले को अपराध के लिए न्यौता देने जैसा है।

लोगों को वर्चुअल से ज़्यादा असल ज़िंदगी पर ध्यान देना चाहिए। लेकिन, इसे पूरी तरह भी नहीं छोड़ा जा सकता तो सुरक्षा के लिए आ रहे नए तरीकों को अपनाएं। फिर भी कोई समस्या हो तो क़ानून का सहारा लेना चाहिए।

भाग 2

साइबर अपराध की बदलती दुनिया

तीसरा अध्याय

साइबर दुनिया और जन सामान्य का अंतर-संबंध

इंटरनेट : ज्ञान का सागर

वैज्ञानिक और तकनीक के क्षेत्र में विकास से इस ब्रह्मांड में कम्प्यूटर के जरिए सूचना के राजमार्ग इन्टरनेट पर चलकर समस्त विश्व एकीकरण के लिए प्रयासरत है। मानव-जीवन की सभी गतिविधियां यथा-राजनीतिक, व्यापारिक, सांस्कृतिक आदि इलेक्ट्रॉनिक सुविधाओं से लाभान्वित हो रही हैं। दुनिया के किसी कोने में बैठा कोई व्यक्ति अपने कम्प्यूटर को इन्टरनेट से जोड़कर सूचना सम्राट बन सकता है। इन्टरनेट से जुड़ा कम्प्यूटर होस्ट कहलाता है। इस साम्राज्य में राजा व रंक सभी अपने होस्ट कम्प्यूटर से सूचनाओं का आदान-प्रदान कर सकते हैं। इन्टरनेट का जन्म शीत-युद्ध के गर्भ से अमेरिका में हुआ। 1960 के दशक में सोवियत संघ के परमाणु आक्रमण से चिंतित अमेरिकी सरकार ने एक ऐसी व्यवस्था की संरचना की जिसमें अमेरिकी शक्ति किसी एक जगह पर केन्द्रित न रहे।

ई-डाक प्रणाली

सत्तर के दशक में अमेरिका की रक्षा अनुसंधान परियोजना एजेंसी में इन्टरनेट से संबंधित दस्तावेजों के प्रकाशन और प्रोटोकाल संचालन के लिए इंटरनेट कारवाई बोर्ड होता है। इंटरनेट की लोकप्रियता के पीछे इसकी विविध प्रणालियां और सेवाएं प्रमुख हैं। इंटरनेट में प्रयुक्त उपकरण भी उल्लेखनीय हैं जो प्रयोक्ताओं की बहुरंगी सेवाओं का उपभोग करने का अवसर देते हैं। इलेक्ट्रॉनिक डाक सर्वाधिक प्रचलित उपकरण है जो लोगों की टेलीफोन

निर्भरता को कम करता है एवं संवादों का आदान-प्रदान करता है। ई-डाक दो तरह के हो सकते हैं- इंटरनेट ई-डाक व गैर इंटरनेट डाक। वर्तमान ई-डाक प्रणाली तेजी से और कम खर्च में डाक भेजने का साधन है।

कैसे काम करता है इंटरनेट?

इसके बाद महत्वपूर्ण हैं डाक सूचियां, सूची सेवाएं और बुलेटिन बिलबोर्ड। बुलेटिन बोर्ड के द्वारा कोई प्रयोक्ता होस्ट कम्प्यूटर से जुड़ता है। इंटरनेट से जुड़कर हम नेटवर्क पर एक समाचार बुलेटिन भी प्राप्त कर सकते हैं और उसे दूसरे कम्प्युटर से जोड़ सकते हैं। आर्ची एक अन्य उपकरण है जो एफ टी.पी. स्थलों को ढूंढने में मदद करता है। वेब के प्रचलित होने के कारण मोफर आँकडों को व्यवस्थित कर वेब स्थलों में बदला जा रहा है। 'आई.सी.क्यू' और 'आई.आर.सी' ऐसे कार्यक्रम हैं, जो आन लाईन वार्तालाप के लिए इटरनेट से जुड़े मित्रों की तलाश करने में प्रयोक्ता को मदद करते हैं। इसमें टंकित शब्दों के माध्यम से दूसरों से बातचीत की जाती है। किसी भी व्यवसाय के मुख्यतः तीन पहलू होते हैं- उत्पादों का विपणन, शरीद-बिक्री का लेखा-जोखा और सेवा या उत्पाद की प्रस्तुति। इंटरनेट से जुड़कर प्रयोक्ता व्यवसायिकता के तीनों पहलुओं का आंकिक सम्पर्क प्राप्त करता है। इंटरनेट की व्यापकता के कारण इलेक्ट्रॉनिक वाणिज्य का बाजार किसी भी भौगोलिक सीमा से मुक्त होकर परिवर्द्धित होता है । उपभोक्ता व व्यवसायी बिना शारीरिक परिश्रम के कम से कम समय में व्यापारिक मामले तय कर सकते हैं। सभी प्रशासनिक फैसले अब इंटरनेट से जुड़े कम्प्यूटरों पर होते हैं और योजनाओं के क्रियान्वयन के लिए समुचित उपाय की भी जानकारी प्राप्त होती है। ग्राम पंचायतों को भी इंटरनेट से जोड़ दिया गया है। इससे ग्रामीण लोगों को सूचनाओं की सरल प्राप्ति हो सके। व्यक्तिगत लाभ से लेकर जनकल्याण तक की दृष्टि से इंटरनेट पर उपयोगी सामग्री प्राप्त हो रही है। इंटरनेट से जुडा विश्व समुदाय एक प्रजातांत्रिक वैज्ञानिक व्यवस्था में सूचना शक्ति का बराबर हकदार बनकर काम करने में यकीन रखता है। लेकिन कुछ लोग गलत इरादों को हासिल

करने के लिए इसका मनमाने तरीके से इस्तेमाल करने पर अमादा हैं।

देश में जहाँ अभी भी बिजली, पानी, आवास, साक्षरता, स्वास्थ्य सुविधा, पोषक भोजन आदि की समस्या है। गांवों में सामुदायिक कम्प्यूटर के जरिए लोगों को सजग और सबल बनाने की कोशिश की जा रही है। हम इंटरनेट पर दुनिया के किसी भी कोने में रहने वाले अपने मित्र से बातचीत कर सकते हैं। विभिन्न दुकानों मे बिकने वाली वस्तुओं को देख सकते हैं और ऑर्डर कर सकते हैं। मंडियों और शेयर बाजार पर नजर रख सकते हैं और सेवाओं का विज्ञापन कर सकते हैं। इंटरनेट पर हम न केवल अखबार पढ़ सकते हैं बल्कि पुस्तकालयों से जरूरी सूचना प्राप्त कर सकते हैं। ठीक उसी प्रकार इंटरनेट के द्वारा पूरे विश्व में कहीं से किसी कोने में सूचना तीव्र गति से दी और ली जा सकती है। इस प्रकार यह कहा जा सकता है कि इंटरनेट विश्व गांव की संकल्पना को साकार कर रहा है।

इंटरनेट : जड़ से जहां तक

सूचना क्रान्ति मानव की अभूतपूर्व उपलब्धि है जो उसकी असीम सृजनात्मक शक्तियों से भी परिचित कराती है। इसने विश्वव्यापी भागदौड़ तथा दुतगामी विकास को एक नया फलक प्रदान किया है। इस क्रान्ति के फलस्वरुप भौगोलिक तथा राजनीतिक सीमाओं से आबद्ध सकीर्णताएँ अपने दायरे से बाहर आई हैं तथा विश्व स्तर पर ज्ञान विज्ञान तथा संवाद के लिए एक मंच प्रस्तुत किया है। इसकी महत्ता, उपयोगिता तथा विस्तार को देखते हुए इसे "सूचना क्रान्ति" के नाम से सम्बोधित किया गया है। सूचना क्रान्ति के व्यापक विस्तार से अब सम्पूर्ण विश्व एक वैश्विक गाँव के रूप में बदल गया है। आधुनिक सूचना क्रान्ति वैज्ञानिक चक्र के तीसरे चरण को पूर्ण कर चौथे चरण में प्रवेश कर रही है तथा विश्व समुदाय तेजी से आगे बढ़ रहा है। इससे प्रतीत होता है कि वर्तमान युग केवल सूचना युग ही है। जिसके पास जितनी अधिक सूचना है, वह उतना ही ज्ञानवान है और जो अपनी जानकारी का

जितना अधिक उपयोग कर सकता है, वह उतना ही अधिक शक्ति सम्पन्न है। आधुनिक सूचना क्रान्ति का सूत्रपात प्रसिद्ध वैज्ञानिक आर्थर सी.क्लार्क की एक विज्ञान कथा 'संचार उपग्रह' की कल्पना से शुरु हुआ। सूचना के क्षेत्र में सबसे प्राचीन तकनीक टेलीग्राफ थी। वर्ष 1876 में ग्राहमबेल ने टेलीफोन का अविष्कार किया। तत्पश्चात् वर्ष 1901 में मार्कोनी द्वारा "बेतार तकनीक" के अविष्कार के बाद तार की आवश्यकता ही समाप्त हो गई तथा सूचना सम्प्रेषुण तार की सीमा से बाहर निकल गयी। टेलीविजन के आविष्कार से दृश्य व श्रव्य दोनों माध्यमों का सम्प्रेषण सम्भव हुआ। वैज्ञानिक आविष्कारों एवं खोजों की श्रृंखला में रेडियो, टेलीफोन, टेलीविजन, कम्प्यूटर, इंटरनेट, प्रिन्टर, मोबाइल फोन, पेजर, कम्पजैंस पद्धति आदि ने इसको क्रान्तिकारी स्वरूप प्रदान किया जिससे ग्लोबल विलेज की संकल्पना मूर्त रूप लेती दिखाई दे रही है। सूचना क्रान्ति ने मानव जीवन के विविध पक्षों को अभूतपूर्व रूप से प्रभावित किया' है। वर्तमान में घर बैठे देश-विदेश की सूचनाएं पल-पल ग्रहण कर रहे हैं। व्यापार जगत्, शिक्षा, समाचार तंत्र, अंतर्राष्ट्रीय वाणिज्य, मनोरंजन, स्वास्थ्य और सरकारी कामकाज आदि कोई भी क्षेत्र कम्प्यूटर और सूचना तकनीक के उपयोग से अछूता नहीं रहा है। देश विदेश के आर्थिक क्षेत्र ने इसका भरपूर लाभ उठाया है। बैकिंग, बीमा, उद्योग, वाणिज्य-व्यापार, चिकित्सा, शिक्षा आदि क्षेत्रों में सूचना प्रौद्योगिकी के नवीनतम प्रयोगों ने आमूलचूल परिवर्तन ला दिया है।

तकनीकी उपकरणों में कम्प्यूटर आज हमारे जीवन का एक महत्वपूर्ण अंग बन चुका है। लेकिन विकास की दौड़ में इतना आगे निकलने के बाद अब हमें कुछ सावधानियों की भी ज़रुरत महसूस होने लगी है। इसका प्रमुख कारण कम्प्यूटर की तीव्रगति, विपुल संग्रह क्षमता, अतिशुद्धता व सक्षमता है । कम्प्यूटर पर इंटरनेट कनेक्शन ने विश्व के लोगों को आपस में जोड़ने का कार्य किया है, जिससे लोगों का कम्प्यूटर की तरफ रुझान बढ़ रहा है। जब सारा विश्व ही सूचना क्रान्ति से प्रभावित है यहां तक कि दैनिक जीवन में भी इस क्रान्ति का असर हो रहा है, तो आवश्यकता इस बात की है कि

आम आदमी तक सूचना क्रान्ति का लाभ सुरक्षित तरीके से पहुँचाया जाए तथा लोगों तक कम्प्यूटर की पहुंच बढ़ाई जाए साथ ही उन्हें किसी भी तरह के संभावित खतरे से भी बचाया जाए। इस समस्या का हल खोजने के लिए भारत तथा अन्य कई देशों में भरसक प्रयास किए जा रहे हैं। एक प्रयास है कम्प्यूटर की कीमतें कम करना तथा ऐसे उपकरण विकसित करना जिससे आम आदमी इंटरनेट से जुड़ा जा सके। इंटरनेट के जरिए आम आदमी को पास लाने की कोशिश का नाम है साइबर कैफे। जिसका तात्पर्य है एक सामुदायिक कम्प्यूटर जिसका वे सभी लोग प्रयोग कर सकें जिनके पास कम्प्यूटर उपलब्ध नहीं है। शहरों में हर किसी के पास इंटरनेट है लेकिन सुदूर गांवों में हर किसी के पास यह सुविधा उपलब्ध नहीं है।

साइबर कैफे और आम आदमी

'साइबर कैफे 'के प्रति लोगों का बढ़ते आकर्षण का कारण है इंटरनेट। इसमें विश्वभर की विस्तृत सूचना एकत्र की जाती है। इंटरनेट का कनेक्शन रखने वाला व्यक्ति किसी भी समय, किसी भी विषय पर तत्काल जानकारी प्राप्त कर सकता है। वास्तव में इंटरनेट विभिन्न नेटवर्कों का एकीकरण रूप ही है। इसकी लोकप्रियता का प्रमुख कारण यह है कि इस समूह का कोई भी प्रभावी (इंचार्ज) नहीं होता दूसरे इस सिस्टम में कोई सेन्सरशिप नहीं है। इंटरनेट पद्धति में सम्पूर्ण सूचनाएं कम्प्यूटरों में भरी होती हैं, इन्हें तकनीकी भाषा में 'वेबसर्वर ' कहा जाता है। ये सभी कम्प्यूटर एक-दूसरे से जुड़े होते हैं और सम्पूर्ण जाल को वर्ल्ड वाइड वेब (www) के नाम से जाना जाता है । इस पूरी प्रणाली ने प्रत्येक (व्यक्तिगत कम्प्यूटर सहित) कम्प्यूटर में निहित जानकारी को 'होम पेज ' के नाम होम पेज को एक पुस्तक, वेबसाइट को पुस्तक अलमारी और वेबसर्वर को पुस्तकालय के रूप में देखा जाए, तो इंटरनेट सिस्टम को लाखों पुस्तकालयों से बनी एक विशाल लाइब्रेरी के रूप में जाना जा सकता है। इंटरनेट हमें अनेक सुविधाएँ भी प्रदान करता है। ई-मेल द्वारा इटरनेट से जुड़े किसी कम्प्यूटर को तत्काल सूचना सम्प्रेषित कर सकते

हैं और वह कम्प्यूटर उस सूचना को मुद्रित तथा आवश्यकतानुसार सुरक्षित रख सकता है। वाणिज्य-व्यापार के क्षेत्र में ई-कामर्स तथा ई-बिजनेस का भरपूर लाभ लिया जा रहा है। इसके माध्यम से वस्तुओं के विज्ञापन एवं क्रय-विक्रय तथा बीमा, उद्योग, व्यापार से सम्बन्धित अनेक महत्वपूर्ण कार्य किए जा रहे हैं। यूनेट की सहायता से नेटवर्क में निहित सूचनाओं के भण्डार को किसी विषय पर रुचि रखने वाले व्यक्तियों से सूचनाओं का आदान-प्रदान एवं विचार विमर्श कर सकते हैं । वीडियो कान्फ्रेनिसिंग के माध्यम से हजारों किमी, दूर कम्प्यूटर स्क्रीन पर बैठे दो व्यक्ति एक-दूसरे से बातचीत कर सकते हैं। मोबाइल फोन और सेटेलाइट फोन सूचना सम्प्रेषण का एक लोकप्रिय माध्यम है। वर्तमान में इस प्रणाली में 'वैप ' नामक तकनीक का समायोजन करके और अधिक सक्षम बना दिया है। इसके अतिरिक्त वर्ल्ड वाइड वेब, टेलनेट, ई फैक्स, मल्टी मीडिया इनमार सेट, पेजर इत्यादि के माध्यम से मानव विभिन्न क्षेत्रों से लाभ उठा रहा है ।

इंटरनेट के फायदे

चिकित्सा के क्षेत्र में सूचना तकनीक ने अभूतपूर्व क्रान्ति मचा दी है। इसके जरिए डॉक्टर दूर स्थित मरीजों को टेलीकम्युनिकेशन एवं सूचना तकनीकी के माध्यम से जाँच कर सकता है तथा रोगों का निदान कर सकता है। इस प्रक्रिया में डॉक्टर मरीज की ई.सी.जी, एक्सरे कैट स्कैन (CAT-SCA N) एम आर आई (MRI) इत्यादि की तस्वीरें कम्प्यूटर वीडियो फाइल खोलकर जाँच कर सकते हैं । इतना ही नहीं डिजिटल कैमरे का प्रयोग करके डॉक्टर मरीज के अन्दरूनी अंग-प्रत्यंगों की जाँच भी कर सकता है ।

इसके अतिरिक्त जन कल्याण के क्षेत्र में भी इंटरनेट महत्वपूर्ण भूमिका निर्वाह कर रहा है। विकास कार्यक्रमों के लिए यह आवश्यक है कि सरकार एवं जनता के मध्य सरल सम्प्रेषण हो जिससे कार्यक्रमों के समुचित रूप से नियन्त्रण एवं निर्देशन हो सके। विश्व के अधिकांश देश इस सुविधा का

लाभ उठा रहे हैं। भारत भी इससे अछूता नहीं है। भारत सरकार ने ग्रामीण विकास एवं गरीबी उन्मूलन कार्यक्रमों का निरीक्षण करने के लिए 1985 में "कम्प्यूटरीकृत" ग्रामीण सूचना प्रणाली की शुरुआत की। अंतरिक्ष में स्थापित उपग्रहों से प्राप्त सूचना एवं आकड़ों का विश्लेषण कर मानसून, वर्षा, तूफान, चक्रवात तथा हिमपात की पूर्व सूचना से कृषि विकास को एक नई दिशा प्राप्त हुई है। आज टेलीफोन नेटवर्क के माध्यम से करोड़ों किसान सीधे मण्डियों से जुड़ गए हैं तथा भाव के उतार-चढ़ाव का विश्लेषण करके समुचित लाभ ले रहे हैं, जो इंटरनेट की उपयोगिता को सिद्ध करता है। इंटरनेट ने वाणिज्य तथा व्यापार के क्षेत्र में क्रान्ति ला दी है। ग्राहकों को अपनी व्यस्त दिनचर्या में से समय निकालकर शहर के ट्रैफिक वाले डिपार्टमेन्टल स्टोर, बैंक, शेयर बाजार या वित्तीय संस्थाओं तक आने-जाने की तकनीक से इंटरनेट ने मुक्ति दिलाई है । यह सब इंटरनेट पर व्यापार के कारण सम्भव हो सका जिसे ई-कॉमर्स के नाम से जानते हैं। एक आकलन के अनुसार वर्ष 2000 में इंटरनेट के माध्यम से ई-कॉमर्स द्वारा लगभग 45 खरब रुपयों का व्यापार हुआ। ई-कॉमर्स से समान व सेवाओं की ऑन लाइन खरीद फरोख्त की जाती है । इस सेवा में सुई से लेकर हैलीकॉप्टर तक के क्रय विक्रय के लिए वेबसाइट उपलब्ध हैं। ई-मेल की तर्ज पर ई-कॉमर्स की शुरुआत हुई है।

यह सेवा चौबीसों घण्टे उपलब्ध रहती है । ई-कॉमर्स की सफलता अभी शुरुआती दौर में है। मगर व्यापार में ग्राहक बढ़ाने और उत्पादकता में वृद्धि के लिए यह सबसे अच्छा व लोकप्रिय तरीका है। आने वाले समय में शायद ही कोई कारोबार होगा जिसका अपनी वेबसाइट न हो । इसके प्रमुख गुणों में व्यापार में दूरी का अत्यधिक कम होना, समय में कमी, न्यूनतम लागत 365 दिनों के चौबीसों घण्टे क्रय-विक्रय करना, नई वस्तु/सेवा का नाम जोड़ना, घटाना, सरल, गलतियों की आशंका कम, व्यापक चुनाव का अवसर, शादी जैसे कार्य भी सम्भव हैं। हालांकि ई-कार्मस के तमाम लाभों के साथ-साथ ऐसी समस्याएं भी हैं, जो इसके विकास में बाधक हैं जैसे वस्तु को हाथ में लेकर नहीं देखना, सामाजिक सम्पर्कों में कमी, कम्प्यूटर तथा पैसे में गड़बड़ी

की सम्भावना, ग्राहक का शिक्षित होना, उच्च व निम्न वर्ग में अन्तर, प्रशिक्षण का अभाव आदि।

इंटरनेट का नकारात्मक प्रभाव

सूचना क्रान्ति की तकनीक ने जहाँ मानव के भौतिकवादी जीवन को सुखद अनुभूतियों से भर दिया है, वहीं दूसरी ओर उसके संस्कृति, सभ्यता, जीवन मूल्यों, इत्यादि को संकट में डाल दिया है। मानव जीवन के विविध पक्ष जहां इससे समृद्ध हुए हैं, वहीं इस क्रान्ति ने उन लोगों के सांस्कृतिक जीवन को गहरा आघात पहुँचाया है जो विश्व के अनेक दुर्गम क्षेत्रों में शताब्दियों से अपने सांस्कृतिक अस्तित्व को संजोकर रखे हैं।

इंटरनेट पर साइबर सेक्स एक आम बात हो गई है । बटन दबाते ही हजारों अश्लील दृश्य सामने प्रत्यक्ष हो जाते हैं। आज खुलेआम अनेक विज्ञापन के माध्यमों से टेलीफोन पर " वाकसेक्स " को प्रोत्साहन दिया जाता है। इंटरनेट पर युवक और युवतियों के लिए अनेक वेबसाइट खोले गए हैं जो परोक्ष रूप से सेक्स अपराध को बढ़ावा दे रहे हैं।

इंटरनेट ने अपराध जगत को बहुत संरक्षण प्रदान किया है। अनेक आतंकवादी संगठन बेवसाइटों का प्रयोग कर भड़काऊ उद्देश्यों, लक्ष्यों एवं कार्यक्रमों द्वारा समाज में घृणा, द्वेष तथा आतंक का माहौल फैला रहे हैं। सूचना तकनीक आतंकवादी संगठन के सदस्यों में वृद्धि तथा सहयोग एवं समर्थन प्राप्ति का भी साधन बन गया है। पेशेवर अपराधी टेलीफोन, इंटरनेट, मोबाइल का प्रयोग धमकी देने के नये माध्यम के रुप में कर रहे हैं। यही नहीं अपराध को अन्तिम रूप देने में भी यह कारगर साबित हो रही है। अपराध के अंतर्राष्ट्रीयकरण में इंटरनेट कारगर भूमिका निभा रहा है। अंडरवर्ल्ड की दुनिया में इंटरनेट के जरिए ही अपराधियों को आपस में जोड़ा जाता है और उसके बाद इसी का इस्तेमाल कर लोगों को धमकाया भी जाता है। अधिक तकनीकी उपकरणों के प्रयोग ने स्वास्थ्य को प्रभावित किया है। व्यक्ति

की स्मरण शक्ति कमजोर होती जा रही है । कम्प्यूटर के स्क्रीन से निकलने वाली चमक से आखों पर बुरा प्रभाव पड़ता है। " सूचना क्रान्ति " पर मानव की बढती हुई निर्भरता ने अनेक समस्याओं को जन्म दिया है। इस दिशा में तत्काल प्रयास किए जाने की आवश्यकता है। थोड़ी-सी गलती अनेक बड़ी समस्याओं को जन्म दे सकती है। साइबर अपराध के अन्तर्गत गुप्त सूचनाओं को चुराना आम बात हो गई है जिसे हम हैकिंग के नाम से भी जानते हैं। हैकिंग के द्वारा अवांछित तत्व किसी भी गुप्त संदेशों जैसे-लोगिन, पासवर्ड, क्रेडिट कार्ड नम्बर आदि को प्राप्त करने की कोशिश करते हैं, आज के शिक्षा प्रणाली में नकल रोकना जापान सरकार के लिए एक चुनौती बन गया है। सूचना तथा तकनीकी के क्षेत्र में महारत हासिल करने वाले अमेरिका को उस समय गहरा धक्का लगा जब उसे पता लगा जब उसके रक्षा एवं प्रतिरक्षा सम्बन्धित गोपनीय दस्तावेज की चोरी हो गई।

सूचना तकनीक ने विश्व में नए-नए अपराधो को जन्म दिया है जिससे इसके अस्तित्व पर संकट के बादल मंडराने लगे हैं। अत: इन सब तथ्यों पर विचार कर हमें इस बात के लिए सोचना होगा कि विज्ञान के नवीनतम अनुप्रयोग 'सूचना क्रान्ति ' का प्रयोग किस प्रकार किया जाए, जिससे इस प्रणाली से उत्पन्न होने वाले घातक परिणामों से हमें मुक्ति मिल सके।

साइबर सुरक्षा भविष्य की ज़रुरत

साइबर सुरक्षा इन दिनों चर्चाओं और खबरों में है । इससे जुड़ी दो महत्वपूर्ण घटनाएं पिछले दिनों घटी-चीन के मिलिट्री हैकरों ने पश्चिमी देशों की सरकारों की कम्प्यूटर प्रणाली पर हमला बोला और अमेरिकी एयर फोर्स ने साइबर स्पेस कमान नाम के संगठन का गठन किया। इसे संयोग ही कहा जाएगा कि दोनों घटनाएं एक ही समय हुई, लेकिन इनसे इक्कीसवीं सदी में साइबर प्रणाली से जुडे खतरों की वास्तविकता और भयावहता का अनुमान लगाया जा सकता है । आज रोजमर्रा की कार्यप्रणाली में साइबर स्पेस का दायरा

उत्तरोत्तर बढ़ता ही जा रहा है । सरकारें, प्रशासन, शिक्षा, संचार और सूचना के विस्तार में इसका बढ़-चढ़कर इस्तेमाल हो रहा हैं। दूसरी ओर आंतकी समूह साइबर तकनीक का उपयोग अपने प्रचार, विभिन्न गुटों के साथ समन्वय तथा अर्थ प्रबंधन के लिए कर रहे है। साइबर तकनीक का इस तरह दुरुपयोग देखते हुए अब विशेषज्ञ भी खासे चिंतित हैं । आज कम्प्यूटर का उपयोग करने वाला हर व्यक्ति कम्प्यूटर वायरस के हमले के बारे में जानता है। जब यह खतरा बड़े पैमाने पर हो तो इसकी भयावहता और दुष्परिणाम के बारे में सहजता से समझा जा सकता है।

आज रेलवे, एयरलाइंस, बैंक, स्टॉक मार्केट, हॉस्पिटल के अलावा आम जनजीवन से जुड़ी हुई सेवाएं कम्प्यूटर नेटवर्क से जुडी हैं, इनमें से तो कई पूरी तरह से इंटरनेट पर ही आश्रित हैं, यदि इनके नेटवर्क के साथ छेड़-छाड़ की गयी, तो क्या परिणाम हो सकते हैं यह बयान करने की नहीं अपितु समझने की बात है। अब तो सैन्य-प्रतिष्ठानों का काम-काज और प्रशासन भी कम्प्यूटर नेटवर्क के साथ जुड़ चुका है । जाहिर है कि यह क्षेत्र भी साइबर आतंक से अछूता नहीं बचा है । इसीलिए सूचना तकनीक के विशेषज्ञ साइबर सुरक्षा को लेकर बेहद चिंतित हैं । साइबर स्पेस एक ऐसा क्षेत्र है जहां बिना किसी खून-खराबे के किसी भी देश की सरकार को आंतकित किया जा सकता है। साइबर के जरिए आतंक फैलाने वाले, कम्प्यूटर से महत्वपूर्ण जानकारियां निकाल सकते हैं तथा इसका इस्तेमाल धमकी देने व सेवाओं को बाधित करने में कर सकते हैं। अभी सामान्य तौर पर साइबर अपराध के जो छोटे-मोटे अपराध सामने आते हैं, वह प्राय: युवा या विद्यार्थी वर्ग द्वारा महज मजा लेने या खुराफात करने के होते हैं, यदि इन्हीं तौर-तरीकों का उपयोग व्यापक पैमाने पर आतंकवादी समूह करने लगें तो भारी मुश्किलें खड़ी हो जायेंगी। यह सही है कि साइबर से जुड़ी अभी तक कोई बड़ी आतंकवादी घटनाएं प्रकाश में नहीं आई हैं, पर इसका यह मतलब कतई नहीं कि आने वाले दिनों के एक साधारण से मामले से लगा सकते हैं। वर्ष 1998 में एक बारह वर्षीय बालक ने अमेरिका के अरिजोना स्थित थियोडोर रुजवेल्ट डैम की कम्प्यूटर

प्रणाली को हैक कर उस पर अपना नियंत्रण स्थापित कर लिया। इस प्रणाली के जरिए बाढ़ नियंत्रण व बांध के गेट का संचालन किया जाता था। यदि वह हैकर चाहता तो कभी भी बांध के गेट खोल सकता था और इससे कितनी बड़ी आबादी में तबाही मच सकती थी बताने की जरूरत नहीं। आज इस बात की पुख्ता खुफिया खबरें हैं कि अलकायदा जैसे कई खतरनाक आतंकवादी संगठन साइबर स्पेस के जरिए दुनिया भर में आतंक फैलाने की फिराक में हैं । ऑन-लाइन से जुड़े आतंकवाद के खतरों को अमेरिका के तत्कालीन राष्ट्रपति बिल क्लिंटन ने वर्ष 1996 में ही भांप लिया था और उन्होंने तभी इस चुनौती से निपटने के लिए क्रिटिकल इन्फ्रास्ट्रक्चर प्रोटेक्सन कमीशन का गठन किया था। साइबर स्पेस में आतंकवाद की घुसपैठ का एक महत्वपूर्ण पहलू यह है कि भविष्य में होने वाले युद्धों और संघर्षों में यह एक भयावह वास्तविकता के रूप में उभरकर सामने आ सकता है। साइबर आतंकवादी नई संचार तकनीक के औजारों और तौर-तरीकों का इस्तेमाल करके नेटवर्क को तहस-नहस कर सकते हैं, हैकिग के साथ ही कम्प्यूटरों को बड़े पैमाने पर वायरस से संक्रमित कर सकते हैं, ऑनलाइन नेटवर्क सेवाओं को बाधित कर सकते हैं। यही नहीं वे सरकारों व प्रतिष्ठानों के महत्वपूर्ण ई-मेल पर भी दखल दे सकते हैं। कोई कम्प्यूटर हैकर आंतकवादियों के साथ मिलकर साइबर से जुड़ी किसी भी खतरनाक घटना को अंजाम दे सकता है। आज जब यह सच दुनिया के सामने आ ही गया है कि आंतकवाद के खूनी खेल में पढे-लिखे विषय विशेषज्ञ, आईटी और मेडिकल के होनहार युवक भी शामिल हो चुके हैं, तो ऐसे में इनकी प्रतिभा का इस्तेमाल नागरिक और सैन्य क्षेत्र के साइबर नेटवर्क को भेदने में सहजता से किया जा सकता है। वैसे तो अभी दुनिया भर के सभी सैन्य संगठन किसी भी तरह के साइबर हमले से बचने के लिए एक सहज तरीका इस्तेमाल करते हैं कि वे अपनी सूचनाओं को इंटरनेट के साथ नहीं जोड़ते, लेकिन यह व्यवस्था भी अभेद्य नहीं है।

साइबर फॉरेंसिक : ज़रुरी नहीं वक्त की मजबूरी है

सेनाएं शांतिकाल में व युद्ध के समय अपने अभियानों को अंजाम देने के लिए इंटरनेट पर तेजी से आश्रित होती जा रही हैं। आज साइबर आतंकवाद और उससे जुड़े अपराधों को गंभीरता से लेते हुए अमेरिका ने साइबर स्पेस कमान गठित करके नई सदी की इस चुनौती से निपटने के लिए कमर कस ली है। भारत जैसे राष्ट्र को भी अपनी सुरक्षा व्यवस्था को चाक-चौबंद करने के लिए ऐसे ही इंतजामों की दरकार है। सौभाग्य से भारत में आईटी के ऐसे बहुत से विशेषज्ञ हैं, जिनकी सेवाएं साइबर आतंकवाद की चुनौती से निपटने के लिए ली जा सकती हैं। सरकार को चाहिए कि नागरिक और सैन्य क्षेत्र की सुरक्षा को देखते हुए वह साइबर फॉरेंसिक की ऐसी नीति व कार्य-योजना तैयार करे, जिससे समय रहते ही आईटी और साइबर से जुड़े अपराधों व आतंक की संभावनाओं से निपटा जा सके।

जिस प्रकार से देश में कम्प्यूटर और इंटरनेट का प्रचलन बढ़ा है, उसके बाद से इस क्षेत्र में अपराध भी तेजी से बढ़े हैं। यही वजह है कि कम्प्यूटर फोरेंसिक का क्षेत्र काफी तेजी से उभरा है। इस समय देश में इंटरनेट का प्रयोग करने वालों की संख्या जितनी तेजी से बढ़ी है, उतनी ही तेजी से ऑनलाइन और साइबर अपराध से जुड़े मामले भी प्रकाश में आने लगे। इनमें ऑनलाइन क्रेडिट कार्ड घोटाला प्रमुख है। इसके अलावा ई-मेल से जुड़ी आपराधिक घटनाओं में भी लगातार बढ़ोतरी हो रही है। इसमें खासकर फर्जी और धमकी भरे ई-मेल भेजना, कंपनियों के साथ धोखाधड़ी, सॉफ्टवेयर की चोरी, एसएमएस हैकिंग, मोबाइल की क्लोनिंग आदि शामिल हैं। इन सबको देखते हुए ही कम्प्यूटर और नेटवर्क सुरक्षाओं पर ज्यादा ध्यान दिया जाने लगा है। यही वजह है कि इन दिनों कम्प्यूटर एक्सपर्ट एवं डिजिटल फोरेंसिक विशेषज्ञों की मांग बढ़ गई है।

आमतौर पर कम्प्यूटर फोरेंसिक विशेषज्ञों को साइबर पुलिस, साइबर

अन्वेषक या डिजिटल डिटेक्टिव भी कहा जाता है। प्रत्येक व्यक्ति साइबर अपराध का कहीं-न-कहीं शिकार होता ही रहता है। सबकुछ साइबर होता जा रहा है, इसलिए इंटरनेट पर सूचना की सुरक्षा को कायम रखने की चिंता भी बढ़ रही है। ऐसे में कानून से जुड़े क्षेत्र से लेकर सूचना प्रौद्योगिकी तक लगभग प्रत्येक क्षेत्र में रोजगार की जबरदस्त संभावनाएं हैं। यह क्षेत्र अपने आपमें काफी विस्तृत है, इसमें टेक्नोलॉजी और कानून दोनों की जानकारी होना चाहिए। कम्प्यूटर और साइबर अपराध के तहत छात्रों को साइबर अपराध से जुड़े विभिन्न पहलुओं से अवगत कराया जाता है, जिसमें कम्प्यूटरीकृत और नेटवर्क प्रचालनों में विभिन्न प्रकार के जोखिमों को समझना, कम्प्यूटर अपराध से जुड़े सुराग की पहचान करना, कम्प्यूटर अपराधों की जांच के पहलुओं के बारे में जानना, कम्प्यूटर से जुड़े अपराधों की रोकथाम के विभिन्न उपायों को समझना और कभी-कभी होने वाले साइबर नुकसान को सीमित रखने के लिए सुरक्षा तकनीकों से परिचित होना शामिल हैं। ई-कॉमर्स और मोबाइल के माध्यम से पैसों का ट्रांसफर करना भी अब हम अपने आसपास देख रहे हैं। ऐसे में किस प्रकार से ऑनलाइन धोखाधड़ी को रोका जा सकता है, यह भी इस विषय के अंतर्गत प्रमुख रूप से सिखाया जाता है।

डिजिटल सबूत

आमतौर पर किसी भी अपराध के होने पर उससे संबंधित सबूत को इकठ्ठा किया जाता है। इस विषय के अंतर्गत डिजिटल सबूत कैसे इकठ्ठा कर सकते हैं, इसका विशेष प्रशिक्षण दिया जाता है। अब कम्प्यूटर के अलावा मोबाइल के माध्यम से कम्प्यूटर से जुड़े सभी कार्य होते हैं। इस कारण इस विषय के अंतर्गत अब खासतौर पर मोबाइल से जुड़े अपराधों को भी शामिल किया जाने लगा है। मोबाइल क्लोनिंग से लेकर इसके माध्यम से होने वाले अपराधों के बारे में भी जानकारी दी जाने लगी है। इस क्षेत्र में विशेषज्ञता हासिल करने के बाद सरकारी और निजी दोनों ही क्षेत्रों में समान रूप से रोजगार के अवसर प्राप्त हो सकते हैं। आप सलाहकार के रूप में भी काम कर

सकते हैं, इसके अलावा कई बहुराष्ट्रीय कंपनियां इस प्रकार के लोगों को बतौर विशेषज्ञ भी रखती हैं। निम्नलिखित विश्वविद्यालयों में इसकी पढाई होती है:-

- एमिटी यूनिवर्सिटी, नोएडा, उत्तरप्रदेश
- ऑल इंडिया इंस्टिट्यूट ऑफ स्पीच एंड हीयरिंग, मैसूर, कर्नाटक
- बुंदेलखंड विश्वविद्यालय, झांसी, उत्तरप्रदेश

इंटरनेट पर धोखाधड़ी : क्या है उपाय?

इंटरनेट पर लोगों के साथ बड़े पैमाने पर धोखाधड़ी की घटनाएं सुनने को मिलती है, परंतु समस्या यही होती है कि आखिर इसकी शिकायत किसे करें? पुलिस विभाग से लेकर अन्य कई जगहों पर अब साइबर अपराधों को लेकर जागृति आ रही है। यही कारण है कि साइबर अपराध विशेषज्ञों की मांग भी बढ़ती जा रही है। तत्कालीन गृह मंत्री राजनाथ सिंह ने फ़रवरी 2019 में, राष्ट्रीय साइबर फॉरेंसिक प्रयोगशाला तथा CyPAD (Cyber Prevention, Awareness & Detection Centre) का उद्घाटन किया था। राष्ट्रीय साइबर फॉरेंसिक प्रयोगशाला भारतीय साइबर अपराध सहयोग केंद्र (I4C) पहल का हिस्सा है। CyPAD दिल्ली पुलिस की साइबर अपराध इकाई है।

साइबर रोकथाम, जागरूकता व खोज केंद्र (CyPAD)

साइबर रोकथाम, जागरूकता व खोज केंद्र (CyPAD) नागरिकों, पुलिस इकाइयों तथा दिल्ली के एजेंसियों को फॉरेंसिक, साइबर सुरक्षा तथा सुरक्षा सम्बन्धी सेवाएं उपलब्ध करवाएगा। यह केंद्र क्रिप्टोकरेंसी फ्रॉड, तकनीक से सम्बंधित अंतर्राष्ट्रीय धोखाधड़ी तथा साइबर सुरक्षा से सम्बंधित पहलुओं

पर कार्य कर रहा है।

राष्ट्रीय साइबर फॉरेंसिक प्रयोगशाला

राष्ट्रीय साइबर फॉरेंसिक प्रयोगशाला केन्द्रीय गृह मंत्रालय के अधीन भारतीय साइबर अपराध सहयोग केंद्र (I4C) पहल का हिस्सा है। राष्ट्रीय साइबर फॉरेंसिक प्रयोगशाला मेमोरी फॉरेंसिक लैब, इमेज एनहांसमेंट लैब, नेटवर्क फोरेंसिक लैब, मैलवेयर लैब, क्रिप्टोकरेंसी फॉरेंसिक लैब, डैमेजड हार्ड डिस्क तथा एडवांस्ड मोबाइल फॉरेंसिक लैब इत्यादि इकाईयां हैं। भारतीय साइबर अपराध सहयोग केंद्र के सात अंग निम्नलिखित हैं :-

1. राष्ट्रीय साइबर अपराध धमकी विश्लेषण इकाई
2. राष्ट्रीय साइबर अपराध रिपोर्टिंग
3. साइबर अपराध के लिए संयुक्त पड़ताल दल के लिए प्लेटफार्म
4. राष्ट्रीय साइबर फॉरेंसिक प्रयोगशाला इकोसिस्टम
5. राष्ट्रीय साइबर अपराध प्रशिक्षण केंद्र
6. साइबर अपराध इकोसिस्टम प्रबंधन इकाई
7. राष्ट्रीय साइबर अनुसन्धान व नवोन्मेष केंद्र

साइबर बुलिंग

साइबर बुलिंग यानि गंदी भाषा, तस्वीरों या धमकियों से इंटरनेट पर तंग करना:

भारतीय दंड संहिता की धाराओं के तहत कोई भी व्यक्ति किसी धर्म के बारे में आहत करने वाली टिप्पणी नहीं कर सकता। ये कानून दंगों को ध्यान में

रखते हुए बना था। ऐसी टिप्पणियों के लिए उपाय ये है कि ऐसे कमेंट्स के आने पर पुलिस को जानकारी दी जानी चाहिए।

ऐसे कई मामले हैं जहां लोग पुलिस के पास गए हैं और शिकायत दर्ज की गई है। फेसबुक पर भी 'रिपोर्ट अब्यूज़' पर जाकर रिपोर्ट किया जा सकता है। लेकिन मामला अत्यंत गंभीर हो तो पुलिस के पास जाना चाहिए।

अगर किसी की प्रोफाइल पर ना लिखा हो तो उसकी लोकेशन कैसे जानें?

प्रोफाइल लोकेशन का पता लगाने के लिए आपको भाषा पर ध्यान देना होता है कि कोई प्रोफाइल किस तरह की भाषा इस्तेमाल कर रहा हैं। चूंकि फेसबुक में आईपी एड्रेस नहीं खोजा जा सकता इसलिए वकील की मदद लेनी होगी। कोर्ट में फेसबुक के ख़िलाफ केस दायर होता है जो उन्हें मज़बूर करता है कि प्रोफाइल की असली लोकेशन बताई जाए।

फेसबुक पर 'फेक आईडी' और ग़लत आदमी का पता कैसे लगाया जाए?

'फेक आईडी' एक बड़ी समस्या है। 'फेक आईडी' के ज़रिए सेक्स से जुड़े मैसेज भेजते हैं या फिर बहुत खराब भाषा का इस्तेमाल करते हुए धमकी भेजते हैं। जिसके नाम पर ये फेक आईडी हैं अगर आप उस आदमी को जानते हैं या वो आपका परिचित है तो उनसे बात करनी चाहिए और फेसबुक से फेक आईडी की रिपोर्ट की जानी चाहिए। जिसके नाम से फेक आईडी बना है उसकी पुलिस से शिकायत करनी चाहिए।

अगर कोई साइबर बुलिंग करे, तो क्या करना चाहिए?

साइबर बुलिंग से निपटने के दो तरह के विकल्प हैं. कानून की मदद से और निजी स्तर पर।

1. अगर किसी फोरम पर कोई आपको तंग कर रहा है तो उस फोरम से निकल जाइए।

2. अगर फिर भी आपको तंग किया जाए तो फेसबुक को रिपोर्ट करें हालांकि फेसबुक इस पर कोई कार्रवाई नहीं करना।

3. अगर धमकी मिले जैसा कि कविता कृष्णन और मीना कंडासामी को मिली तो इस पर पुलिस में रिपोर्ट दर्ज की जानी चाहिए थी।

4. अगर पुलिस एक्शन न ले तो सीधे वकील के ज़रिए केस दायर किया जा सकता है।

महिलाओं के साथ अगर बुलिंग हो तो वो कानून में किन धाराओं का सहारा ले सकती हैं।

पहला तो सेक्शन 509 कहता है कि शब्द या गतिविधि या संकेत अगर महिलाओं की मॉडेस्टी को भंग करता है तो इसके खिलाफ मामला दर्ज हो सकता है। ये बुलिंग के लिए इस्तेमाल होने वाले शब्दों पर भी लागू होता है। क्योंकि महिलाओं के खिलाफ अभद्र भाषा का इस्तेमाल अपराध है। सेक्शन 66 ए का क्लाज़ बी बुलिंग के लिए ठीक बैठता है। ये कानून इंटरनेट से जुड़े क़ानूनों का हिस्सा है। इनमें तीन साल तक की सज़ा का प्रावधान है। कई बार पुलिस को इन कानूनों के बारे में पता नहीं होता है। ऐसे में प्रिंटआउट लेकर जाएं और उन्हें दिखाएं।

कई बार साइबर प्रोपेगैंडा के मक़सद से किसी इंसान के प्रति गलत अफवाहों को फेसबुक या अन्य सोशल नेटवर्किंग वेबसाइट्स पर फैलाया जाता है। ऐसे मामलों में जब उस संदेश को फेसबुक को "रिपोर्ट एब्यूज़" करके भेजा जाता है तो जवाब आता है कि हमारे मापदंडों के आधार पर कुछ भी गलत नहीं पाया गया". ऐसे मामलों को कैसे निपटा जाए?

फेसबुक ऐसी टिप्पणियों को तवज्जो इसलिए नहीं देता है क्योंकि फेसबुक पर अमरीकी कानून लागू होता है। लेकिन भारतीय कानून के अनुसार ऐसे मामलों में मानहानि का मामला बनता है। सीधे पुलिस में शिकायत होनी चाहिए। इसमें सूचना प्रसारण का कानून भी लग सकता है। ऐसे मामले में दोनों कानून साथ-साथ चलेंगे।

किसी लड़की को गंदे संदेश या गाली कोई भेजे तो ऐसी समस्या से कैसे निपटना चाहिए?

ये संभवत लड़की को परेशान करने का मामला है। पुलिस में रिपोर्ट दर्ज की जानी चाहिए। उसे अपना फेसबुक डिऐक्टिवेट करना चाहिए लेकिन इसके अलावा 'प्राइवेसी सेटिंग्स' में जाकर बदलाव करें ताकि मेसेज भेजने वाले आपको ऐसे संदेश न भेज पाएं।

अगर गंदे संदेश भेजने वाला आदमी आपके फ्रेंड लिस्ट में है तो उसे ब्लॉक किया जा सकता है ताकि वो संदेश न भेज पाए।

साइबर बुलिंग की पुलिस में शिकायत करने के लिए भारत के मौजूदा कानून में भी प्रावधान हैं।

फेसबुक पर अगर कोई ज़बरदस्ती दोस्त बनना चाहे, तो उसे ब्लॉक करने के सिवाय और क्या विकल्प हो सकता है?

आप उस प्रोफाइल को रिपोर्ट कर सकते हैं लेकिन ब्लॉक कर देने पर वो आपको देख नहीं पाएगा तो फिर वो आपको दोस्त बनाने की कोई कोशिश कर ही नहीं पाएगा। फेसबुक से शिकायत भी कर सकते हैं कि ये प्रोफाइल आपको परेशान कर सकता है या कर रहा है।

अध्याय चार

साइबर फॉरेंसिक टूल और डिजिटल प्रौद्योगिकी

साइबर क्राइम के नए तरीके

अश्लील विडियो देखना या वेबकैम से अश्लील विडियो शूट करना आपको परेशानी में डाल सकता है। हाल में आई एक रिपोर्ट में कहा गया है कि दुनियाभर के लाखों यूज़र्स को उनके सेक्स विडियो लीक कर देने की धमकी देकर फिरौती की मांग की जाती है। आपको जानकर हैरानी होगी कि ये पूरा खेल इंटरनेट और ईमेल के जरिए हो रहा है। ग्लोबल साइबर सिक्यॉरिटी फर्म चेकपॉइंट की एक रिपोर्ट के मुताबिक Phorpiex नाम के बॉटनेट का पता लगाया गया है। यह यूज़र्स को हर घंटे 30 हजार ईमेल भेजता है। इसमें सेक्स कॉन्टेंट को लीक करने की धमकी देकर फिरौती की मांग की जाती है। रिपोर्ट में कहा गया है कि पिछले 5 महीनों में Phorpiex के खाते में 110,000 डॉलर ट्रांसफर हुए हैं। Phorpiex को इसलिए खतरनाक माना जा रहा है कि इसे यूज़र के पासवर्ड का भी पता होता है। यह ब्लैकमेल कर फिरौती की मांग करने वाले ईमेल की शुरुआत में ही यूजर को उनके पासवर्ड के बारे में बता कर डरा देता है। गलत तरीके से पैसा कमाने का यह बिल्कुल नया तरीका कहा जा सकता है। इसमें न तो किसी को फोन करने की जरूरत पड़ती है और न ही कहीं जाकर पैसे लेने की। यह पूरा खेल इंटरनेट के जरिए हो रहा है। साइबर क्रिमिनल्स यूज़र को एक ईमेल भेज सेक्स कॉन्टेंट को लीक करने की धमकी देते हैं और ऐसा करने से रोकने के लिए यूज़र्स मजबूरी में उनके खाते में पैसे ट्रांसफर कर देते हैं।

10 साल से सक्रिय है Phorpiex

बताया जा रहा है कि बॉटनेट पिछले 10 साल से सक्रिय है। यह इस वक्त 4 लाख से ज्यादा इंफेक्टेड होस्ट को ऑपरेट करता है। कुछ साल पहले तक Phorpiex अलग-अलग मैलवेयर के जरिए क्रिप्टोकरंसी कमाता था। रिसर्चर्स इसे एक खतरनाक स्पैम बॉट बता रहे हैं जो बड़े स्तर पर सेक्सटॉर्शन कैंपेन चला रहा है। यह बड़ी आसानी से कमांड और कंट्रोल सर्वर से ईमेल अड्रेस के डेटाबेस को कलेक्ट कर लेता है। इसके बाद इन ईमेल अड्रेस में से किसी एक को चुन कर उसे ऐसे ईमेल भेजे जाते हैं। यह स्पैम बॉट हर घंटे ऐसे 30 हजार ईमेल भेज सकता है। ऐसे एक स्पैम से यह एक बार में 2 करोड़ 70 लाख से ज्यादा यूज़र्स को अपना शिकार बना सकता है। रिसर्चर्स का कहना है कि Phorpiex हैकर्स के पास यूज़र्स के ईमेल पासवर्ड पिछले कई सालों में हुए डेटा लीक के कारण मिले हैं।

साइबर क्राइम के कुछ और प्रकार

1. **व्हाइट हैट हैकर्स** - वे मानते हैं कि सूचना साझा करना अच्छा है और जानकारी तक पहुंच को सुविधाजनक बनाने के द्वारा अपनी विशेषज्ञता साझा करने का उनका कर्तव्य है। हालांकि, कुछ सफेद टोपी हैकर ऐसे भी हैं, जो कंप्यूटर सिस्टम पर बस "आनन्द की सवारी" कर रहे हैं।

2. **ब्लैक हैट हैकर्स** - इनके घुसपैठ के बाद नुकसान होना तय है। ये डेटा चोरी या संशोधित कर सकते हैं या वायरस या मैलवेयर डाल देते हैं जो सिस्टम को नुकसान पहुंचाते हैं। उन्हें 'क्रैकर' भी कहा जाता है।

3. **ग्रे हैट हैकर्स** - आमतौर पर नैतिक लेकिन कभी-कभी हैकर के द्वारा नैतिकता का उल्लंघन होता है हैकर्स नेटवर्क, स्टैंड-अलोन कंप्यूटर

और सॉफ्टवेयर को हैक करते हैं। नेटवर्क हैकर्स केवल चुनौती, जिज्ञासा और सूचना के वितरण के लिए निजी कंप्यूटर नेटवर्क पर अनधिकृत पहुंच प्राप्त करने का प्रयास करते हैं। क्रैकर चोरी या जानकारी बदलने या मैलवेयर (वायरस या कीड़े) डालने जैसी क्षति के साथ अनधिकृत घुसपैठ करते हैं।

4. **साइबर स्टॉलिंग** - इस अपराध में किसी को परेशान करने के लिए इंटरनेट का उपयोग करना शामिल है व्यवहार में झूठे आरोप, धमकियां आदि शामिल हैं। आम तौर पर, साइबर स्टॉलर्स के अधिकांश लोग पुरुष हैं और अधिकांश पीड़ित महिलाएं हैं।

5. **स्पैमिंग** - स्पैमिंग इंटरनेट पर अवांछित थोक और व्यावसायिक संदेश भेज रहा है। हालांकि अधिकांश ईमेल उपयोगकर्ताओं को परेशान करते हुए, यह गैरकानूनी नहीं है, जब तक कि यह नेटवर्क के ओवरलोडिंग और ग्राहकों को सेवा में बाधित होने या क्षति पैदा करने के लिए नुकसान का कारण बनता है। इंटरनेट सेवा प्रदाता के प्रति उपभोक्ता दृष्टिकोण पर नकारात्मक असर पड़ता है।

6. **फ़िशिंग** - यह एक इलेक्ट्रॉनिक संचार में एक विश्वसनीय इकाई के रूप में प्रच्छन्न रूप से उपयोगकर्ता के नाम, पासवर्ड और क्रेडिट कार्ड विवरण जैसे संवेदनशील जानकारी प्राप्त करने की एक आपराधिक रूप से धोखाधड़ी की प्रक्रिया है।

7. **सॉफ्टवेयर की चोरी** - व्यापार या व्यक्तिगत उपयोग के लिए यह सॉफ्टवेयर का एक गैरकानूनी प्रजनन और वितरण है। यह प्रतिलिपि का उल्लंघन का एक प्रकार है और इसे लाइसेंस समझौते का उल्लंघन माना जाता है। चूंकि अनधिकृत उपयोगकर्ता लाइसेंस समझौते का पक्ष नहीं है, इसलिए समाधान निकालना मुश्किल होता है।

8. **वेब जैकींग** - शब्द का उपयोग पासवर्ड को क्रैकिंग करने के लिए किया जाता है। इसके तहत किसी वेब साइट पर नियंत्रण के लिए मजबूती के साथ हैकर हमला करता है।

9. **साइबर आतंकवाद** - सरकार को डराने या मजबूर करने के लिए कंप्यूटर संसाधनों का उपयोग, साइबर आतंकवाद कहा जाता है। व्यक्तियों और समूहों ने अक्सर सरकारों को धमकी देने और देश के नागरिकों को आतंकित करने के लिए इंटरनेट के गुमनाम चरित्र का फायदा उठाने का प्रयास किया है।

जैसे-जैसे लोगों की निर्भरता कंप्यूटर के ऊपर बढ़ती जा रही है, वैसे-वैसे साइबर क्राइम भी बढ़ रहा है। ऐसे में साइबर क्राइम पर रोक लगाने के लिए विशेषज्ञों की जरूरत पड़ रही है। सामान्य पुलिस और कानून ऐसे अपराधियों से निपटने में सक्षम नहीं है। इसलिए कुछ मामलों में साइबर फॉरेंसिक एक्सपर्ट के अलावा साइबर लॉ के जानकारों की जरूरत इस तरह के मामलों से निपटने के लिए पड़ती है।

साइबर फॉरेंसिक गुनाह के कुछ प्रकरण

1. IPR Theft प्रकरण : मुंबई

यह प्रकरण एक महिला से सम्बन्धित है जो कि मुम्बई के एक छोटे घर में रहती थी । यह महिला अत्याधुनिक तकनीकी उपकरणों के बारे में उत्सुक थी और सदा नए उपकरणों विशेष तौर पर कम्प्यूटर सम्बन्धित उपकरणों को खरीदने के लिए सबसे आगे थी । इस महिला को इंटरनेट पर घंटों तक चैट करने का बहुत शौक था। एक बार सायबर गुनहगार जो कि रशिया से था उसने उस महिला से चैट करते समय Trojan Install कर दिया जिससे कंप्यूटर का पूरा control उसके हाथ में आ गया और उसने रशिया में अपने रुम में बैठे-बैठे ही इस महिला के कंप्यूटर से जुड़ा web camera on

किया । तत्पश्चात् उस महिला के कमरे में जो भी हुआ वह इंटरनेट पर पूरी दुनिया में live प्रसारित हुआ और यह प्रकरण 3-4 माह तक चलता रहा और महिला को मालूम भी नहीं था कि उसके साथ क्या हो रहा है । जल्द ही वह मुम्बई में किसी नौकरी के संदर्भ में मौखिक परीक्षा देने गई । उस महिला को देख उसके होनेवाले बॉस की नियत खराब हो गई क्योंकि उसने वह प्रकरण देख रखा था । साइबर गुनहगार जिसने Trojan का प्रयोग किया था उस महिला की इज्जत से खिलवाड़ करने के लिए वह कभी पकड़ा नहीं गया।

2. Dos Attack प्रकरण : दिल्ली

कुछ युवाओं के साथ मिलकर दिल्ली के एक मार्केटिंग स्नातक ने एक छोटी-सी विज्ञापन से सम्बन्धित कम्पनी खोली । कई महीने संघर्ष करके कम्पनी को एक स्तर पर लाने के बाद, इन सभी युवाओं ने अपने बिज़नस में एक बहुत बड़ी परियोजना के लिए अनुबंध करने के लिए एक जर्मनी की कम्पनी को सहमत किया । जर्मनी कम्पनी की मार्केटिंग टीम ने भारतीय टीम को प्रस्ताव भेजने के लिए (ई मेल द्वारा) एक तिथि निर्धारित की थी । निर्धारित तिथिवाले दिन आई.एस.पी.जो कि इंटरनेट सेवाएँ दे रहा था, उसके सर्वर पर Dos Attack हुआ जिस कारण उस आई.एस.पी.सर्वर से जुड़े सभी सर्वर का सम्बन्ध टूट गया और कुछ क्षणों में उस इलाके में सभी इंटरनेट की सेवाएँ पूरी तरह ठप्प हो गई जिस कारण इन युवाओं की नई स्थापित कम्पनी की डील नहीं हो पाई और एक बहुत बड़ी परियोजना हाथ से निकल गई । इसका प्रभाव युवाओं की कम्पनी पर इतना अधिक हुआ कि उनके पास कम्पनी चलाने के लिए भी पैसों का अभाव हो गया और कम्पनी देखते ही देखते बन्द हो गई ।

3. Password Cracking प्रकरण – Auckland (न्यूज़ीलैंड)

आकलैंड में युवा महिला इंटरनेट का उपयोग बहुत कम करती थी । वह इंटरनेट का प्रयोग केवल आस्ट्रेलिया में बैठे अपने कुछ मित्रों को ई-मेल

करने के लिए करती थी । एक दिन उस महिला को फोन आया बहुत गन्दी भाषा में और Sexual Comments से भरा जो कि किसी अनजान व्यक्ति ने किया था और उसका यह कहना था कि उसने इस महिला के बारे में अभद्र टिप्पणी पढ़ी थी । महिला ने गुस्से में फोन काट दिया । अगले दिन पुन: उसी व्यक्ति का फोन उस महिला को आता है और उसी प्रकार व्यक्ति अभद्र टिप्पणी करनी शुरु कर देता है जिससे महिला बहुत परेशान होकर अपने पति को अनुभव बताती है और दोनों पुलिस में रिपोर्ट दर्ज करवाते हैं। पुलिस की छानबीन से पता चलता है कि महिला के पति ने एक कर्मचारी को नौकरी से निकाला था जिस कारण कर्मचारी बहुत गुस्से में था और वह गुस्से में महिला के ई-मेल अकाउन्ट के पासवर्ड को Crack करता है और अभद्र टिप्पणी Message Board पर डाल देता है जिससे Auckland के बदतमीज युवा जो Sex Favour चाहते थे, महिला के घर के फोन पर सम्पर्क करने लगे ।

साइबर दुनिया में पासवर्ड तोड़ने से सम्बन्धित विधियाँ

1. Password का अनुमान लगाना:

यह सबसे आसान व सबसे अधिक प्रयोग में लाने वाली विधि है किन्तु बहुत लाभदायक नहीं है । इसी विधि द्वारा अपराधी सबसे पहले व्यक्तिगत जानकारी एकत्रित करता है जिसमें उसका ध्यान प्रमुख तौर पर मित्रों ,माता पिता, पति-पत्नी, बेटा -बेटी के नाम व जन्मतिथि,फोन नं. लेने पर केन्द्रित होता है । इन सूचनाओं के आधार पर विभिन्न जोड़- तोड़ लगाकर पासवर्ड का अनुमान लगाया जा सकता है ।

2. Default Password द्वारा Password जानना :

ऑनलाइन बुकिंग, शॉपिंग में रजिस्टर करते समय हमें एक पासवर्ड दिया जाता है । कई वेबसाइट्स पर पासवर्ड देने के बाद अपने आप पासवर्ड खत्म

नहीं होता जब तक उसे खुद बदला न जाए। यही नहीं कई स्थानों पर ऐसे पासवर्ड में समानताएँ भी होती हैं । ऐसी स्थिति में साइबर दुनिया के शातिर खिलाड़ियों द्वारा पासवर्ड जानना आसान हो जाता है ।

3. Dictionary पर आधारित पासवर्ड जानना:

यदि आपने पासवर्ड में अंग्रेजी वर्णमाला का ही प्रयोग किया है तो साइबर अपराधियों द्वारा शब्दों के जोड़- तोड़ करनेवाले सॉफ्टवेअर उपलब्ध होते हैं जिससे पासवर्ड जान लेते हैं । हालांकि यह इतना आसान नहीं है क्योंकि भाषा की शब्दावली बहुत बड़ी और अँग्रेजी के 26 अक्षरों से पता नहीं कितने word बनाए जा सकते हैं किन्तु फिर भी यह नामुमकिन नहीं है ।

4. Brute force, password हमला :

यह विधि अक्सर सायबर अपराधियों द्वारा अपनाई जाती है जब अन्य सभी विधियाँ फेल हो जाएं तो इस विधि द्वारा अपराधी Automatic Tool का प्रयोग करता है। keyboard पर बनी सभी keys का मिलाप करके जैसे ही सही पासवर्ड मिलता है कम्प्यूटर की स्क्रीन पर दिखने लगता है। यह विधि बहुत कठिन व समय लेने वाली है परंतु इससे पासवर्ड ढूँढना असंभव नहीं है।

साइबर गुनाह के परिप्रेक्ष्य में भारत की स्थिति :

भारत में पुलिस में रिपोर्ट किए गए साइबर गुनाह मुख्य तौर पर DAS Attack, Website Hack करना,SPAM मेल भेजना, किसी रिमोट द्वारा कम्प्यूटर पर वायरस डालना,अश्लील फोटो या भाषा को इन्टरनेट पर डालना, फिशिंग, Cyber stalking, Cyber Squatting, DOS Attack इत्यादि पर आधारित हैं। इन सभी हमलों से सम्बन्धित रिपोर्ट से कुछ चौंकाने वाले तथ्य मिलते हैं जो निम्न हैं –

1. 69% सूचना चुराने से सम्बन्धित अपराध किसी निकट सम्बन्धी, किसी करीबी मित्र, संस्था में कार्यरत किसी सह कर्मचारी द्वारा किए गए होते हैं ।

2. देश में खोज या विश्लेषण में जुटे संस्थानों का डाटा बहुत ही महत्वपूर्ण होता है और इसे गुप्त रखना अत्यावश्यक है । इस दृष्टि से कार्य हो रहा है किन्तु अभी बहुत कुछ करना बाकी है ।

3. Symantec द्वारा किए एक Survey के अनुसार हमारे देश में वैद्य मेल की तुलना में SPAM या Junk मेल का अनुपात सबसे अधिक है ।

4. भारत के घरों में प्रयोग होने वाली पीसी के उपभोक्ताओं की संख्या 37.7% है जो कि यदि अंकों में आंकी जाए तो बहुत अधिक है । इससे गौर करने लायक बात यह है कि इसमें अधिकांश उपभोक्ता या तो तकनीकी तौर पर अनपढ़ हैं या उनके ज्ञान का स्तर बहुत कम है ।

5. भारत में 86% सायबर गुनाह बॉट के द्वारा हो रहे हैं । ऐसे हमलों का केन्द्र- बिन्दु दिल्ली व मुम्बई है ।

6. भारत में हो रहे साइबर गुनाह में बहुत बड़ा सहभाग युवा पीढ़ी का है ।

7. हमारे देश में साइबर गुनाह का मुख्य स्रोत साइबर Cafe बनते जा रहे हैं । यहाँ तक कि आतंकवादी कैफे में मिल रहे एकान्त वातावरण का भरपूर लाभ उठा रहे हैं। यही नहीं साइबर कैफे गोपनियता की सुविधा प्रदान करने के कारण अश्लील वैबसाइट का प्रयोग करने के लिए युवा पीढ़ी साइबर कैफे न केवल जा रही है बल्कि उन्हें इस बात का नशा हो गया है ।

8. इंटरनेट के विकास व ऑनलाइन कारोबार में बढौत्तरी के कारण इंटरनेट के उपभोक्ताओं की संख्या बहुत तेजी से बढ़ी है जिसके कारण Phishing गुनाह से सम्बन्धित वेबसाइट होसट करने वाले प्रमुख देशों में हमारे देश का नाम भी आने लगा है और ऐसी वेबसाइट का मूल उद्देश्य गुप्त सूचनाओं जिनमें पासवर्ड व क्रेडिट कार्ड से सम्बन्धित सूचनाओं की चोरी करना प्रमुख है ।

साइबर गुनाह पर लगाम लगाने हेतु सरकार द्वारा उठाए गए प्रमुख कदम :

1. IT ACT 2000 को वर्ष 2000 में पास कर कानून का आकार देना जिसमें साइबर गुनाह से सम्बन्धित कानूनी प्रावधान किया गया है । यही नहीं वर्ष 2006, 2008, 2012 में कानून में आवश्यकता अनुसार संशोधन किए गये हैं । इस कानून में साइबर गुनाह से सम्बन्धित विशेष प्रावधान किए गए हैं और बड़े गुनाह के लिए सजा निर्धारित की गई है ।

2. भारतीय पुलिस बल को विभिन्न साइबर कैफे पर नजर रखने के लिए Electronic Eye की सहायता लेने के लिए अधिकृत किया गया है। पुलिस विभाग के सभी शहरों के स्तर पर स्थित कार्यालयों में साइबर कक्ष का गठन किया गया है ।

3. हर राज्य में कंप्यूटर Emergency Response teams का गठन किया गया है जिनका मुख्य उत्तरदायित्व आपसी समन्वय बनाकर सायबर गुनाह की शिकायत दर्ज होते ही तत्काल कार्रवाई करना है। यह सभी संस्थाएं वर्तमान व भविष्य में आने वाली साइबर गुनाह से सम्बन्धित चुनौतियों को खोजते हैं और रिपोर्ट बनाकर सरकार के सामने प्रस्तुत करते हैं। दिशा निदेश पाने के लिए और निदेश मिलने

पर उचित कार्रवाई करते हैं ।

साइबर गुनाह पर लगाम लगाने हेतु सरकार तेजी से अग्रसर है। किन्तु जाने माने विशेषज्ञों की राय कुछ अलग है । श्री .प्रतीक भार्गव, सायबर विशेषज्ञ के अनुसार राष्ट्रीय सुरक्षा के मुद्दे पर साइबर गुनाह से हो रही क्षति को रोकने हेतु बहुत काम करना अभी बाकी है । श्री.पवन दुगल जाने माने साइबर विशेषज्ञ के अनुसार साइबर गुनाह केवल हमारे देश में ही नहीं बल्कि समूचे विश्व में अपनी जगह बना चुके हैं और चाहे भारत के प्रमुख शहरों में साइबर गुनाह से सम्बन्धित कक्ष बना दिए हैं। फिर भी अधिकांश साइबर गुनाह से सम्बन्धित घटनायें पुलिस तक पहुँच ही नहीं पाती क्योंकि अधिकांश जनता को इस बारे में जागरूकता ही नहीं है । ऐसी स्थिति में कम्प्यूटर व इन्टरनेट प्रयोग करनेवाले प्रत्येक नागरिक का परम कर्तव्य बनता है कि वह साइबर गुनाह से सम्बन्धित तकनीकी जानकारी प्राप्त करें । यही नहीं कानूनी प्रावधानों की जानकारी भी प्राप्त करना आवश्यक है ।

(क) हर माता-पिता अपने बच्चों को दिए गए कम्प्यूटर व अपने बच्चों की दिनचर्या पर नजर रखें। कम्प्यूटर व मोबाईल पर देखी गई वेबसाइट के बारे में जानकारी रखें कि वह कोई वेबसाइट बार – बार क्यों देख रहा है । यदि खुद नहीं कर सकते तो किसी विश्वासपात्र की सहायता लें । मेरा मानना है कि हर माता पिता का अपने बच्चों के प्रति यह मूल उत्तरदायित्व है ।

(ख) Print Media जिसमें समाचार पत्र व सामयिक पत्रिकाएँ आती हैं ये, सभी प्रमुख भूमिका अदा कर सकती हैं । युवाओं को साइबर गुनाह के प्रति जागरूक करने के लिए वह उनमें चेतना पैदा कर सकती है।

(ग) कम्प्यूटर का विषय सी.बी.एस.ई, आई.सी.एस.ई. बोर्ड ने छठी कक्षा से पढ़ाना आरम्भ कर दिया है और बच्चा कक्षा सात या आठ तक इंटरनेट प्रयोग करने हेतु सक्षम हो जाता है । नौवीं , दसवीं कक्षा में

सी, जावा पढ़ने के साथ साइबर सुरक्षा से सम्बन्धित प्रकरण अवश्य होना चाहिए ।

भारत अपनी युवा शक्ति के लिए विश्व भर में विशेष स्थान रखता है। चाहे हम NASAमें वैज्ञानिकों की बात करें या विश्वविख्यात सूचना प्रौद्योगिकी व Electronic कम्पनियों का नाम लें जिनमें Microsoft,Cisco, Google, Intel, redhat प्रमुख हैं, की बात करें इन सभी कम्पनियों में भारतीयों का अग्रिम योगदान है। आवश्यकता है युवा शक्ति को विशेषकर ऐसे वैज्ञानिकों को अपने देश की ओर आकर्षित करने की और उन्हें सरकार की प्रमुख Task Force के तौर पर अग्रिम योगदान हेतु प्रेरित करने की । इससे प्रमुख भूमिका सरकार को निभाने की आवश्यकता है । किसी भी चुनौतिपूर्ण कार्य की शुरुआत सदा कठिन होती है किन्तु एक बार शुरुआत होने पर रफ्तार अपने आप बन जाती है । सरकार के अधीन स्वयंसेवी सूचना प्रौद्योगिकी संस्थाएं इसमें अहम भूमिका निभा सकती हैं ।

गुनाहों के प्रति विशेष संगणकीय उपाय

प्रत्येक भारतीय का यह कर्तव्य है कि इंटरनेट का प्रयोग उससे हो रहे लाभ को ध्यान में रखकर व एक ज़िम्मेदार नागरिक के तौर पर करें । सभी साइबर कानून (IT act 2008) के रक्षक बनकर व कानून में बताए नियमों व सीमाओं का पालन करें ।

एक जिम्मेदार इंटरनेट उपभोक्ता के तौर पर अपने कम्प्यूटर की व उस पर पड़े डाटा के रखरखाव की पूर्व ज़िम्मेदारी खुद उठाकर, पासवर्ड का विशेष ध्यान रखें, उन्हें समय – समय पर बदलें, ई मेल को ध्यानपूर्वक प्रयोग करें, अटैचमैंट को ध्यान देकर डाऊनलोड करें । यह बिलकुल उसी प्रकार है जैसे हम अपने निजी जीवन में अपनी व अपने परिवार की कमाई को ध्यान में

रखते हुए पैसे का रखरखाव करते हैं । हमें पासवर्ड, ई-मेल का विशेष ध्यान रखना चाहिए।

आजकल के युग में जहां प्रत्येक व्यक्ति दूसरे से आगे निकलने की होड़ में है। हमारा दायित्व बनता है कि निजी कम्प्यूटर व डाटा के रखरखाव ही नहीं बल्कि अपने सहयोगियों, मित्रों, पड़ोसियों और समाज के प्रति उत्तरदायित्व को समझते हुए उनके कम्प्यूटर और डाटा का ध्यान भी रखें और उन्हें शिक्षित करें जिससे भविष्य में यह भूमिका वे खुद अदा कर सकें ।

खुद को जागरूक करना

हम तकनीकी व प्रौद्योगिकी की दौड़ में तभी आगे बढ़ सकते हैं यदि हम स्वयं के प्रति जागरूक हों। ऐसी स्थिति में हमारे लिए जानना अनिवार्य हो जाता है कि हम क्या करें और क्या न करें । उक्त तथ्य पर विवरण कुछ इस प्रकार है। साइबर गुनाह तथा सुरक्षा के विविध संगणकीय उपायः–

क्या करें

अपने कम्प्यूटर पर पड़े डाटा व सूचनाओं की ज़िम्मेदारी खुद उठाएँ| सुरक्षा के सन्दर्भ में धमकियों व सूचनाओं के प्रति सदा जागरूक रहें एवं अति आधुनिक तकनीकी ज्ञान को अर्जित करने हेतु सदा तत्पर रहें।

क्या न करें

कभी भी सायबर गुनाह को छोटा न समझें व इसे दर किनार न करें, क्योंकि किसी भी गलत कार्य की शुरुआत छोटे स्तर पर होती है । इस विषय के सन्दर्भ में पहले डाटा फिर पासवर्ड और तत्पश्चात् अन्य प्रकार की बड़ी हानि भी हो सकती है। कभी भी ऐसा न सोचे कि सायबर गुनाह केवल लापरवाह व्यक्तियों के साथ ही होता है।

इन्टरनेट पर बने अपने प्रत्येक एकाउन्ट का सही संचालन

इन्टरनेट पर बनाए प्रत्येक अकाउन्ट का संचालन व रखरखाव स्वयं करें । यदि ऐसे कार्य को करने हेतु सक्षम नहीं है तो किसी विशेषज्ञ से या संस्थान में प्रशिक्षण प्राप्त कर योग्यता हासिल करें । क्योंकि ऐसा करने से सबसे बड़ी उपलब्धि यह रहेगी कि आपके मन से इन्टरनेट पर काम करने का भय चला जाएगा व अभ्यास करके आप खुद ही सक्षम हो जाएंगे। अकाउन्ट के सन्दर्भ में भी कुछ बिन्दु ध्यान देने योग्य हैं जो निम्न हैं –

क्या करें

पासवर्ड में सदा छोटे बड़े , अक्षर, अंकों व विशेष Character का मिश्रण करें ।

सदा पासवर्ड ऐसा रखें जिसका अनुमान लगाना बहुत कठिन हो लेकिन आपके खुद के लिए याद रखना आसान हो जिससे कि आपको अपने किसी डायरी /पृष्ठ / किसी अन्य स्थान पर उसे लिखकर रखना न पड़े ।

पासवर्ड सदा वह हो जिसे आप keyboard पर देखे बिना डाल सकें जिससे आपके पास खड़ा कोई भी व्यक्ति उसके बारे में किसी प्रकार का अनुमान न लगा सके ।

पहली बार किसी वेबसाइट पर पंजीकरण करने पर निकलने वाले Default पासवर्ड को तुरन्त बदलें। पासवर्ड को समय – समय पर बदलते रहें।

कम्प्यूटर व इन्टरनेट पर कार्य करते समय कभी भी जरा सा भी शक होने पर तुरन्त पासवर्ड बदलें।

कम्प्यूटर पर कार्य समाप्त कर उसे लॉग ऑफ / शट डाउन अवश्य करें।

ई – मेल अकाउन्ट खोलने पर कार्य करने के बाद खुद sign out करें और

कभी भी स्क्रीन के दाँये कोने पर बने क्लोज बटन का प्रयोग न करें । ई-मेल अकाउन्ट को कभी खुला न छोड़ें ।

क्या न करें

कभी भी स्वयं के नाम पर अथवा अपनी धर्मपत्नी,माता-पिता , बेटा -बेटी के नाम पर पासवर्ड न रखें।

पासवर्ड में कभी ऐसे अंकों का प्रयोग न करें जिसके बारे में अनुमान लगाना आसान हो जैसे जन्मतिथि, लाईसेंस क्र. फोन नं. आदि।

कभी भी केवल अंकों या केवल अंग्रेजी अक्षरों या संख्या के नाम या अंकों के क्रम वाला पासवर्ड न बनाएं। यानी एक क्रम में आने वाले अंकों का प्रयोग न करें।

कभी भी कीबोर्ड पर एक साथ लगी ' की 'को दबानेवाले शब्दों से बने पासवर्ड का चयन न करें जैसे Qwerty शब्दावली में लिखित शब्दों का चयन कर पासवर्ड न रखें|

एक बार प्रयोग किए गए पासवर्ड का पुन: प्रयोग न करें।

एक ही पासवर्ड का प्रयोग सभी एकाउन्ट के लिए न करें।

कभी भी पासवर्ड को किसी मित्र या निकट सम्बन्धी से भी न बताएं।

यदि किसी पासवर्ड को बताना अनिवार्य है तो उसे ई मेल या SMS या फोन से न भेजें।

जहां तक संभव हो सके Remember my password option का प्रयोग न करें। क्योंकि यदि आपके किसी मित्र ने मेल एकाउन्ट खोल लिया तो वह तुरन्त पासवर्ड बदल कर हानि पहुंचा सकता है।

कभी भी अपने बैंक अकाउंट,डेबिट कार्ड , क्रेडिट कार्ड से सम्बन्धित सूचना ई मेल पर न रखें।

मेल एकाउन्ट में किसी अज्ञात व्यक्ति से आई मेल को न खोलें। यही नहीं यदि गलती से खुल भी जाए तो मेल में लिखित लिंक को तो कतई न दबाएँ क्योंकि ऐसा करने पर दूसरा अकाउन्ट खुल सकता है और आपके अकाउन्ट की पूरी सूचना उस अज्ञात व्यक्ति तक पहुँच सकती है और उस व्यक्ति की गंदी मंशा होने पर आपकी हानि हो सकती है।

यदि आपका कम्प्यूटर नेटवर्क पर है और कुछ भी शेअर किया है तो गुप्त सूचनाएँ और डाटा कम्प्यूटर से हटा लें।

अपनी व्यक्तिगत सूचना आदि इन्टरनेट पर न रखें । यह बिन्दु महिलाओं के लिए विशेष तौर पर ध्यान देने योग्य हैं।

कभी भी अपनी व्यक्तिगत सूचना सोशल नेटवर्किंग साइट पर न दें क्योंकि ऐसे एकाउन्ट को बहुत सारे अनजान व्यक्ति भी देखते हैं। यदि बहुत अनिवार्य है तो कम से कम सूचना डालें जितनी पंजीकरण हेतु अनिवार्य हो।

साइबर फॉरेंसिक लैब में डीएनए की सुविधा

महिलाओं के खिलाफ बढ़ते अपराध से निपटने के लिए सभी राज्यों की साइबर फॉरेंसिक प्रयोगशालाओं में डीएनए जांच की सुविधाएं उपलब्ध कराई गई है। उत्तर प्रदेश, तमिलनाडु, पश्चिम बंगाल, मध्य प्रदेश, हिमाचल प्रदेश, जम्मू कश्मीर, महाराष्ट्र, पंजाब, राजस्थान, मिजोरम, मणिपुर, त्रिपुरा और दिल्ली की फॉरेंसिक विज्ञान प्रयोगशालाओं में 131.09 करोड़ रुपये की लागत से डीएनए जांच सुविधाएं मुहैया कराई गई है।

गृह मंत्रालय के एक अधिकारी के अनुसार महिलाओं एवं बच्चों के खिलाफ साइबर अपराध निवारण परियोजना के तौर पर इन राज्यों में 223.19 करोड़

रुपये की साइबर फॉरेंसिक प्रयोगशालाएं और साइबर फॉरेंसिक प्रशिक्षण सुविधाएं मुहैया कराई जा रही हैं ।

पांच राज्यों-अरुणाचल प्रदेश, हिमाचल प्रदेश, मध्य प्रदेश, तेलंगाना और उत्तराखंड में पहले ही साइबर फॉरेंसिक प्रशिक्षण प्रयोगशालाएं हैं। इस उद्देश्य के लिए 410 सरकारी अभियोजकों और न्यायिक अधिकारियों समेत कुल 3,664 कर्मियों को प्रशिक्षण दिया गया है। महिलाओं की सुरक्षा सुधारने के लिए तैयार की गई परियोजनाओं के वास्ते केंद्र सरकार द्वारा बनाए गए निर्भया फंड के तहत यह परियोजना लागू की जा रही है। राष्ट्रीय अपराध रिकॉर्ड ब्यूरो के अनुसार, भारत में वर्ष 2016 में साइबर अपराध के 12,187 मामले दर्ज किए गए जबकि वर्ष 2015 में 11,331 मामले दर्ज किए गए थे ।

फॉरेंसिक विज्ञान, अपराधी के अपराध या बेगुनाही साबित कर सकता है । आपराधिक कानून में, यह शारीरिक कार्यों की पहचान, विश्लेषण और मूल्यांकन के माध्यम से नागरिक कार्यों में व्यापक मुद्दों को हल करने में मदद कर सकता है। अन्य सबूत एक सटीक फॉरेंसिक विज्ञान की परिभाषा विज्ञान की पारंपरिक अवधारणा से परे हैं और इसमें लेखांकन, मनोवैज्ञानिक परीक्षण और आंकड़ों के विवरण और अन्य साक्ष्य शामिल हो सकते हैं। फोरेंसिक वैज्ञानिक क्षेत्र में डीएनए विश्लेषण, फिंगरप्रिंटिंग, ऑटोप्सी, पैथोलॉजी और विष विज्ञान शामिल हो सकते हैं ।

फोरेंसिक विज्ञान में कैरियर के लिए कम से कम कॉलेज की डिग्री की आवश्यकता होती है, देश-विदेश में बढ़ रही आतंकी घटनाओं ने फॉरेंसिक विशेषज्ञों की डिमांड बढ़ा दी है। आपराधिक वारदातों के सूत्रधारों की धर-पकड़ के लिए प्रशिक्षित सुरक्षा बलों की जरूरत आज समाज और समय की डिमांड है।

इस साइंस को जानकार अपराध से जुड़े लोगों को पकड़वाने में काफी मदद

होती है। अपराधियों या आतंकवादी का स्कैच तैयार कराने में फॉरेंसिक साइंस के एक्सपर्ट काफी सहायक होते हैं। अदालत भी इस विज्ञान की मदद लेकर जांच को आगे बढ़ाती है। आतंकवादी गुत्थियां हों या रहस्यमय मौत, इसे सुलझाने में फॉरेंसिक साइंस की अहम भूमिका होती है। फॉरेंसिक साइंटिस्ट से प्राप्त इनपुट को लेकर ही इंवेस्टिगेटिंग ऑफिसर अदालत के समक्ष हाजिर होता है। जरूरत पडने पर फॉरेंसिक एक्सपर्ट घटना स्थल का निरीक्षण करता है। इस फील्ड के लोग ब्लड सहित शरीर के अन्य तरल पदार्थो की जांच कर अपराधियों तक पहुंचने में मददगार साबित होते हैं।

देश में साइबर अपराधों के बढ़ने की सबसे बड़ी वजह साइबर कानून का नहीं होना है। साइबर सुरक्षा को मजबूत करने के लिए लोगों को साइबर अपराधों के प्रति जागरूक करना भी जरूरी है। यह कहना है देश के मशहूर वकील व साइबर एक्सपर्ट डॉ. पवन दुग्गल का। डॉ. दुग्गल ने बताया कि इस समय सबसे बड़ा साइबर अपराध, डाटा और वित्तीय चोरी का है। देश में इस साल करीब 10 मिलियन डॉलर की वित्तीय चोरी की आशंका है और विश्व स्तर पर इसका आंकड़ा दो खरब डॉलर से ज्यादा का है। इसका मुख्य कारण देश में अपना साइबर अपराध कानून का न होना है। अभी साइबर अपराधों को आईटी एक्ट में कवर किया जाता है। यह जमानती अपराध हैं और तीन साल की अधिकतम सजा का प्रावधान है। ऐसे में सख्त और मजबूत साइबर कानून बनाए जाने की जरूरत है। उन्होंने बताया कि कानून बनाने में कोई दिक्कत नहीं। राष्ट्रीय अपराध ब्यूरो के पास साइबर अपराधों का काफी डाटा है। उसे एकत्र करने की जरूरत है।

साइबर अपराध व सुरक्षा से जुड़े मुद्दों पर चर्चा के दौरान यह बात सामने आई है कि लोगों में जागरुकता की कमी है मजबूत कानून के अभाव में साइबर अपराधों का ग्राफ लगातार बढ़ रहा है। साइबर सुरक्षा प्रदान करने के लिए क्या कदम उठाए जाएं, इस पर भी चर्चा की गई। इस दौरान लोगों ने कहा कि विदेशों में बैठे हैकर हमारे साइबर क्षेत्र में लगातार घुसपैठ कर रहे हैं और

इसमें सर्च इंजन की भी बड़ी भूमिका है। इसके साथ ही साइबर सुरक्षा को मजबूत करने के लिए जरूरी है कि हम अपने देश में ही ज्यादातर सॉफ्टवेयर का निर्माण करें।

भारत सरकार के संचार व सूचना प्रौद्योगिकी मंत्रालय के वरिष्ठ निदेशक राकेश महेश्वरी ने कहा कि इस समय साइबर जगत का नियंत्रण हमारे बच्चों के हाथ में है। शिक्षक व अभिभावक भी बच्चों से कम जानते हैं क्योंकि उन्हें जानकारी नहीं है। बच्चों पर अंकुश लगाना उनके नियंत्रण में नहीं है। हम इंटरनेट पर जो सामग्री है, उसे रोकने के उपाय कर सकते हैं। इससे संबंधित शिकायतों के लिए पोर्टल भी बनाया गया है।

इंटरनेट की दुनिया में संतुलन ज़रुरी

इंटरनेट ने दुनिया को एक गांव बना दिया है । घर बैठे आप दुनिया के किसी भी शहर या गांव की तस्वीर और उसके बारे में जानकारियां अपने कंप्यूटर पर ले सकते हैं। इसने जहां जन-साधारण की जिंदगी आसान की है, वहीं इससे कुछ की जिंदगी मुश्किल में भी आ गई है। इस माध्यम का अब दुरुपयोग होने लगा है।

सुरक्षा सिस्टम को भेदने वाले हैकर्स और वायरस ही इसके दुश्मन नहीं हैं, अब मोर्फिंग (धड़ किसी का और सिर किसी का लगाकर फोटो बनाना), पोर्नोग्राफी (अश्लील फिल्में), पेडोफाइल (बाल यौन शोषण), सेक्स रैकेट से लेकर लिंग निर्धारण के टेस्ट भी इसके जरिये होने लगे हैं। कई बार अपराध ऐसे होते हैं कि उनका स्रोत विदेशी जमीन होती है। वहां न तो पुलिस पहुंच पाती है और न ही सरकार कुछ कर सकती है।

देश में इस मामले में जागरूकता बढ़ी है। सरकार ने वर्ष 2000 में आईटी एक्ट बनाया और वर्ष 2008 में इसे संशोधित भी किया लेकिन इसके बावजूद साइबर क्राइम को रोकना मुश्किल हो रहा है। दुनिया का सबसे मजूबत

कंप्यूटर नेटवर्क भी हैकरों से सुरक्षित नहीं है। पिछले दिनों चीनी हैकरों ने राष्ट्रीय सुरक्षा सलाहकार के दफ्तर के कंप्यूटरों को हैक करने की कोशिश की जिसे समय रहते नाकाम कर दिया गया। लेकिन सेना अपने कंप्यूटरों को चीनी हैकिंग से नहीं बचा पाई। इस तरह से देखें तो लगभग यूरोप और अमेरिका तक हैकरों से परेशान हैं।

देश में साइबर क्राइम से निपटने के लिए आईटी एक्ट बनाया गया है, जिसमें वेबसाइट ब्लॉक करने तक के प्रावधान हैं। लेकिन यह एक्ट देश के अंदर ही ठीक से लागू नहीं हो पा रहा है। कंप्यूटर की दुनिया ऐसी है जिसमें अनेक प्रॉक्सी सर्वर होते हैं। किस सर्वर से अपराध किया गया और यह सर्वर कहां स्थित है, यह पता लगना काफी मुश्किल है। यदि पता लग भी जाए तो उसे ब्लॉक करना उससे भी कठिन होता है क्योंकि जिस देश में यह सर्वर होगा, वहां भारत के कानून लागू नहीं होंगे। जन्म से पूर्व लिंग निर्धारण के लिए किट बेचने वाली एक वेबसाइट को ब्लॉक करने से सरकार ने मना कर दिया है क्योंकि यह साइट गूगल और याहू पर भी उपलब्ध है। वेबसाइट ब्लॉक करने के बारे में सरकार का मत है कि किसी भी साइट को ब्लॉक तभी किया जा सकता है जब उसमें प्रदर्शित सामग्री या सूचनाएं राष्ट्रीय सुरक्षा के लिए खतरा हों। विधि मंत्रालय के एक वरिष्ठ अधिकारी ने कहा कि साइट ब्लॉक करना एक आपात शक्ति है जिसके इस्तेमाल को राष्ट्रीय सुरक्षा से जुड़े मामलों में ही जायज ठहराया जा सकता है।

सरकार पिछले दरवाजे से और मनमाने तरीके से वेबसाइटों को ब्लॉक करने की पक्षधर नहीं है। इस बारे में नैतिक थानेदारी को हतोत्साहित करना चाहिए। संशोधित आईटी एक्ट जो गत वर्ष अक्तूबर में प्रभाव में आया है, में पोर्नोग्राफी से निपटने के लिए पर्याप्त प्रावधान हैं। हालांकि यह इंटरनेट की सतत समस्या है।

वहीं बाल यौन शोषण इससे भी बुरा है। आईटी एक्ट की धारा-79 सर्विस

प्रोवाइडर की जिम्मेदारी तय करती है। यदि पुलिस उससे एक बार कहती है कि वह अपनी साइट से आपत्तिजनक सामग्री हटा ले और वह उसे नहीं हटाता है तो उसे तीन साल तक की सजा हो सकती है।

आईटी एक्ट में आईपीसी को मद्देनजर रखते हुए सुधार किया गया है। दोनों कानूनों के प्रावधानों को एक साथ लागू कर अश्लीलता पर आसानी से काबू पाया जा सकता है। संभवत: आईटी एक्ट में संशोधन के बाद धारा 60 कमजोर हो गई है, कानून का पालन करवाने वाली एजेंसियों के सामने यह समस्या सबसे गंभीर है कि इंटरनेट पर अश्लीलता किसे कहा जाए?

यदि किसी यूजर ने वेबसाइट पर अश्लील सामग्री पोस्ट कर दी है तो इस मामले में सर्विस प्रोवाइडर को सीधे जिम्मेदार नहीं ठहराया जा सकता। उस पर कार्रवाई करने से पहले उसे अपनी साइट को साफ करने को मौका देना पड़ेगा। अमेरिका और चीन के मामलों में देखा गया है कि वेबसाइट को ब्लॉक करने से कोई मकसद हल नहीं हुआ है।

क्या है साइबर क्राइम :-

ऐसा गैरकानूनी काम जिसमें कंप्यूटर को हथियार की तरह इस्तेमाल किया गया हो और इस काम का निशाना भी अन्य कंप्यूटर होते हैं।

साइबर क्राइम के नए-नए तरीके

साइबर स्टाकिंग - इसका मतलब इंटरनेट पर किसी व्यक्ति का पीछा करना और उसके बुलेटिन बोर्ड पर संदेश भेजना और उसके चैट रुम में घुस जाना।

ई मेल बॉम्बिंग - किसी व्यक्ति की ईमेल पर इतनी ज्यादा मेल भेजना कि उसका अकाउंट ही ठप हो जाए।

डाटा डिडलिंग - इस हमले में कंप्यूटर के कच्चे डाटा को प्रोसेस होने से पहले

ही बदल दिया जाता है। जैसे ही प्रोसेस पूर्ण होता है डाटा फिर मूल रूप में आ जाता है।

सलामी अटैक - इस मामले में गुपचुप तरीके से आर्थिक अपराध को अंजाम दिया जाता है। ये अपराध बैंकों में ज्यादा होता है जैसे कोई क्लर्क यदि ऐसा प्रोग्राम बैंक सर्वर में डाल दे जिससे हर खाते से इतना कम धन कटता है कि वह नजरअंदाज होता रहता है।

लॉजिक बम - यह स्वतंत्र प्रोग्राम होता है। इसमें प्रोग्राम इस तरह से बनाया जाता है कि यह तभी एक्टिवेट हो जब कोई विशेष तारीख या घटना आती है। बाकी समय ये प्रोग्राम सुप्त पड़े रहते हैं।

ट्रोजन हॉर्स - यह एक अनाधिकृत प्रोग्राम है जो अंदर से ऐसे काम करता है जैसे यह अधिकृत प्रोग्राम हो।

साइबर क्राइम से निपटना काफी दिक्कतों भरा काम है। हालांकि सरकार समय के साथ-साथ कानूनों में सुधार भी कर रही है। नए संशोधन में मोबाइल तथा व्यक्तिगत डिजिटल असिस्टेंस को कम्युनिकेशन का साधन माना गया है, जिससे मोबाइल फोन के जरिये होने वाले अपराधों को भी साइबर क्राइम कहा गया है। इन अपराधों का रजिस्ट्रेशन करने के लिए विशेष प्रक्रिया विकसित करने की जरूरत है। जहां तक दूसरे देशों में रखे सर्वर से होने वाले अपराधों का मामला है तो इसमें इन देशों के साथ समझौता करने से ही काम चल सकता है।

भारत में साइबर अपराधों से निपटने की मौजूदा स्थिति क्या है?

तकनीक के बदलते दौर में भारत ने भी इस दिशा में काफी कदम उठाए हैं लेकिन वे उतने बेहतर नहीं हैं। साइबर कानून में बुनियादी खामियां है। साइबर क्राइम में जमानत दिए जाने का प्रावधान है। इससे उल्लंघन करने वालों में किसी तरह का डर नहीं बैठता है। लोग यह समझते हैं कि नियमों

को तोड़ने के बाद उन्हें जमानत तो मिल ही जाएगी। जहां तक साइबर मामले में सजा पाने का सवाल है तो इसके तहत 1995 से लेकर अभी तक केवल सात लोगों को ही सजा हुई है।

साइबर अपराधों से निपटने में कौन सा कानून कितना प्रभावी है?

देश में साइबर अपराधों से निपटने के लिए आईटी एक्ट 2000 है। इंटरनेट के बढ़ते इस्तेमाल को देखते हुए इसमें 2008 में संशोधन किया गया है। हालांकि, पिछले कुछ सालों में काफी बदलाव देखने को मिला है। आजकल मोबाइल जिंदगी का अहम हिस्सा बन चुका है। इसके बावजूद भी इसके इस्तेमाल को लेकर मौजूदा आईटी एक्ट में इससे जुड़ा कोई प्रावधान नहीं है।

सोशल मीडिया साइबर कानून के दायरे में आता है?

सोशल मीडिया को साइबर कानून के दायरे में बांधने को लेकर स्थिति अभी भी पूरी तरह साफ नहीं है। इस दिशा में अभी कुछ भी ठोस काम नहीं किया जा रहा है। इसके जरिए मोबाइल क्राइम भी कवर नहीं होता है। मतलब आप अगर बड़े लोगों के खिलाफ कुछ लिखते हैं तो कार्रवाई हो सकती है अगर आम आदमी के खिलाफ लिखते हैं तो कोई कार्रवाई होगी या नहीं कुछ कह नहीं सकते।

आईटी एक्ट 2000 का 66ए प्रावधान क्या है?

इसके तहत प्रावधान काफी खतरनाक हैं। इसके मुताबिक, अगर किसी व्यक्ति को किसी भाषा या इलेक्ट्रॉनिक संदेश के जरिए ठेस पहुंचती है तो यह नियम का उल्लंघन माना जाएगा। सरकार ने इस पर अंकुश लगा रखा है। इससे संबंधित एक मामला फिलहाल सुप्रीम कोर्ट में चल रहा है।

अंतरराष्ट्रीय स्तर पर साइबर क्राइम से निपटने में क्या-क्या चुनौतियां है?

दिल्ली में आयोजित अंतरराष्ट्रीय स्तर के साइबर क्राइम से संबंधित एक सम्मेलन में मौजूदा ट्रेंड, चुनौती और उसकी पहचान करने के लिए चर्चा की गई। इसके अलावा मौजूदा विकल्पों को राष्ट्रीय और वैश्विक स्तर पर तलाशने की दिशा में काम किया जा रहा है ताकि आम उपभोक्ता इससे लाभान्वित हो सकें।

वैश्विक स्तर पर साइबर कानून में बदलाव?

अंतरराष्ट्रीय स्तर पर साइबर कानून में हो रहे बदलावों का न्याय क्षेत्र पर पड़ने वाले प्रभाव का मामला चर्चा में है। यह सभी संबंधित पक्षों पर प्रभाव डालेगा जिनका संबंध डिजिटल एवं मोबाइल इकोसिस्टम से है। ऐसे समय में जरूरत इस बात की है कि अंतरराष्ट्रीय स्तर पर एक ऐसा नेटवर्क बनाया जाए जिसमें साइबर क्राइम और साइबर लीगल लॉ से जुड़े प्रोफेशनल शामिल हों। भारत तेजी से डिजिटलाइजेशन की तरफ बढ़ रहा है। वर्तमान में भारत में 45 करोड़ इंटरनेट उपभोक्ता हैं जो आने वाले तीन सालों में करीब 82.9 करोड़ हो जाएंगे। सवा अरब आबादी वाले देश में इसे लेकर ढेरों चुनौतियां तथा खतरे हैं। एक रिपोर्ट के अनुसार करीब 48 फीसदी भारतीय ऑनलाइन उपभोक्ता कभी न कभी ऑनलाइन जालसाजी या धोखाधड़ी के शिकार हुए हैं। यह समस्या अब बड़े शहरों तक ही सीमित नहीं रही। छोटे शहरों में भी साइबर क्राइम की घटनाएं तेजी से बढ़ रही हैं। गौरतलब है कि साइबर फ्रॉड और साइबर क्राइम को रोकने के लिए गृह मंत्रालय की तरफ से गठित साइबर एंड इन्फार्मेशन सिक्योरिटी ब्रांच अब साइबर क्राइम को रोकने के लिए कड़े कदम उठा रही है।

दिल्ली में पिछले साल आयोजित एक वैश्विक सम्मेलन में 124 देशों के प्रतिनिधि शामिल हुए जिसमें साइबर अपराधों पर कैसे अंकुश लगे इसी पर

चर्चा हुई। भारत में साइबर अपराध की घटनाएं तेजी से बढ़ रही हैं। सरकारी आंकड़ों के मुताबिक वर्ष 2014 के मुकाबले वर्ष 2015 में इन घटनाओं में सौ फीसदी से भी ज्यादा वृद्धि दर्ज की गई। वहीं वर्ष 2013 में ऐसे 71,780 मामले सामने आए जो वर्ष 2014 में बढ़कर 1.49 लाख हो गये। चिंता की बात यह है कि वर्ष 2015 में ऐसे अपराधों की संख्या दोगुनी से भी ज्यादा बढ़कर तीन लाख हो गई। आईआईटी की रिपोर्ट यह बताती है कि हाल ही में कई रहस्यमय गुटों की ओर से रक्षा, दूरसंचार और शोध संस्थानों की वेबसाइट हैक करने के मामले सामने आए हैं। इसी के साथ वित्तीय क्षेत्रों में भी फर्जी पैन कार्ड, नौकरी के लिए गलत दस्तावेज पेश करना, गलत इनकम सर्टिफिकेट, आइडेंडिटी चोरी के मामले भी 75 फीसदी बढ़े हैं। ऐसे ही कुछ अपराध जैसे ऑनलाइन ठगी, साइबर फ्राड तथा सोशल साइट्स के ढेरों अपराध सामने आए हैं। लोगों की मेहनत की कमाई जो बैंको में जमा रहती है वह भी साइबर फ्रॉड का शिकार हो जाती है।

साइबर फॉरेंसिक लैब की क्या विशेषता है?

फॉरेंसिक शब्द लैटिन भाषा के शब्द फोरेसिंग से लिया गया है जिसका मतलब है फोरम के समक्ष। रोमनकाल में आपराधिक मामलों को लोगों के एक समूह (फोरम) के सामने रखा जाता था। वहां पर दोनों पक्षों को बोलने का मौका मिलता था। जिसके पास ठोस सबूत होते थे उसी के पक्ष में निर्णय जाता था। अत: फोरेंसिक साइंस पूर्व में घटित घटनाओं, आधारों तथा तथ्यों का एकत्रीकरण तथा उनकी जांच करने का वैज्ञानिक तरीका है। भारत में फॉरेंसिक साइंस की शुरुआत वर्ष 1959 में सागर विश्वविद्यालय से हुई। आज आपराधिक जगत की समस्याएं सुलझाने के लिए फॉरेंसिक साइंस प्रशासन और कानून का ठोस हथियार बन चुका है। फॉरेंसिक जांच की सहायता से जांच एजेंसियां अनेक प्रकार के अपराधों का खुलासा कर अपराधियों तक पहुंच जाती हैं। खासकर इसका प्रयोग मर्डर, आत्महत्या, दुर्घटना, विस्फोट, चोरी, डकैती, जालसाजी, रेप तथा किसी भी वस्तु की

असली-नकली पहचान करने के लिए किया जाता है। हांलाकि कहा जाता है कि अपराधी कितना भी शातिर क्यों न हो कोई ना कोई सबूत छोड़ता ही है, लेकिन अगर कोई भी सबूत हाथ न लगे तो? ऐसी ही मुश्किल घटना को सुलझाने के लिए विज्ञान की जिस पद्धति का प्रयोग किया जाता है उसे फॉरेंसिक लैब कहा जाता है। बढ़ते साइबर अपराधों से बचने के लिए कुछ सतर्कता व्यक्ति खुद भी बरत सकता है। जैसे-

अपने स्मार्टफोन पर वाई-फाई के जरिए इंटरनेट एक्सेस कर रहे हैं तो उस नेटवर्क की सिक्यूरिटी या पासवर्ड के बारे में जांच परख कर लें। जिस नेटवर्क में पासवर्ड नहीं लगा है उससे अपनी डिवाइस को भी कनेक्ट ना करें। अपने ई-मेल अकाउंट को मैनेज करते वक्त किसी भी अनजान व्यक्ति द्वारा भेजा गया पॉपअप, अटैचमेंट, नोटिफिकेशन या किसी लिंक पर क्लिक ना करें। कोई भी वेबसाइट खोलने जा रहे हो तो हमेशा यूआरएल को टाइप करके खोलें। सीधे लिंक पर क्लिक करने से हैंकिंग का खतरा बना रहता है। अपने अकाउंट को पूरी तरह सुरक्षित रखें।

किसी भी इन्फर्मेशन या फोटो को शेयर सिर्फ उन्हीं लोगों को करें जिन्हें आप जानते हैं। अपना पासवर्ड बदलते रहना चाहिए। अगर कोई घटना घटित होती है तो लोकल पुलिस को इसकी जानकारी देनी चाहिए।

अपने सिस्टम को काम करने के बाद हमेशा लॉक कर देना चाहिए। हमारे देश में साइबर क्राइम के तहत कानून सख्त हैं जिसमें सजा के साथ जुमार्ना भी है। किसी कम्प्यूटर डिवाइस नेटवर्क में घुसपैठ करके डाटा से छेड़छाड़ करना हैकिंग कहलाता है। जरूरी नहीं कि ऐसी हैकिंग के दौरान उस सिस्टम को नुकसान पहुंचा ही हो। कोई नुकसान नहीं भी हुआ है तो भी घुसपैठ करना साइबर क्राइम के तहत आता है। अपराध साबित होने पर आईपीसी की धाराओं के तहत सजा तथा जुर्माने का प्रावधान है। गोपनीय डाटा चोरी करना भी साइबर अपराध है। इसमें भी जुर्माने तथा सजा का प्रावधान है।

कम्प्यूटर में आए वायरस और स्पाईवेयर को हटाने पर लोग ध्यान नहीं देते। ऐसे में वायरस दूसरों के सिस्टम तक पहुंच जाते हैं। वायरस बनाने वाले अपराधियों की पूरी एक इंडस्ट्री है। इस अपराध में भी सजा तथा जुर्माने का प्रावधान है।

यदि कोई व्यक्ति दूसरों के क्रेडिट कार्ड, इलेक्ट्रॉनिक सिगनेचर वगैरह का प्रयोग कर पैसा निकालता है तो यह भी बड़े जुर्म के दायरे में आता है। यह जुर्म भारत में सबसे ज्यादा पाए जाने वाले जुर्मों में से एक है। इसमें भी सजा तथा जुर्माना का प्रावधान है। इंटरनेट के माध्यम से अश्लीलता का व्यापार भी बढ़ा है। ऐसे में पोर्नोग्रॉफी प्रकाशित करना तथा दूसरों तक पहुंचाना भी अवैध है। इसे गंभीर अपराध में शामिल करने को लेकर भारतीय कानून ज्यादा सख्त है। इसमें सख्त जेल तथा जुर्माना है। बच्चों और महिलाओं को तंग करना, अश्लील धमकाने वाले संदेश भेजना या अन्य किसी रूप से परेशान करना भी साइबर अपराध में आता है।

भाग 3

साइबर फॉरेंसिक – नई प्रौद्योगिकी नई संभावनाएं

अध्याय पांच

साइबर अपराध की जांच-पड़ताल के अनोखे तरीके और नई तकनीक

परिचय

भारतीय साइबर अपराध समन्वय केंद्र (I4C) की स्थापना की योजना अनुमानित लागत 415.86 करोड़ रुपये के साथ अक्टूबर 2018 में अनुमोदित की गई थी । यह योजना व्यापक और समन्वित तरीके से सभी प्रकार के साइबर अपराध से निपटने के लिए है। इस योजना के सात घटक हैं, जैसे कि नेशनल साइबर क्राइम थ्रेट एनालिटिक्स यूनिट, नेशनल साइबर क्राइम रिपोर्टिंग पोर्टल, नेशनल साइबर क्राइम ट्रेनिंग सेंटर, साइबर क्राइम इकोसिस्टम मैनेजमेंट यूनिट, नेशनल साइबर क्राइम रिसर्च एंड इनोवेशन सेंटर, नेशनल साइबर क्राइम फॉरेंसिक लैबोरेट्री ईको सिस्टम और प्लेटफॉर्म फॉर ज्वाइंट साइबर अपराध जांच दल। केंद्रीय गृह मंत्रालय की पहल पर, 15 राज्यों और केंद्र शासित प्रदेशों ने संबंधित राज्यों / केंद्रशासित प्रदेशों में क्षेत्रीय साइबर अपराध समन्वय केंद्र स्थापित करने के लिए अपनी सहमति दी है। राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल (www.cybercrime.gov.in) एक नागरिक-केंद्रित पहल है जो पोर्टल के माध्यम से नागरिकों को साइबर अपराधों की ऑनलाइन रिपोर्ट करने में सक्षम बनाएगी। सभी साइबर अपराध से संबंधित शिकायतों को राज्यों और केंद्र शासित प्रदेशों की संबंधित कानून प्रवर्तन एजेंसियों द्वारा कानून के अनुसार कार्रवाई करने के लिए एक्सेस उपलब्ध है । यह पोर्टल 30 अगस्त, 2019 को पायलट आधार पर शुरू किया गया था। यह महिलाओं, बच्चों, विशेष रूप से बाल पोर्नोग्राफी, बाल यौन शोषण सामग्री, रेप/गैंग रेप से संबंधित ऑनलाइन सामग्री, आदि के खिलाफ अपराधों पर विशेष ध्यान देने के साथ सभी

साइबर अपराधों को दर्ज करने में सक्षम बनाता है।

अब तक, इस पोर्टल के साथ 700 से अधिक पुलिस जिले और 3,900 से अधिक पुलिस स्टेशन जुड़े हुए हैं। सफल कार्यान्वयन के बाद, यह पोर्टल मामलों की जांच करने के लिए कानून प्रवर्तन एजेंसियों की क्षमता में सुधार कर सकता है और अभियोजन की सफलता में सुधार करेगा। यह पोर्टल वित्तीय अपराधों और सोशल मीडिया से संबंधित अपराधों जैसे कि स्टाकिंग, साइबर बुलीइंग आदि जैसे अपराधों पर भी ध्यान केंद्रित करता है। यह पोर्टल एक समन्वित तरीके से साइबर अपराधों से निपटने के लिए विभिन्न राज्यों, जिलों और पुलिस स्टेशनों की कानून प्रवर्तन एजेंसियों के बीच समन्वय में और प्रभावी तरीके से सुधार करेगा। गृह मंत्रालय एक व्यापक और समन्वित तरीके से साइबर अपराधों से निपटने के लिए एक इको सिस्टम प्रदान करने और बनाने के लिए प्रतिबद्ध है। भविष्य में, यह पोर्टल साइबर क्राइम की रोकथाम और पोर्टल पर घटनाओं की रिपोर्ट करने के लिए जनता को स्वचालित इंटरैक्टिव सहायता प्रणाली के लिए चैटबॉट प्रदान करेगा।

राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल पर शिकायत कैसे दर्ज करें

यह पोर्टल साइबर अपराध की शिकायतों की ऑनलाइन रिपोर्ट करने के लिए पीड़ितों / शिकायतकर्ताओं को सुविधा प्रदान करने के लिए भारत सरकार की एक पहल है। यह पोर्टल केवल साइबर अपराधों से संबंधित शिकायतों, विशेष रूप से महिलाओं और बच्चों के खिलाफ साइबर अपराधों के लिए है। इस पोर्टल पर दर्ज की गई शिकायतों को कानून प्रवर्तन एजेंसियों / पुलिस द्वारा शिकायतों में उपलब्ध सूचना के आधार पर निपटाया जाता है। त्वरित कार्रवाई के लिए शिकायत दर्ज करते समय सही और सटीक विवरण प्रदान करना अनिवार्य है। आपातकालीन स्थिति में या साइबर अपराधों के अलावा अन्य अपराधों की रिपोर्टिंग के लिए कृपया स्थानीय पुलिस से संपर्क करें। राष्ट्रीय पुलिस हेल्पलाइन नंबर 100 है। राष्ट्रीय महिला हेल्पलाइन नंबर 181

है। हेल्पलाइन नंबर – 155260 पर सुबह 09:00 बजे से शाम 06:00 बजे तक संपर्क कर सकते हैं। फिलहाल 15 राज्यों और केंद्र शासित प्रदेशों ने क्षेत्रीय साइबर अपराध समन्वय केंद्र स्थापित करने के लिये अपनी सहमति व्यक्त की है। यह अत्याधुनिक केंद्र दिल्ली में स्थित है।

राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल : www.cybercrime.gov.in

यह पोर्टल नागरिकों को ऑनलाइन साइबर अपराध के खिलाफ शिकायत करने में सक्षम बनाता है। यह पोर्टल महिलाओं, बच्चों, विशेष रूप से बाल पोर्नोग्राफी, बाल यौन शोषण सामग्री, बलात्कार/सामूहिक बलात्कार से संबंधित ऑनलाइन सामग्री के खिलाफ अपराधों पर विशेष ध्यान देने के साथ सभी साइबर अपराधों के खिलाफ शिकायत दर्ज करने पर केंद्रित है।

नागरिक इस पोर्टल की वेबसाइट के माध्यम से किसी भी तरह के साइबर अपराध के बारे में शिकायत दर्ज कर सकेंगे, चाहे वह किसी भी स्थान पर हो। यह पोर्टल वित्तीय अपराध तथा सोशल मीडिया से संबंधित अपराधों जैसे कि स्टॉकिंग (Stalking) एवं साइबरबुलिंग (Cyberbullying) आदि जैसे अपराधों पर भी ध्यान केंद्रित करता है।

अन्य तथ्य :

केंद्र सरकार द्वारा साइबर अपराध के प्रति जागरुकता फैलाने और साइबर अपराध से बचाव के लिये, साइबर अलर्ट/एडवाइजरी, कानून प्रवर्तन अधिकारियों/न्यायाधीशों/अभियोजकों की क्षमता निर्माण करने तथा साइबर फोरेंसिक सुविधाओं में सुधार करने आदि के लिये कदम उठाए गए हैं। पुलिस और लोक व्यवस्था राज्य सूची का विषय हैं। अतः राज्य/संघ राज्य क्षेत्र अपने यहाँ कानून के माध्यम से अपराधों की रोकथाम, अपराधियों का पता लगाने, जाँच और अभियोजन के लिये मुख्य रूप से जिम्मेदार हैं।

साइबर क्राइम की शिकायत दर्ज कराते समय क्या क्या सबूत हो सकते हैं,

उसकी सूची नीचे दी गई हैः-

क्रेडिट कार्ड की रसीद ।

बैंक के पासबुक की प्रति ।

लिफाफा (यदि पत्र डाक या कूरियर के जरिए आया हो) ।

विवरण पुस्तिका ।

ऑनलाइन धनराशि स्थानांतरण रसीद ।

ईमेल की प्रति ।

वेबपेज की यूआरएल ।

चैट की विस्तृत जानकारी ।

संदिग्ध मोबाइल नंबर का स्क्रीन शॉट ।

वीडियो ।

तस्वीरें ।

किसी अन्य प्रकार के दस्तावेज ।

भारतीय साइबर क्राइम समन्वय केन्द्र (आई4सी) योजना का ब्योरा

1 आई4सी योजना का संक्षिप्त विवरण ।

2 आई4सी योजना के घटक ।

3 राष्ट्रीय साइबर थ्रेट विश्लेषण यूनिट (TAU) ।

4 राष्ट्रीय साइबर क्राइम रिपोर्टिंग पोर्टल ।

5 संयुक्त साइबर क्राइम जांच टीम के लिए प्लेटफार्म ।

6 राष्ट्रीय साइबर क्राइम फोरेन्सिक प्रयोगशाला पारिस्थितिकी ।

7 राष्ट्रीय साइबर क्राइम प्रशिक्षण केन्द्र (NCTC) ।

8 साइबर क्राइम पारिस्थितिकी प्रबंधन यूनिट ।

9 राष्ट्रीय साइबर अनुसंधान एवं नवोन्मेषण केन्द्र ।

आई4सी योजना का संक्षिप्त विवरण

साइबर क्राइम के विरुद्ध लड़ने में नोडल बिंदु के रूप में कार्य करना। एलईए की अनुसंधान समस्याओं/जरूरतों की पहचान करना और भारत एवं विदेश में शैक्षणिक अनुसंधान संस्थाओं के सहयोग से नई प्रौद्योगिकियां और फोरेन्सिक उपकरण विकसित करने में आर एंड डी कार्यक्लाप शुरु करना।

यह योजना 415.86 करोड़ रुपये के परिव्यय के साथ प्रस्तावित है और दो वर्ष तक चलती रहेगी।

अतिवादियों और आंतकवादियों की गतिविधियों को रोकने के लिए साइबर स्पेस के दुरुपयोग को रोकना।

तेजी से बदलती हुई प्रौद्योगिकी और अन्तर्राष्ट्रीय सहयोग के साथ कदम मिलाकर चलने के लिए साइबर कानूनों में यथापेक्षित संशोधनों का सुझाव देना।

गृह मंत्रालय में संबंधित नोडल प्राधिकारी के परामर्श से साइबर क्राइम से संबंधित अन्य देशों के साथ हुई पारस्परिक विधिक सहायता संधि

(एमएलएटी) के कार्यान्वयन से संबंधित सभी गतिविधियों का समन्वय करना।

आई4सी योजना के घटक

राष्ट्रीय साइबर थ्रेट विश्लेषण यूनिट ।

राष्ट्रीय साइबर क्राइम रिपोर्टिंग ।

संयुक्त साइबर क्राइम जांच टीम के लिए प्लेटफार्म ।

राष्ट्रीय साइबर क्राइम फोरेन्सिक प्रयोगशाला (NCFL) पारिस्थितिकी ।

राष्ट्रीय साइबर क्राइम प्रशिक्षण केन्द्र (NCTC) ।

साइबर क्राइम पारिस्थितिकी प्रबंधन यूनिट ।

राष्ट्रीय साइबर अनुसंधान एवं नवोन्मेषण केन्द्र ।

1. राष्ट्रीय साइबर जोखिम विश्लेषण यूनिट

यह कार्य राष्ट्रीय साइबर जोखिम विश्लेषण यूनिट से पूरा किया जाएगा, जो विधि प्रवर्तन कार्मिकों, निजी क्षेत्र के व्यक्तियों, शैक्षणिक संस्थाओं और अनुसंधान संगठनों को साइबर क्राइम के सभी जटिल स्वरूपों का विश्लेषण करने में सामूहिक रूप से कार्य करने के लिए एक प्लेटफार्म मुहैया कराएगा।

जोखिम विश्लेषण यूनिट, साइबर क्राइम जोखिम आसूचना रिपोर्टे भी तैयार करेगी और विशेष साइबर क्राइम केन्द्रित चर्चाओं पर आवधिक परिसंवाद आयोजित करेगी ।

विधि प्रवर्तन विशेषज्ञों और उद्योग विशेषज्ञों को एक साथ लाने के लिए मल्टी-स्टेकहोल्डर माहौल तैयार करेगी ।

2. राष्ट्रीय साइबर क्राइम रिपोर्टिंग

यह इकाई विशेषज्ञ जांच टीमों का सृजन करने के लिए राज्य और केन्द्र स्तरों पर पहले से स्थापित जांच इकाईयों और अलग-अलग क्षेत्रों के विशेषज्ञों के साथ मिलकर काम करेगी ।

तेजी से बदलते साइबर क्राइम खतरों के संबंध में वास्तविक समय पर कार्रवाई करने की क्षमता रखेगी।

साइबर और साइबर जनित अपराधों की जांच करने के लिए सहभागियों के साथ सहयोग करने में समर्थ होगी।

3. संयुक्त साइबर क्राइम जांच टीम के लिए प्लेटफार्म

इसका उद्देश्य मुख्य साइबर क्राइम थ्रेट और लक्ष्यों के विरुद्ध आसूचनाजनित अभियान चलाना और समन्वित कार्रवाई करना है।

इससे साइबर क्राइम के विरुद्ध संयुक्त पहचान करने, प्राथमिकता, तैयारी और बहु-क्षेत्राधिकार रखने की सुविधा मिलेगी।

4. साइबर क्राइम पारिस्थितिकी प्रबंधन यूनिट

पारिस्थितिकी प्रणाली विकसित करना जो शिक्षाविदों, उद्योग और सरकार को साइबर क्राइम आधारित सुस्थापित मानक प्रचालन प्रक्रियों को संचालित करने, उनकी जांच करने, साइबर क्राइम के प्रभावों और साइबार क्राइम पर कार्रवाई करने के क्षेत्र को एक साथ लाएगी व साइबर क्राइम का मुकाबला करने वाली पारिस्थितिकी प्रणाली के सभी घटकों के विकास के लिए शुरुआती (इनक्यूबेशन) सहायता प्रदान करेगी।

5. राष्ट्रीय साइबर अनुसंधान एवं नवोन्मेषण केन्द्र

उभरती हुए प्रौद्योगिकी विकासों का पता करना, ऐसी संभावित असुरक्षा की पूर्व भविष्यवाणी करना जिनका साइबर अपराधियों द्वारा दुरूपयोग किया जा सकता है।

सभी स्टेकहोल्डरों, चाहे वो शिक्षा के क्षेत्र, अथवा निजी क्षेत्र अथवा अन्तर-सरकारी संगठनों से हो, की क्षमता और विशेषज्ञता को परिपूर्ण करना।

साइबर क्राइम, साइबर क्राइम प्रभाव परिरोधन और जांच पर केन्द्रित अनुसंधान और नवोन्मेष के क्षेत्र में ऐसे सभी संगठनों के साथ सामरिक भागीदारी करना।

इंटरनेट की बदलती दुनिया

मौजूदा दौर में इंटरनेट की दुनिया सहज और सरल होने के साथ ही कई मामलों में काफी जटिल भी हो चुकी है। लिहाजा सुविधा का लाभ लेते समय सावधानी बरतना भी बेहद ज़रुरी है। ऐसा नहीं करने पर संभव है कि आप भी कभी न कभी इंटरनेट पर फैले अपराध के मकड़जाल का शिकार हो जाएं। लेकिन आप पहले से ही कुछ सतर्कता अपना लेते हैं तो किसी बड़े नुकसान से बच सकते हैं। खासकर आजकल सोशल मीडिया के जरिए वायरस या ठगी व अन्य तरह के अपराधों के मामले ज्यादा बढ़ रहे हैं। इंटरनेट के जरिए होने वाले अपराधों को साइबर क्राइम कहा जाता है, जिसमें कई प्रकार के अपराध आते हैं। साइबर क्राइम में ठगी, धोखाधड़ी, धमकी, कार्ड क्लोनिंग, छेड़छाड़ और आपत्तिजनक कंटेंट शेयर या किसी की भावनाओं को ठेस पहुंचाने के अपराध प्रमुख रूप से आते हैं। कई बार देखने को मिलता है कि लोगों को यह पता नहीं होता कि उनके साथ कुछ गलत हुआ है तो वह क्या करें? कहां जाएं और किससे शिकायत करें? लेकिन यहां हम आपको कुछ ऐसी बातें बताने जा रहे हैं जिन्हें ध्यान रखा जाए तो काफी हद तक इन

अपराधों का शिकार होने से बचा जा सकता है -

सावधानी बरतें- साइबर अपराध से बचे

1. सबूत सहेज कर रखें-

आपके साथ सोशल मीडिया पर गलत व्यवहार होता है धोखाधड़ी का शिकार होते हैं तो ऐसे में आप संबंधित पेज का स्क्रीन शॉट, लिंक, डेट और टाइम आदि को सहेज कर रखें ताकि शिकायत के वक्त संबंधित अथॉरिटी को सबूत के रूप में दिया जा सके। इससे न सिर्फ आरोपियों को पकड़ने में मदद मिलेगी बल्कि अपराध करने वालों में भी खौफ बैठेगा। खाते से पैसे निकाले गए हैं तो इसकी जानकारी तुरंत बैंक के कस्टमर केयर में दें या कार्ड ब्लॉक कराएं।

2. संबंधित अथॉरिटी को शिकायत करें-

ऑनलाइन अपराध का शिकार होने के बाद आप संबंधित अथॉरिटी या संस्था से शिकायत करें। जैसे क्रेडिट कार्ड से पैसे निकाले जाने पर बैंक से शिकायत करें, फेसबुक से कोई तंग कर रहा है तो हेल्प सेंटर के रिपोर्टिंग सेक्शन में जाकर उसकी प्रोफाइल को रिपोर्ट करें या उसे ब्लॉक करें। मामला गंभीर होने पर पुलिस से भी शिकायत करें। मामला ज्यादा बड़ा हो तो उसकी शिकायत जिले में मौजूद पुलिस की साइबर सेल में करें।

क्रेडिट कार्ड से निकासी की सीमा रखें-

अगर आपके क्रेडिट कार्ड की कभी क्लोनिंग हो जाए या चोरी हो तो भी आप ज्यादा नुकसान से बच सकते हैं। लेकिन इसके लिए जरूरी है कि आप क्रेडिट कार्ड से शॉपिंग नगद निकासी की सीमा 10-20 हजार रुपए से ज्यादा न रखें। इससे फायदा यह होगा कि चोरी करने वाला कम से कम रकम निकाल पाएगा और आप बहुत बड़े नुकसान से बच सकते हैं।

एंटीवायरस लगवाएं

हैकिंग और डाटा चोरी की ज्यादातर घटनाएं वायरस के जरिए अंजाम दी जाती हैं। ऐसे में जरूरी है कि आप अपने कम्यूटर में एंटी वायरस लगवाएं। या फिर आप एप्पल जैसे ब्रांड का कम्यूटर रख सकते हैं, जिसमें वायरस का डर नहीं होता।

अनचाहे लिंक्स पर क्लिक न करें

वायरस और हैकिंग से बचना चाहते हैं तो फेसबुक, वॉट्सएप और ईमेल से आने वाले अनचाहे लिंक्स पर क्लिक न करें। सोशल मीडिया में कोई अनजाना शख्स कुछ मेसेज करता है और किसी लिंक पर क्लिक करने के लिए कहता है तो उससे सावधान रहें। ऐसे शख्स को बिना कुछ जवाब दिए ही ब्लॉक करें।

पासवर्ड बदलते रहें

आप अपने डेबिट कार्ड या क्रेडिट कार्ड या सोशल मीडिया अकाउंट का पासवर्ड समय समय पर बदलते रहें। कई बार हम बिना लॉक किए बिना ही फोन को जेब में रख लेते हैं। जिससे फोन से कोई मैसेस या कुछ दूसरे एक्शन होने का खतरा रहता है। पासवर्ड से कम से कम 10 अंकों का रखें और कोशिश करें कि कोई नाम या डेट ऑफ बर्थ या मोबाइल नंबर जैसी चीजें न हों।

इंटरनेट : जानकारी और जोखिम का संगम

कुल मिलाकर देखें तो जिस गति से तकनीक ने उन्नति की है, उसी गति से मनुष्य की इंटरनेट पर निर्भरता भी बढ़ी है। एक ही जगह पर बैठकर, इंटरनेट के जरिये मनुष्य की पहुँच, विश्व के हर कोने तक आसान हुई है। आज के समय में हर वो चीज़ जिसके विषय में इंसान सोच सकता है, उस तक उसकी पहुँच

इंटरनेट के माध्यम से हो सकती है, जैसे कि सोशल नेटवर्किंग, ऑनलाइन शॉपिंग, डेटा स्टोर करना, गेमिंग, ऑनलाइन स्टडी, ऑनलाइन जॉब इत्यादि। आज के समय में इंटरनेट का उपयोग लगभग हर क्षेत्र में किया जाता है। इंटरनेट के विकास और इसके संबंधित लाभों के साथ साइबर अपराधों की अवधारणा भी विकसित हुई है। साइबर अपराध विभिन्न रुपों में किए जाते हैं। कुछ साल पहले, इंटरनेट के माध्यम से होने वाले अपराधों के बारे में जागरूकता का अभाव था। साइबर अपराधों के मामलों में भारत भी उन देशों से पीछे नहीं है, जहां साइबर अपराधों की घटनाओं की दर भी दिन-प्रतिदिन बढ़ती जा रही है। साइबर अपराध के मामलों में एक साइबर क्रिमिनल, किसी उपकरण का उपयोग, उपयोगकर्ता की व्यक्तिगत जानकारी, गोपनीय व्यावसायिक जानकारी, सरकारी जानकारी या किसी डिवाइस को अक्षम करने के लिए कर सकता है। उपरोक्त सूचनाओं को ऑनलाइन बेचना या खरीदना भी एक साइबर अपराध है। इसमें कोई संशय नहीं है कि साइबर अपराध एक आपराधिक गतिविधि है, जिसे कंप्यूटर और इंटरनेट के उपयोग द्वारा अंजाम दिया जाता है। साइबर अपराध, जिसे 'इलेक्ट्रॉनिक अपराध' के रूप में भी जाना जाता है, एक ऐसा अपराध है जिसमें किसी भी अपराध को करने के लिए, कंप्यूटर, नेटवर्क डिवाइस या नेटवर्क का उपयोग, एक वस्तु या उपकरण के रूप में किया जाता है। जहाँ इनके (कंप्यूटर, नेटवर्क डिवाइस या नेटवर्क) के जरिये ऐसे अपराधों को अंजाम दिया जाता है वहीं इन्हें लक्ष्य बनाते हुए इनके विरुद्ध अपराध भी किया जाता है। ऐसे अपराध में साइबर जबरन वसूली, पहचान की चोरी, क्रेडिट कार्ड धोखाधड़ी, कंप्यूटर से व्यक्तिगत डेटा हैक करना, फ़िशिंग, अवैध डाउनलोडिंग, साइबर स्टॉकिंग, वायरस प्रसार, सहित कई प्रकार की गतिविधियाँ शामिल हैं। गौरतलब है कि सॉफ्टवेयर चोरी भी साइबर अपराध का ही एक रूप है, जिसमें यह जरूरी नहीं है कि साइबर अपराधी, ऑनलाइन पोर्टल के माध्यम से ही अपराध करे। साइबर अपराध को दो तरीकों से वर्गीकृत किया जा सकता है:

1. वैसे अपराध जिनमें कंप्यूटर पर हमला किया जाता है। इस तरह के

अपराधों के उदाहरण हैकिंग, वायरस हमले, डॉस हमले आदि हैं।

2. अपराध जिनमे कंप्यूटर को एक हथियार/उपकरण/ के रूप में उपयोग किया जाता है। इस प्रकार के अपराधों में साइबर आतंकवाद, आईपीआर उल्लंघन, क्रेडिट कार्ड धोखाधड़ी, ईएफटी धोखाधड़ी, पोर्नोग्राफी आदि शामिल हैं।

साइबर कानून क्या है?

साइबर कानून शब्द का प्रयोग संचार प्रौद्योगिकी, विशेष रूप से ऑनलाइन यानी इंटरनेट के इस्तेमाल से संबंधित कानूनी पहलुओं के बारे में चर्चा करने के लिए किया जाता है। इसे कानून के एक अलग क्षेत्र के रूप में नहीं कहा जा सकता है, जैसा संपत्ति या अनुबंध के मामले में होता है, क्योंकि साइबर कानून में, कई कानून सम्बन्धी क्षेत्रों का समागम होता है. इसके अंतर्गत बौद्धिक संपदा, गोपनीयता, अभिव्यक्ति की स्वतंत्रता और अधिकार जैसे कानूनी मामले/मुद्दे शामिल हैं। साइबर कानून के विभिन्न प्रकार के उद्देश्य होते हैं। कुछ कानून इस बात को लेकर नियम बनाते हैं कि व्यक्ति और कंपनियां, कंप्यूटर और इंटरनेट का उपयोग कैसे कर सकती हैं, जबकि कुछ कानून इंटरनेट पर अवैध गतिविधियों के माध्यम से लोगों को अपराध का शिकार बनने से बचाते हैं। संक्षेप में, साइबर कानून वह प्रयास है जिसके जरिए भौतिक दुनिया के लिए लागू कानून की प्रणाली का उपयोग, इंटरनेट पर मानव गतिविधि द्वारा प्रस्तुत चुनौतियों से निपटने के लिए किया जाता है। भारत में सूचना प्रौद्योगिकी कानून (आईटी कानून) 2000, आईटी (संशोधन) अधिनियम 2008 द्वारा संशोधित साइबर कानून के रूप में जाना जाता है। इस कानून में "अपराध" के रूप में एक अलग अध्याय मौजूद है। हालांकि इसमें कई कमियां भी हैं और यह साइबर युद्ध की निगरानी के लिए एक बहुत प्रभावी कानून नहीं है, इसके अलावा विभिन्न साइबर अपराधों का उल्लेख, अपराध के उक्त अध्याय में दंड के साथ दंडनीय अपराध के रूप

में किया गया है। साइबर अपराध के अंतर्गत 3 प्रमुख श्रेणियां आती हैं: व्यक्तिगत, संपत्ति और सरकार। दूसरे शब्दों में, प्रमुख रूप से किसी व्यक्ति/निकाय, संपत्ति एवं सरकार के खिलाफ साइबर अपराध किये जाते हैं। संपत्ति विशेष के विरुद्ध साइबर अपराध: कुछ ऑनलाइन अपराध संपत्ति के खिलाफ होते हैं जैसे कि कंप्यूटर या सर्वर के खिलाफ या उसे जरिया बनाकर। इन अपराधों में डीडीओएस हमले, हैकिंग, वायरस ट्रांसमिशन, साइबर और टाइपो स्क्वाटिंग, कॉपीराइट उल्लंघन, आईपीआर उल्लंघन आदि शामिल हैं। मान लीजिए कोई आपको एक वेब-लिंक भेजे, जिसपर क्लिक करने के पश्च्यात एक वेबपेज खुले जहाँ आपसे आपके बैंक खाते/गोपनीय दस्तावेज संबंधित सारी जानकारी मांगी जाए और ऐसा कहा जाए कि यह जानकारी रिज़र्व बैंक ऑफ़ इंडिया या सरकार की ओर से मांगी जा रही है, आप वहां सारी जानकारी दे दें और फिर उस जानकारी के इस्तेमाल से आपके दस्तावेज एवं बैंक खाते के साथ छेड़छाड़ की जाये, तो यह संपत्ति के विरुद्ध साइबर हमला कहा जायेगा।

व्यक्ति विशेष के विरुद्ध साइबर अपराध: ऐसे अपराध, यद्यपि ऑनलाइन होते हैं, परन्तु वे वास्तविक लोगों के जीवन को प्रभावित करते हैं। इनमें से कुछ अपराधों में साइबर उत्पीड़न और साइबरस्टॉकिंग, चाइल्ड पोर्नोग्राफी का वितरण, विभिन्न प्रकार के स्पूफिंग, क्रेडिट कार्ड धोखाधड़ी, मानव तस्करी, पहचान की चोरी और ऑनलाइन बदनाम किया जाना शामिल हैं। साइबर अपराध की इस श्रेणी में किसी व्यक्ति या समूह के खिलाफ दुर्भावनापूर्ण या अवैध जानकारी को ऑनलाइन वितरित किया जाता है। सरकार के विरुद्ध साइबर अपराध: यह सबसे गंभीर साइबर अपराध माना जाता है। सरकार के खिलाफ किये गए ऐसे अपराध को साइबर आतंकवाद के रूप में भी जाना जाता है। सरकारी साइबर अपराध में सरकारी वेबसाइट या सैन्य वेबसाइट को हैक किया जाना शामिल हैं। गौरतलब है कि जब सरकार के खिलाफ एक साइबर अपराध किया जाता है, तो इसे उस राष्ट्र की संप्रभुता पर हमला और युद्ध की कार्रवाई माना जाता है। ये अपराधी आमतौर पर आतंकवादी

या अन्य देशों की दुश्मन सरकारें होती हैं। यह सच है कि अधिकांश इंटरनेट उपयोगकर्ता इस तथ्य पर ध्यान नहीं देते हैं कि उनकी जानकारी को हैक किया जा सकता है और ऐसे लोग शायद ही कभी अपने पासवर्ड को बदलते/दस्तावेज की सुरक्षा सुनिश्चित करते हैं। वे सतर्क होकर इन्टरनेट का उपयोग करने के विषय में जागरूकता नहीं रखते हैं और अपनी जानकारी पर साइबर हमले को लेकर सचेत नहीं रहते हैं और इसी के चलते तमाम लोग, अनजाने में साइबर अपराध की चपेट में आ जाते हैं। हमें अपने आप को और दूसरों को इसके निवारक उपायों को लेकर शिक्षित करना चाहिए, ताकि हम और आप एक व्यक्ति या व्यवसाय के रूप में खुद के बचाव के लिए सतर्कता बरत सकें। इसके अलावा साइबर अपराधों के मुद्दे से निपटने के लिए, विभिन्न शहरों के CID (आपराधिक जांच विभाग) ने विभिन्न शहरों में साइबर क्राइम सेल खोले हैं। भारत का सूचना प्रौद्योगिकी अधिनियम (IT Act) स्पष्ट रूप से यह कहता है कि जब साइबर अपराध किया जाता है, तो इसका एक वैश्विक अधिकार क्षेत्र (Jurisdiction) है और इसलिए किसी भी साइबर सेल में इसको लेकर शिकायत दर्ज की जा सकती है। गौरतलब है कि केंद्र सरकार ने साइबर अपराधों के बारे में जागरूकता फैलाने, अलर्ट/सलाह जारी करने, कानून प्रवर्तन कर्मियों/अभियोजन/न्यायिक अधिकारियों की क्षमता निर्माण/प्रशिक्षण के लिए एवं ऐसे अपराधों को रोकने और जांच में तेजी लाने के लिए साइबर फोरेंसिक सुविधाओं में सुधार आदि के लिए कदम उठाए हैं।

ई-मेल स्पूफिंग और फ्रॉड

बैंक के नंबरों से आने वाली कॉल पर सोच समझकर जवाब दें। कहीं ऐसा न हो कि आप साइबर स्पूफिंग का शिकार हो जाएं और अपने खाते में जमा रकम से हाथ धो बैठें। इन दिनों बढ़ते स्पूफिंग के मामले की रोकथाम के लिए साइबर विशेषज्ञ पुलिस के विवेचकों को इसकी जानकारी दे रहे हैं। पुलिस मुख्यालय पर स्पूफिंग को देखते हुए पिछले दिनों काफी विचार

विमर्श किया गया। विशेषज्ञों के मुताबिक फर्जी तरीके से बैंकों की तरफ से मेल भेजने या बैंकों की हेल्प लाइन के नंबरों को प्रदर्शित करने वाली फोन कॉल से खातों से रकम उड़ाने के मामले ज्यादा हैं।

स्पूफिंग अपराध में सजा का प्रावधान

ई-मेल स्पूफिंग या कॉल से होने वाले साइबर अपराध के मामलों को आईटी एक्ट-2008 के तहत दंडनीय अपराध माना गया है। इसमें मुकदमा दर्ज होने पर आरोपी को तीन साल की सजा और एक लाख रुपये जुर्माने का प्रावधान है। वहीं, आईपीसी की धारा 465 के तहत आरोपी को दो साल की सजा, जुर्माना और धारा 466 में सात साल की सजा व जुर्माने का प्रावधान है।

जानें- कैसे होती है स्पूफिंग

अभियोजन निदेशालय के अपर पुलिस महानिदेशक आशुतोष पांडेय के अनुसार, स्पूफिंग के जरिए उपभोक्ता को जिस नंबर से कॉल की जाती है। वह उसके फोन पर बैंक की हेल्पलाइन या बैंक के अधिकारी के नंबर से प्रदर्शित होता है। कई बार उपभोक्ता गूगल से बैंक की हेल्पलाइन का नंबर तलाश कर फोन करता है तब भी वह स्पूफिंग का शिकार हो जाता है। साइबर अपराधियों ने इंटरनेट पर कई फर्जी नंबर व अकाउंट पोस्ट किए हैं। उपभोक्ता जब इन नंबरों से बैंक को कॉल करता है तो वह एटीएम अथवा खाते की जानकारी हासिल करते हैं।

अपराधी खाते अथवा एटीएम को अपडेट करने के नाम पर लिंक भेजते हैं। इस पर क्लिक करते ही खाते से रकम उड़ा दी जाती है। ऐसे मामलों में किस एप या तकनीक से रोका जा सकता है इसकी विवेचकों को जानकारी दी जा रही है।

हाल में हुई साइबर अपराध से जुड़ी घटनाएं

- बिजनौर के धामपुर में बीती 5 नवंबर को आदित्यवीर सिंह के पास एसबीआई के मैनेजर के नाम से फोन आया। खाता अपडेट करने के लिए भेजे गए लिंक का इस्तेमाल करने पर खाते से 50 हजार पार कर दिए गए।

- प्रयागराज के जार्ज टाउन में एक होटल मैनेजर सनी अब्बास को स्विगी पेमेंट के लिए लिंक से भुगतान करने को कहा गया। जैसे ही लिंक पर क्लिक किया, खाते से 47,900 रुपये उड़ा लिए गए।

- लखनऊ के चिनहट में डॉ. शैलेंद्र कुमार भारती ने डेबिट कार्ड से खरीदारी की। आर्डर वापस किया तो लिंक भेजकर दस रुपये जमा करने को कहा। इसके बाद एसबीआई के खाते से 5,900 व पीएनबी से तीन हजार रुपये निकाल लिए गए।

- प्रयागराज के शिवकुटी में शुभम शर्मा को फोन-पे के फर्जी लिंक भेज कर उनके खाते से 11 हजार रुपये उड़ाए गए।

- लखनऊ के आलमबाग में रिया जैन को फर्जी लिंक भेज कर उनके खाते से 52,970 रुपये निकाल लिए गए।

कभी डाकुओं के लिए कुख्यात बाह (आगरा के पास) के बीहड़ों में अब साइबर डकैतों ने अड्डा जमा लिया है। दिल्ली, हरियाणा, राजस्थान, गुजरात और महाराष्ट्र के लगभग तीन हजार लोगों से तकरीबन डेढ़ करोड़ रुपये की ठगी करने वाले गैंग के बदमाशों को साइबर सेल ने बाह थाना क्षेत्र से गिरफ्तार किया है। ये लोग अलग-अलग राज्यों के अखबारों में विज्ञापन के जरिए एनआरआई युवतियों से डेटिंग करवाने का झांसा देते थे। इच्छुक लोगों से रजिस्ट्रेशन और होटल खर्च के नाम पर बैंक खातों में रकम जमा करवा लेते थे। गिरोह के फरार सदस्यों की गिरफ्तारी को दबिश चल रही

है। आइजी ए सतीश गणेश ने बताया कि बाह के सिंघावली निवासी सचिन और खेड़ा राठौर के मझटीला गांव निवासी दीवान सिंह मिलकर यह गिरोह चला रहे थे। 22 वर्षीय सचिन मिश्र हाई स्कूल फेल है। उसका एक रिश्तेदार ठगी का यह खेल खेलता था। उससे सीखकर दो वर्ष पहले उसने भी गिरोह बना लिया। इन्होंने भिंड के दो लड़कों को टेलिकॉलर बनाया हुआ था। इनमें से एक को एक हजार और दूसरे को डेढ़ हजार रुपये देता था। दीवान सिंह ने ठगी की रकम से 500 गज में तीन मंजिला कोठी बनाई है। वहीं सचिन की भी कोठी है।

ऐसे फंसाते थे अपने जाल में

सचिन और दीवान विभिन्न राज्यों में विज्ञापन एजेंसियों के माध्यम से ठगी का विज्ञापन प्रकाशित कराते थे। इसमें लिखा होता था कि एनआरआई गर्लफ्रेंड बनाने के इच्छुक लोग कॉल करें। इसमें एक नंबर दिया जाता था, जिसे टेलिकॉलर रिसीव करते थे। वे कॉल करने वालों को एनआरआई, विदेशी और इंडियन हर तरह की गर्लफ्रेंड उपलब्ध होने की जानकारी देते थे। कॉलर अगर इसके लिए तैयार होता था तो उससे पहले 1650 रुपये रजिस्ट्रेशन के नाम पर खाते में जमा करा लेते थे। इसके बाद महिला से मुलाकात कराने के नाम पर होटल का किराया, टैक्सी का बिल आदि के नाम पर 15 हजार से लेकर 70 हजार रुपये तक लेते थे। इसके बाद कॉलर का मोबाइल नंबर ब्लॉक कर देते।

नशे का भी था कारोबार

पुलिस को शातिरों के पास से एक डायरी मिली है। इसमें ठगी का शिकार बने ढाई से तीन हजार लोगों का लेखा-जोखा है। इसमें सभी से डेढ़ करोड़ रुपये आने का हिसाब भी है। ये ठग ओडिशा से नशे का कारोबार भी कर रहे थे। इस संबंध में उनसे पूछताछ की जा रही है। खेड़ा राठौर थाने में गिरफ्तार और फरार शातिरों के खिलाफ मुकदमा दर्ज किया गया है।

फर्जी आईडी के नंबर से करते थे कॉल

ठगी की रकम जमा कराने के लिए बैंक ऑफ बड़ौदा (भिंड शाखा) के खाते का प्रयोग किया जा रहा था। यह खाता किसी गौरव के नाम पर है। इस बैंक खाते से करोड़ों रुपये की जमा और निकासी हो चुकी है। जिस नंबर से ये कॉल करते थे, वह भी ढाई हजार रुपये में भिंड के एक व्यक्ति से खरीदी थी, पर उसकी आईडी फर्जी है।

गैंग में 24 से अधिक सदस्य

आरोपियों से विज्ञापन की छायाप्रतियां, मोबाइल नंबर, मोबाइल फोन, एक डायरी (जिसमें दो हजार लोगों के नंबर और उनसे आए रकम का ब्यौरा है) और बैंक खातों का विवरण बरामद किया गया है। इस गैंग में 24 से अधिक सदस्य हैं। इनमें मध्य प्रदेश के भी लोग शामिल हैं। इनमें छह लोग अशोक निवासी ग्राम दडहेता, जैतपुर (एमपी), नंदा, बृजेश, सुनील, खुशीलाल और सौबित फरार हैं। लेकिन अब सभी तरह के साइबर अपराध पर नज़र रखने के लिए सरकार ने एक खास एजेंसी का गठन किया है इसका नाम है भारतीय साइबर अपराध समन्वय केंद्र' (आई 4 सी)। इसके तहत कुल सात एजेंसियां काम करेंगी। सेंटर की स्थापना से लेकर इसके काम शुरु करने तक इजरायल सभी तरह की तकनीकी मदद उपलब्ध करा रहा है।

इसमें नेशनल साइबर क्राइम थ्रेट ऐनालेटिक्स यूनिट, नेशनल साइबर क्राइम रिपोर्टिंग पोर्टल, साइबर क्राइम इकोसिस्टम मेनेजमेंट यूनिट, नेशनल साइबर क्राइम ट्रेनिंग सेंटर, नेशनल साइबर क्राइम रिसर्च एंड इनोवेशन सेंटर और प्लेटफोर्म फॉर ज्वाइंट साइबर क्राइम इन्वेस्टिगेशन टीम शामिल रहेगी।

मौजूदा साक्ष्यों से पता चलता है कि साइबर अपराधों के सिलसिले में पीड़ित बहुत ही कम मामलों में रिपोर्ट दर्ज करवाते हैं और साइबर अपराधों के अन्वेषण व अभियोजन में समस्या है। यह स्थिति दर्शाती है कि साइबर

अपराधी 96% से 99% तक आश्वस्त रहता है कि उसे उसके ऐसे अपराध के लिए कभी सजा नहीं हो पाएगी। इससे यह भी पता चलता है कि सुरक्षा उत्पाद बेचने वाले विभिन्न वेंडर्स की ओर से 'सिर्फ रक्षा' की रणनीति अपनाया जाना भी प्रभावी नहीं है।

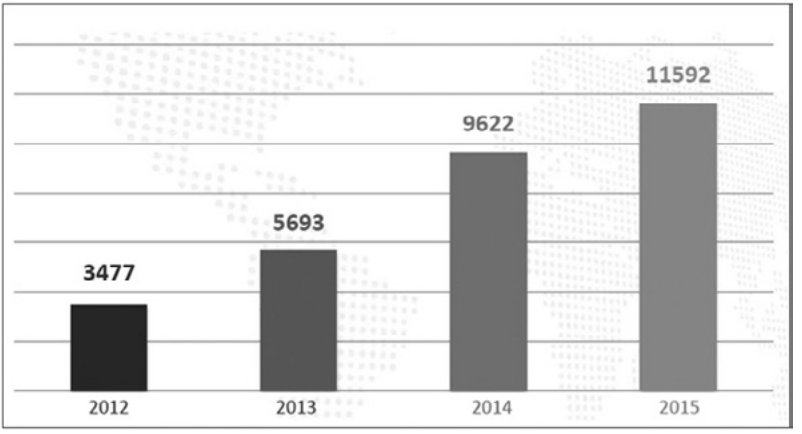
	प्रकार	**2014**	**2015**
1.	वेबसाइट को खराब किया जाना	25,037	26,244
2.	वेबसाइट में घुसपैठ और मालवेयर का प्रसार	7,286	961
3.	वायरस/मैलीसियास कोड	4,307	9,830
4.	नेटवर्क की स्कैनिंग और प्रोबिंग	3,317	3,673
5.	स्पैम	85,659	61,628
6.	फिशिंग	1,122	534
7.	अन्य	3,610	8,213
	कुल मामले	1,30,338	1,11,083

साक्ष्य

सीईआरटी-आईएन और एनसीआरबी (राष्ट्रीय अपराध रिकार्ड ब्यूरो) की ओर से प्रकाशित विभिन्न रिपोर्टों के मुताबिक भारत में साइबर अपराध के कुल दर्ज मामलों में अभियोजन और दोष सिद्धि की दर महज 4.88% और 1.78% (क्रमानुसार) ही है।

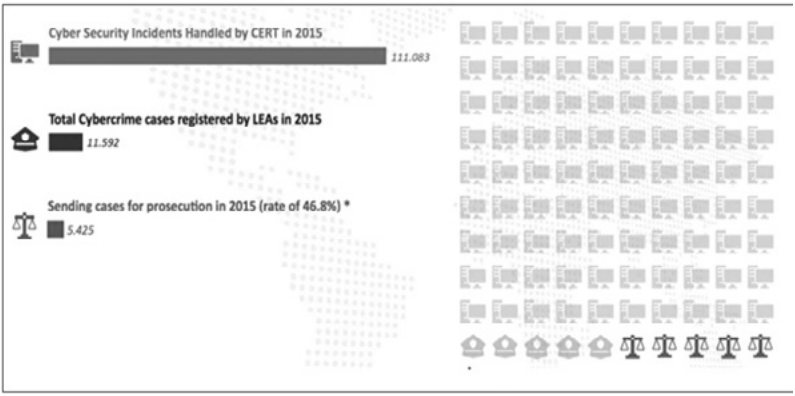
इलेक्ट्रॉनिक्स और सूचना प्रौद्योगिकी मंत्रालय के तहत इंडियन कंप्यूटर एमरजेंसी रिस्पांस टीम (सीईआरटी-आईएन) ही साइबर सुरक्षा से संबंधित मामलों के लिए नोडल एजेंसी है। सीईआरटी स्पैम, वेबसाइट को नुकसान पहुंचाने, वेबसाइट में घुसपैठ करने, फिशिंग, मालवेयर फैलाने, कोड और

नेटवर्क में अनाधिकार घुसपैठ और पड़ताल करने जैसे मामले देखता है। दिलचस्प बात यह है कि वर्ष 2015 में सीईआरटी की ओर से देखे जाने वाले साइबर सुरक्षा संबंधी मामलों में 14.7% की कमी आई है।

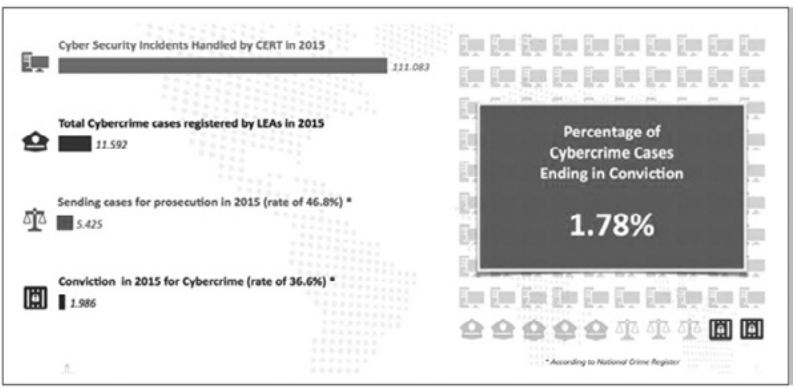


भारत में दर्ज किए गए साइबर अपराध के मामलों की संख्या

दूसरी तरफ भारत में वर्ष 2015 के दौरान दर्ज किए गए साइबर अपराध के मामलों में 20% की अच्छी-खासी बढ़ोतरी दर्ज हुई है। हालांकि भारत में साइबर अपराधों के मामलों में अभियोजन अब भी बहुत कम है। वर्ष 2015 के दौरान सिर्फ 5,425 मामले ही अभियोजन के लिए भेजे गए। वर्ष 2015 के दौरान दोष सिद्धि या सजा तक पहुंचने वाले साइबर अपराध के दर्ज मामलों का औसत तो और भी कम 1.78% ही है।



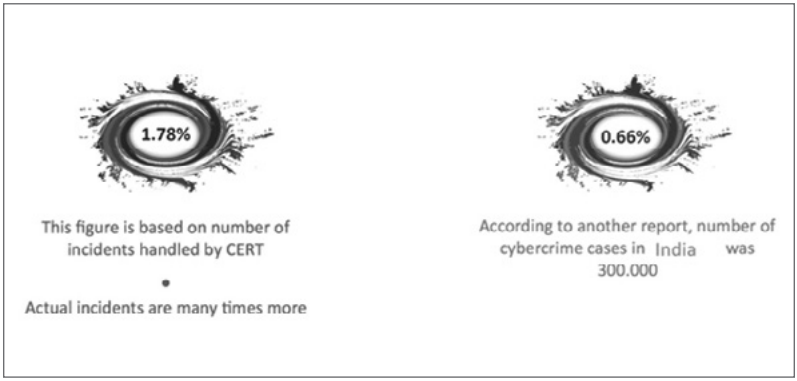
2015 में साइबर अपराध का अभियोजन



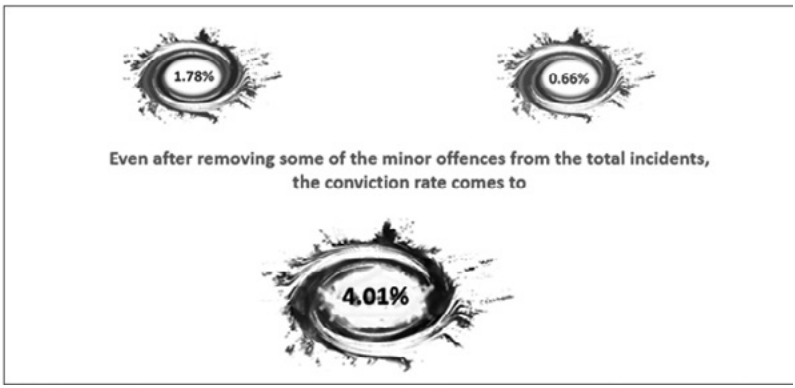
साइबर अपराधों में 2015 के दौरान अपराध सिद्धि

हालांकि वर्ष 2015 के दौरान साइबर अपराध के मामलों के दर्ज होने में बढ़ोतरी हुई, लेकिन यह संख्या (11,592) बताती है कि अब भी भारत में एलईए की वजह से साइबर अपराधों की सूचना बहुत कम ही दर्ज करवाई जा रही है। कंपनियां यह सोच कर मामले दर्ज नहीं करवातीं कि उनकी प्रतिष्ठा को नुकसान पहुंचेगा, साथ ही कंपनियों और लोगों को इन मामलों को सुलझाने को ले कर एलईए की क्षमता पर भी विश्वास नहीं है। अभियोजन तक पहुंचने वाले मामलों का प्रतिशत (कुल रजिस्टर्ड मामलों का 46%) यह भी दर्शाता है कि जिन मामलों में विभिन्न अलग-अलग कार्यक्षेत्रों से जांच की

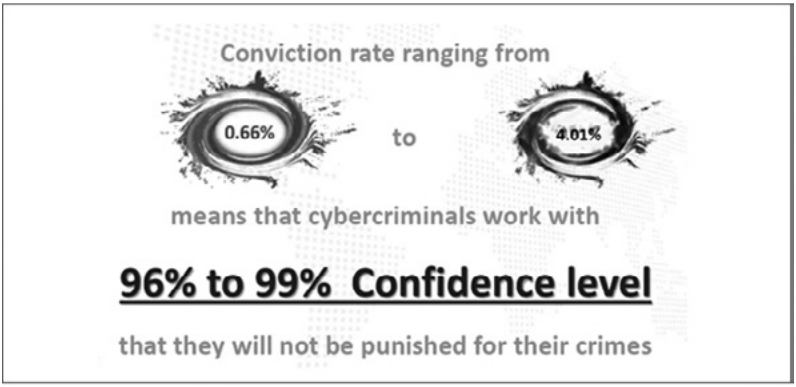
जरूरत होती है उन साइबर अपराधों की जांच की क्षमता और मजबूत किए जाने की जरूरत है।



दोष सिद्धि तक पहुंचने वाले साइबर अपराध के मामलों का प्रतिशत



छोटे अपराधों को हटा कर दोष सिद्धि तक पहुंचने वाले मामलों का प्रतिशत



साइबर अपराधों में दोष सिद्धि की निम्न दर

भारत के सूचना प्रौद्योगिकी केंद्र के रूप में मशहूर बैंगलुरु साइबर अपराध की दर में भी अव्वल है, जहां प्रति एक लाख आबादी पर साइबर क्राइम की दर 32 है। इसके बाद जयपुर में 22, लखनऊ में 21, कानपुर में 8 और मुंबई में साइबर क्राइम प्रति एक लाख आबादी पर 7 के औसत से दर्ज़ किया गया। चेन्नई, कोझीकोड, कोयम्बटूर, दिल्ली और कोलकाता में साइबर क्राइम की तादाद सबसे कम देखी गई, जहां ये प्रति एक लाख आबादी पर दो से भी कम रही। साइबर अपराधों के मामलों में अभियोजन और सजा की निम्न दर की वजह से साइबर अपराधियों के मन में भय पैदा नहीं हो पाता। इसका मतलब है कि सुरक्षित साइबर जगत को सुनिश्चित करने के लिए सिर्फ एंटी-वायरस, फायरवॉल और आईडीएस जैसे रक्षा उपाय पर ही ध्यान देते रहना काफी नहीं है। सफल अभियोजन के जरिए अपराधियों के मन में कानून का खौफ भी पैदा करना जरूरी है।

साइबर अपराध में अभियोजन और सजा की निम्न दर से निपटने के लिए जरूरी है कि:-

साइबर अपराध के मामलों में कानून का पालन करवाने वाली एजेंसियां घटना होने के बाद प्रतिक्रिया में सक्रिय होने के रवैये की बजाय पहले से सक्रिय हों। इसके लिए उन्हें निजी क्षेत्र और अकादमिक जगत के लोगों

सहित सभी संबंधित पक्षों को साथ लेना होगा।

कानून का पालन करवाने वाली एजेंसियों की क्षमता को बेहतर किया जाए। इसके लिए उनके कौशल को बढ़ाने के साथ ही ढांचागत सुविधाओं को भी मजबूत करने पर ध्यान देना होगा।

अंतरराष्ट्रीय स्तर पर खुफिया सूचना जुटाने और उन पर काम करने का मंच विकसित किया जाए।

साइबर अपराध का मुकाबला करने के लिए एजेंसियों को रणनीतिक और शोध सहयोग उपलब्ध करवाया जाए।

अध्याय छह

साइबर फॉरेंसिक : अवसर और चुनौतियां

परिचय

राष्ट्रीय अपराध रिकॉर्ड ब्यूरो ने साल 2015-17 के आंकड़े जारी कर दिए हैं। इस रिपोर्ट में दिए गए आंकड़ों के आधार पर बात करें तो साल 2015-17 के बीच देशभर में 45,705 साइबर क्राइम हुए हैं। साल 2015 में देश में 11,331, 2016 में 12,187 और 2017 में 21,593 साइबर क्राइम दर्ज हुए हैं। कुल मिलाकर देखें तो तीन सालों में साइबर क्राइम 1.7 फीसदी की दर से बढ़ा है। राष्ट्रीय अपराध रिकॉर्ड ब्यूरो ने साइबर क्राइम के आंकड़ों को राज्यवार भी जारी किया है जिसके मुताबिक वर्ष 2015 में सबसे ज्यादा साइबर क्राइम उत्तर प्रदेश में हुए हैं जिनकी संख्या 2208 है। वहीं वर्ष 2017 में यूपी में सबसे ज्यादा 4971 साइबर क्राइम हुए हैं। साल 2015-17 तक साइबर क्राइम में सबसे ज्यादा यानी 5 फीसदी की वृद्धि कर्नाटक में दर्ज की गई है। इन तीन सालों में सबसे कम साइबर क्राइम नागालैंड में हुआ है जिसकी संख्या सिर्फ 2 है, वहीं केंद्र शासित प्रदेश में अधिक साइबर क्राइम दिल्ली में (874) हुए हैं। जबकि केंद्र शासित प्रदेश में से लक्षद्वीप में साल 2015-17 के बीच कोई साइबर क्राइम हुआ ही नहीं है।

TABLE 9A.1

Cyber Crimes (State/UT-wise) – 2015-2017

S. No	State/UT	2015	2016	2017	Percentage Share of State/UT (2017)	Mid-Year Projected Population (in Lakhs) (2017)+	Rate of Total Cyber Crimes (2017)++
1	2	3	4	5	6	7	8
STATES:							
1	Andhra Pradesh	536	616	931	4.3	521.3	1.8
2	Arunachal Pradesh	6	4	1	0.0	13.3	0.1
3	Assam	483	696	1120	5.1	329.3	3.4
4	Bihar	242	309	433	2.0	1054.5	0.4
5	Chhattisgarh	103	90	171	0.8	262.9	0.7
6	Goa	17	31	13	0.1	20.4	0.6
7	Gujarat	242	362	458	2.1	637.7	0.7
8	Haryana	224	401	504	2.3	280.0	1.8
9	Himachal Pradesh	50	31	56	0.3	71.7	0.8
10	Jammu & Kashmir	34	28	63	0.3	125.9	0.5
11	Jharkhand	180	259	720	3.3	342.1	2.1
12	Karnataka	1447	1101	3174	14.6	630.9	5.0
13	Kerala	290	283	320	1.5	359.4	0.9
14	Madhya Pradesh	231	258	490	2.2	793.3	0.6
15	Maharashtra	2195	2380	3604	16.5	1219.9	3.0
16	Manipur	6	11	74	0.3	26.3	2.8
17	Meghalaya	56	39	39	0.2	28.1	1.4
18	Mizoram	8	1	10	0.0	10.8	0.9
19	Nagaland	0	2	0	0.0	24.1	0.0
20	Odisha	386	317	824	3.8	429.2	1.9
21	Punjab	149	102	176	0.8	294.6	0.6
22	Rajasthan	949	941	1304	6.0	742.5	1.8
23	Sikkim	1	1	1	0.0	6.6	0.2
24	Tamil Nadu	142	144	228	1.0	698.4	0.3
25	Telangana	687	593	1209	5.5	371.3	3.3
26	Tripura	13	8	7	0.0	38.8	0.2
27	Uttar Pradesh	2208	2639	4971	22.8	2226.1	2.2
28	Uttarakhand	48	62	124	0.6	108.0	1.1
29	West Bengal	398	478	568	2.6	946.0	0.6
	TOTAL STATE(S)	**11331**	**12187**	**21593**	**99.1**	**12613.4**	**1.7**
UNION TERRITORIES:							
30	A & N Islands	6	3	3	0.0	5.7	0.5
31	Chandigarh	77	26	32	0.1	18.9	1.7
32	D&N Haveli	0	1	1	0.0	4.4	0.2
33	Daman & Diu	1	0	0	0.0	3.5	0.0
34	Delhi UT	177	98	162	0.7	221.0	0.7
35	Lakshadweep	0	0	0	0.0	0.8	0.0
36	Puducherry	0	2	5	0.0	17.6	0.3
	TOTAL UT(S)	**261**	**130**	**203**	**0.9**	**271.9**	**0.7**
	TOTAL (ALL INDIA)	**11592**	**12317**	**21796**	**100.0**	**12885.3**	**1.7**

Note : i) '++ Crime Rate is calculated as Crime per one lakh of population.

TABLE 9A.1 Page 1 of 1

ii) '+ Population Source: Registrar General of India estimated population of 2017 based on 2001 Census.

III) As per data provided by States/UTs

देश में साइबर सुरक्षा से जुड़े मामले बढ़ रहे हैं। वर्ष 2017 में फिशिंग, वेबसाइट घुसपैठ, वायरस और रैनसमवेयर अटैक जैसे 53 हजार से ज्यादा

मामले सामने आए। राज्यसभा में एक सवाल के लिखित जवाब में सूचना प्रौद्योगिकी मंत्री रवि शंकर प्रसाद ने यह जानकारी दी। उन्होंने बताया कि इंडियन कंप्यूटर इमर्जेंसी रेस्पॉन्स टीम (सीईआरटी-इन) ने इस बार यह रिपोर्ट तैयार की है। वर्ष 2014 में साइबर सुरक्षा के 44,679 मामले देखने को मिले थे। वर्ष 2015 में इस तरह के 49,455 मामले सामने आए। वर्ष 2016 में यह आंकड़ा 50,362 हो गया। वर्ष 2017 में इनकी संख्या बढ़कर 53,081 हो गई।

श्री प्रसाद ने कहा कि आईटी व इससे जुड़ी सेवाओं का विस्तार तेजी से हो रहा है। इसके साथ साइबर अपराध भी बढ़े हैं। इन साइबर अपराध में वित्तीय धोखाधड़ी, बैंक कार्ड और ई-वॉलेट के गलत इस्तेमाल जैसे मामले शामिल हैं। नेशनल क्राइम रिकॉर्ड ब्यूरो के आंकड़े इसकी बानगी देते हैं। इनके मुताबिक, वर्ष 2014 में साइबर अपराध के कुल 9,622 मामले दर्ज हुए। वर्ष 2015 में ये बढ़कर 11,592 हो गए। वर्ष 2016 में इनकी संख्या 12,317 रही।

साइबर अपराध के मामलों पर अंकुश लगाने के लिए सरकार ने कई कदम उठाए हैं। इनमें आईटी एक्ट 2000 को लागू करना शामिल है। इस कानून में मौजूदा साइबर अपराधों से निपटने के लिए पर्याप्त प्रावधान हैं। इसके अलावा सभी राज्यों में साइबर क्राइम सेल बनाए गए हैं। इनमें साइबर अपराध के मामलों की जांच होती है।

संसद को दी गयी एक जानकारी में सरकार ने कहा है कि पिछले तीन साल में देश में सायबर क्राइम के 1,44,496 मामले सामने आये हैं। सायबर सुरक्षा से जुड़े मामलों में फिशिंग, स्कैनिंग/प्रोबिंग, वेबसाइट के जरिए धोखाधड़ी, वायरस अटैक जैसी चीजें शामिल हैं।

साइबर फॉरेंसिक साइंस का महत्व

सवाल अपनों की असली पहचान जानने का हो या फिर गुनहगारों को

पकड़ने का, फॉरेंसिक साइंटिस्ट हर जगह अपनी कारगर भूमिका निभाता है। दुनिया भर में बेतहाशा बढ़ रहे क्राइम के ग्राफ ने साइबर फॉरेंसिक विज्ञान और इसके एक्सपर्ट की मांग में भारी उछाल ला दिया है। चूंकि यह पूरी तरह साइंस की रिसर्च वाली फील्ड है, इसलिए साइंटिस्ट, स्कॉलर्स और रिसर्चरों को भी यह खूब भा रहा है, पर इस फील्ड में एंट्रेस से पहले कुछ अहम बातों पर गौर करना जरूरी है।

फॉरेंसिक साइंस का उपयोग क्रिमिनल की खोज करने के लिए किया जाता है। कभी-कभी तो ये ही डीएनए जांच के द्वारा दो बिछुड़ों को मिलाता भी है। अहम बात यह है कि अब इसमें काफी नई टेक्नॉलजी का यूज भी होने लगा है। इसके एक्सपर्ट क्राइम स्पॉट से प्रूफ इकट्ठा करते हैं और फिर उन्हें सबूत के रूप में कोर्ट में पेश किया जाता है, ताकि कानून का राज कायम रहे।

यह क्षेत्र उन लोगों के लिए बेहतर है, जो जिज्ञासु और साहसिक कार्यों में दिलचस्पी रखते हैं। दरअसल, इस क्षेत्र में काम करने वाले सभी लोगों के लिए चुनौती हर कदम पर मौजूद होती है। आपराधिक स्थलों पर मौजूद सबूतों (शारीरिक प्रमाणों) का विश्लेषण किया जाता है। फिर उसे दोषी व्यक्ति (सस्पेक्ट) से तुलना कर, कोर्ट के सामने सबसे मजबूत प्रूफ को पेश किया जाता है। इससे आपके अंदर चीजों को समझने की क्वॉलिटी होनी जरूरी है।

इस तरह के प्रूफ में ब्लड के सैंपल, सैलाइवा, शरीर के दूसरे पदार्थ, बाल, फिंगर प्रिंट्स, पैरों के निशान, यूरीन में पाए जाने वाले अल्कोहल, स्पर्म, विस्फोटक पदार्थ आदि हो सकते हैं। इन सबूतों के आधार पर ही फॉरेंसिक साइंटिस्ट रिपोर्ट तैयार करते हैं। ये ऐसे वैज्ञानिक होते हैं, जो पुलिस के साथ काम करके सही सबूतों की जानकारी प्रदान करते हैं।

फॉरेंसिक साइंस में मास्टर्स करने के लिए छात्र को ग्रैजुएशन में 60 प्रतिशत अंकों के साथ फिजिक्स, कैमिस्ट्री, बॉटनी, बॉयोकेमिस्ट्री, माइक्रोबायॉलजी,

बी.फार्मा, बी.डी.एस अथवा अप्लाइड साइंस में ग्रैजुएशन होना जरूरी है।

वहीं अगर आप डॉक्टर हैं यानी कम से कम एम.बी.बी.एस की डिग्री आपके पास है, तो फॉरेंसिक साइंस में एम.डी. करना जरूरी है। भारत के ज्यादातर बड़े मेडिकल यूनिवर्सिटीज में जहां एम.बी.बी.एस. कोर्स होता है, वहीं फॉरेंसिक साइंस में एम.डी. की पढ़ाई भी होती है।

कोई भी भारतीय जिनकी उम्र 30 वर्ष से कम हो और नीचे दिए गए विषयों में प्रथम श्रेणी में मास्टर की डिग्री प्राप्त हो वह किसी भी यूनिवर्सिटी से पी.एच.डी. कर सकता है। ये विषय हैं, फिजिक्स, कैमिस्ट्री, बॉयोकेमिस्ट्री, एंथ्रोपलॉजी, माइक्रोबायॉलजी, कंप्यूटर साइंस, कंप्यूटर इंजिनियरिंग, फॉरेंसिक साइकॉलजी आदि। या फिर इन्हीं विषयों में एम.फिल की डिग्री प्राप्त कर लें।

इस क्षेत्र में सफल होने के लिए सबसे अहम है, चीजों को जानने की जिज्ञासा। इसके अलावा एक फॉरेंसिक साइंटिस्ट में इन गुणों का होना भी आवश्यक है। जैसे, सावधानीपूर्वक कार्य करना, बुद्धिमता, टीम वर्क, तार्किक और नियमपूर्वक कार्य करने की विशेषता। इनके अलावा, वैज्ञानिक विश्लेषण करने की क्षमता का होना भी जरूरी है। प्रयोगशाला में कार्य करने के लिए आंखों की रोशनी भी सही होनी चाहिए। इनके अलावा आपका कोई क्रिमिनल बैक ग्राउंड भी नहीं होना चाहिए।

फॉरेंसिक एक्सपर्ट का कोर्स कर लेने के बाद आपको कई फील्ड में जॉब का मौका मिल सकता है। जैसे कि लॉ एनफोर्समेंट एजेंसी, पुलिस विभाग, लीगल सिस्टम, गवर्नमेंट के इन्वेस्टिगेटिव सर्विस और प्राइवेट एजेंसी में रोजगार प्राप्त की जा सकती है। इनके अलावा, विभिन्न कालेजों और संस्थानों में शिक्षण कार्य भी कर सकते हैं। सरकारी संस्थानों के अंतर्गत आई.बी., सी.बी.आई आदि आकर्षक फर्मों में इन्वेस्टिगेटिव ऑफिसर एवं स्टेट पुलिस फोर्स के क्राइम सेल में भी आपको फॉरेंसिक साइंटिस्ट के रूप में कार्य

करने का मौका मिलता है। फॉरेंसिक साइंटिस्ट के लिए फॉरेंसिक लैब में कार्य करना जरूरी होता है और कभी-कभी प्राइवेट जासूसी संस्थानों के साथ मिलकर भी काम करते हैं, ताकि क्रिमिनल और क्राइम के बीच रिलेशन का पता लगाया जा सके।

1. क्राइम सीन इन्वेस्टिगेशन

फॉरेंसिक साइंस के इस फील्ड में प्रवेश के बाद आपको जिन विषयों पर खास ध्यान देना होता है, वे हैं, सुरक्षा, सबूत से संबंधित वस्तुओं को निर्धारित एवं एकत्र करना, सबूतों को डिटेल में जानना और चल रही घटनाक्रम का फिर से यथासंभव निर्माण करना आदि। मुकम्मल बात यह है कि क्राइम सीन इन्वेस्टिगेशन का क्षेत्र काफी व्यापक होता है। इसके अंतर्गत एक साधारण से घर में लगे आग से लेकर कई मंजिला इमारत और शहरों में हुए बम विस्फोट तक जैसे भयानक हादसों की इन्वेस्टिगेशन शामिल होती है।

योग्यता

फॉरेंसिक इन्वेस्टिगेशन में डिप्लोमा या डिग्री अथवा एनालिटिकल कैमिस्ट्री में डिग्री।

2. फॉरेंसिक पथॉलजी/ मेडिसिन

फॉरेंसिक पथॉलजिस्ट का कार्य हत्या या आत्महत्या के केस में मौत के कारण और समय का पता करना होता है। इस फील्ड के जानकार द्वारा ही पोस्टमार्टम किया जाता है। मेडिकल की डिग्री (एम.बी.बी.एस) एम.डी. के साथ या फॉरेंसिक साइंस में पोस्ट ग्रैजुएट।

3. फॉरेंसिक एंथ्रोपॉलोजी

इसके अंतर्गत मानव कंकाल का अध्ययन किया जाता है और उनकी पहचान

की जाती है। किसी भी तरह के डिजास्टर्स जैसे, प्लेन क्रैश, विस्फोट, आग और अन्य कारणों से मृत्यु होने पर फॉरेंसिक एंथ्रोपोलॉजिस्ट को बुलाया जाता है। इनका कार्य क्षत-विक्षत शरीर को पहचानना, उनकी उम्र, सेक्स, पूर्वज और अन्य चीजों की खोज करना होता है। एंथ्रोपोलॉजी में पी.एच. डी. की डिग्री के साथ-साथ बॉडी पार्ट्स (एनाटॉमी) और हड्डियों की रचना (ऑस्टियोलॉजी) की पढ़ाई करना जरूरी है। इनके अलावा, मेडिकल की डिग्री, पीजी के साथ होनी चाहिए।

4. फॉरेंसिक साइकॉलजी

इसका संबंध व्यक्ति के मानसिक स्थिति से है। क्राइम के समय दोषी की मानसिक स्थिति का पता करना और कोर्ट की कार्रवाई के समय व्यक्ति मानसिक रूप से स्वस्थ है या नहीं, इन सभी बातों का पता लगाना इनका ही कार्य है। इसी तरह फॉरेंसिक डेंटिस्ट्री, सेरोलॉजी, फॉरेंसिक इंजीनियर के रूप में काम करने का भी मौका मिल सकता है।

5. इनकम (आय)

एक फॉरेंसिक एक्सपर्ट की कमाई सरकार द्वारा नियत की गई सैलरी पर आधारित होती है। फिर भी यह राशि 30-50 हजार रुपये प्रतिमाह से कम नहीं होगी। इसके अलावा, कई तरह की सुविधाएं भी मिलती हैं। अनुभव के साथ ही यह राशि भी बढ़ती जाएगी।

- इंस्टीट्यूट ऑफ क्रिमिनॉलजी ऐंड फॉरेंसिक साइंस, 4-ई, झंडेवालान एक्सटेंशन, रानी झांसी रोड, नई दिल्ली-110056

- गुरु गोविन्द सिंह इंद्रप्रस्थ यूनिवर्सिटी, कश्मीरी गेट, दिल्ली-110006

- सेंट्रल फॉरेंसिक लैबरेट्री, कोलकाता, सी.एफ.आई कॉम्प्लेक्स, 30 गोराचंद रोड, कोलकाता-700014

- डॉ. हरिसिंह गौर विश्वविद्यालय, गौर नगर, सागर, मध्य प्रदेश

- फॉरेंसिक साइंस डिपार्टमेंट, फॉरेंसिक हाउस, 30-ए, कामाराजार सालय, माइलापुर, चेन्नई-600004

- डॉ. भीमराव अम्बेडकर यूनिवर्सिटी, सिनेट हाउस, पालीवल पार्क, आगरा-282004

- पंजाब यूनिवर्सिटी, पटियाला-147002

- लखनऊ विश्वविद्यालय, बादशाह बाग, लखनऊ-226007

साइबर क्राइम की रिपोर्ट दर्ज कराने के लिए अब थानों के चक्कर काटने की जरूरत नहीं पड़ेगी। कोई भी पीड़ित घर बैठे अपने मोबाइल या कंप्यूटर से अपनी शिकायत ऑनलाइन दर्ज करा सकेगा। इसके लिए नेशनल साइबर क्राइम रिपोर्टिंग पोर्टल (एनसीआरपी) की सेवाएं शुरु कर दी गई है। इस व्यवस्था के तहत जिले के सभी थाना प्रभारियों को लॉगिन आईडी दे दी गई है। पुलिस अधीक्षक (शहर) को इस पोर्टल के लिए जिले का नोडल अधिकारी नियुक्त किया गया है। वहीं राज्य में पोर्टल के नोडल अधिकारी पुलिस महानिदेशक होंगे। इस सेवा के शुरु होने से एक तरफ पीड़ितों को सुविधा हो जाएगी, वहीं सभी थाना प्रभारियों की जिम्मेदारी तय होने से जालसाजों के लिए देश के किसी भी हिस्से में पुलिस से बच पाना मुश्किल हो जाएगा।

ऐसे काम करेगा पोर्टल

पुलिस अधीक्षक (शहर) के मुताबिक इस व्यवस्था से साइबर अपराध के मामले केंद्रीकृत हो जाएंगे। सभी मामलों को दिल्ली से देखा जाएगा। मामला जहां से संबंधित होगा, वहां के थाना प्रभारी को पोर्टल के जरिए ही गाइडलाइन मिलेगी। नई व्यवस्था के तहत अब विभिन्न जिलों में अलग से

साइबर थाना खोलने की आवश्यकता नहीं रह गई है। दरअसल यह सारा काम एनसीआरपी के जरिए ही हो जाएंगे।

ऐसे दर्ज कराएं शिकायत

नेशनल साइबर क्राइम रिपोर्टिंग पोर्टल पर शिकायत दर्ज कराने के लिए सबसे पहले https://cybercrime.gov.in खोलना होगा। इस पोर्टल पर दो विकल्प मिलेंगे। पहले विकल्प में साइबर क्राइम की जानकारी दी गई है, वहीं दूसरे विकल्प पर क्लिक करते ही एक नया विंडो खुलेगा। इस पर क्लिक करने पर दो विकल्प मिलेंगे, पहला विकल्प महिला अपराध से संबंधित साइबर क्राइम का होगा, जबकि दूसरा विकल्प अन्य प्रकार के साइबर क्राइम के लिए है।

अभी केवल महिलाओं के अपराध दर्ज होते थे

इस पोर्टल पर अभी तक केवल महिलाओं या बच्चों से संबंधित साइबर अपराध के मामलों को ही दर्ज किया जाता था। केंद्रीय गृह मंत्रालय की पहल पर इस पोर्टल को लोकप्रिय बनाने की दिशा में काम हो रहा है। अब कोई शिकायत लेकर थाने जाता है तो पहले पोर्टल पर शिकायत दर्ज करने की सलाह दी जाएगी।

साइबर अपराध – भारतीयों से जुड़े मामले

1. पुणे सिटीबैंक एमफसिस कॉल सेंटर फ्रॉड

यह सोर्सिंग इंजीनियरिंग का मामला है। चार अमेरिकी ग्राहकों के सिटी बैंक खातों से 3,50,000 अमेरिकी डॉलर बेईमानी से पुणे में फर्जी खातों में इंटरनेट के जरिए हस्तांतरित किए गए थे। कॉल सेंटर के कुछ कर्मचारियों ने अमेरिका के ग्राहकों का विश्वास हासिल कर लिया और ग्राहकों को मुश्किल परिस्थितियों में मदद करने की आड़ में पिन नंबर प्राप्त किया। बाद में उन्होंने

इन नंबरों को धोखाधड़ी करने के लिए इस्तेमाल किया। उच्चतम सुरक्षा भारत में कॉल सेंटरों में प्रचलित है क्योंकि उन्हें पता है कि वे अपना व्यवसाय खो देंगे। कॉल सेंटर के कर्मचारियों की जांच तब होती है जब वे अंदर और बाहर जाते हैं ताकि वे संख्याओं को कॉपी न कर सकें और इसलिए वे इन नोटों को नहीं देख पाए। उन्हें इन नंबरों को याद किया जाना चाहिए, तुरंत साइबर कैफे में जाकर ग्राहकों के सिटी बैंक खाते तक पहुंचा। सभी खातों को पुणे में खोला गया था और ग्राहकों ने शिकायत की कि उनके खातों से पैसा पुणे के खातों में स्थानांतरित कर दिया गया था और इसी तरह अपराधियों का पता लगाया गया था। पुलिस कॉल सेंटर की ईमानदारी को साबित करने में सक्षम रही है और उन खातों को जकड़ लिया है जहां धन हस्तांतरित किया गया था।

2. आंध्र प्रदेश कर मामला

आंध्र प्रदेश में एक प्लास्टिक फर्म के मालिक को गिरफ्तार किया गया और सतर्कता विभाग ने उसके घर से 22 करोड़ की नकदी बरामद की थी। उन्होंने उनसे बेहिसाब नकदी के बारे में स्पष्टीकरण मांगा। आरोपी व्यक्ति ने व्यापार की वैधता को साबित करने के लिए 6,000 वाउचर जमा कर दिए, लेकिन वाउचर और उसके कंप्यूटर की सामग्री की सावधानीपूर्वक जांच करने के बाद यह पता चला कि छापा मारने के बाद उन सभी को बनाया गया था। यह पता चला था कि आरोपी एक कंपनी की आड़ में पांच व्यवसाय चला रहा था और नकली और कम्प्यूटरीकृत वाउचर का उपयोग विक्रय रिकॉर्ड दिखाने और कर बचाने के लिए करता था। इस तरह आंध्र प्रदेश के प्रमुख कारोबारी की संदिग्ध रणनीति का पर्दाफाश किया गया क्योंकि विभाग के अधिकारियों ने आरोपी व्यक्ति द्वारा इस्तेमाल किए गए कंप्यूटरों को पकड़ लिया था।

3. Sony.Sambandh.Com Case

सोनी इंडिया प्राइवेट लिमिटेड द्वारा एक शिकायत दायर की गई थी, जो एक वेबसाइट www.sonysambandh.com चलाती है, जो अनिवासी भारतीयों को लक्षित करती है। वेबसाइट ने एनआरआई को ऑनलाइन भुगतान पर भारत में अपने दोस्तों और रिश्तेदारों को सोनी उत्पादों को भेजने की सुविधा प्रदान की है। कंपनी संबंधित प्राप्तकर्ताओं को उत्पाद वितरित करने का प्रयास करती है। मई 2002 में, किसी ने बारबरा कैम्पा की पहचान के तहत वेबसाइट पर लॉग इन किया और एक सोनी रंगीन टेलीविजन सेट और तारहित हेड फोन का आदेश दिया। उसने भुगतान के लिए अपना क्रेडिट कार्ड नंबर दिया और अनुरोध किया कि उत्पाद नोएडा में आरिफ अजीम को दिया जाए। भुगतान को क्रेडिट कार्ड एजेंसी द्वारा विधिवत रूप से किया गया था। उचित परिश्रम और जांच की प्रासंगिक प्रक्रियाओं का पालन करने के बाद, कंपनी ने आरीफ अजीम को सामान वितरित कर दिया। डिलीवरी के समय, कंपनी ने डिजिटल तस्वीरें लीं, जिसमें वितरण को अरिफ अजीम ने स्वीकार किया था। लेकिन डेढ़ महीनों के बाद क्रेडिट कार्ड एजेंसी ने कंपनी को बताया कि यह वास्तविक मालिक के रूप में अनधिकृत लेनदेन था। कंपनी ने केंद्रीय जांच ब्यूरो (सीबीआई) में ऑनलाइन धोखाधड़ी के लिए एक शिकायत दर्ज की, जिसमें एक मामला दर्ज किया गया था। मामले की जांच की गई और आरिफ अजीम को गिरफ्तार कर लिया गया। जांच से पता चला कि आरिफ अजीम, नोएडा में एक कॉल सेंटर पर काम करता है और काम करते समय उसने एक अमेरिकी नागरिक के क्रेडिट कार्ड नंबर तक पहुंच बना ली थी जिसका उसने कंपनी की साइट पर दुरुपयोग किया था। सीबीआई ने रंगीन टीवी और तारहित हेड फोन को पुनः प्राप्त किया। अदालत ने आरिफ अजीम को भारतीय दंड संहिता की धारा 418, 41 9 और 420 के तहत धोखाधड़ी के लिए दोषी ठहराया। यह पहली बार है कि साइबर अपराधी को दोषी ठहराया गया है। अदालत ने हालांकि, महसूस

किया कि आरोपी 24 साल का एक छोटा लड़का है और पहली बार अपराध किया है, निस्संदेह विचार लेने की आवश्यकता है। इसलिए अदालत ने अभियुक्त को एक वर्ष तक परिवीक्षा पर रिहा कर दिया। यह फैसला पूरे राष्ट्र के लिए बहुत महत्वपूर्ण है। साइबर क्राइम के इस मामले में पहली सजा होने के अलावा, यह दिखाया है कि भारतीय दंड संहिता को कुछ श्रेणियों के साइबर अपराधों के लिए प्रभावी रुप से लागू किया जा सकता है जो सूचना प्रौद्योगिकी अधिनियम 2000 के अंतर्गत नहीं आते हैं।

साइबर ठग कोबी ब्रायंट के वॉलपेपर से बना रहे शिकार, आप भी रहें सावधान

जहां दुनियाभर में दिग्गज बास्केटबॉल प्लेयर कोबी ब्रायंट के फैन्स उनके निधन से दुखी हैं, वहीं हैकर्स ने इस मौके का फायदा उठाते हुए लोगों को अपना शिकार बनाना शुरु कर दिया। इसके लिए उन्होंने ब्रायंट के वॉलपेपर का सहारा लिया। दिग्गज बास्केटबॉल प्लेयर कोबी ब्रायंट का हाल ही में हेलिकॉप्टर क्रैश में निधन हो गया था। उनके साथ उनकी बेटी जियाना और 7 अन्य लोगों की भी मौत हो गई थी। जहां दुनियाभर में ब्रायंट के फैन्स उनके निधन से दुखी हैं, वहीं हैकर्स ने इस मौके का फायदा उठाते हुए लोगों को अपना शिकार बनाना शुरु कर दिया। जालसाजों ने एक कंप्यूटर वॉलपेपर में मैलवेयर को छिपाकर लोगों को चूना लगाने की योजना बनाई थी, जो आखिरकार सामने आ गई।

मैलवेयर कंप्यूटर पर कब्जा कर लेता है

दरअसल माइक्रोसॉफ्ट ने एक ऐसे ही क्रिप्टोजैकिंग मैलवेयर का पता लगाकर उसे डिऐक्टिवेट कर दिया है जो कोबी ब्रायंट के नाइकी (Nike) वॉलपेपर में छिपा हुआ था। क्रिप्टोजैकिंग एक ऐसा मालवेयर है जो आपके डिवाइस में छिप जाता है और बिटकॉइन जैसी कीमती ऑनलाइन करेंसी की माइनिंग के लिए कंप्यूटिंग रिसोर्स की चोरी करता है। माइक्रोसॉफ्ट

सिक्यॉरिटी इंटेलिजेंस ने ट्वीट के जरिए इस मैलवेयर की जानकारी दी।

माइक्रोसॉफ्ट ने इस HTML फाइल को ट्रोजन मैलवेयर बताया है। यह सॉफ्टवेयर इस तरह डिजाइन किया गया है कि यह कंप्यूटर के सीपीयू को हाईजैक करके इसका इस्तेमाल क्रिप्टो करेंसी की माइनिंग के लिए करता है। इस पूरे प्रोसेस को ही क्रिप्टोजैकिंग कहा जाता है। माइक्रोसॉफ्ट का कहना है कि अब जब भी कोई यूजर उस वेबसाइट पर जाएगा जहां से यह वॉलपेपर डाउनलोड हो सकता है तो विंडोज का सिक्यॉरिटी सिस्टम तुरंत इसका पता लगा लेगा।

संदर्भ ग्रंथ – सूची

1. http://www.cyberforensics.in/?AspxAutoDetectCookieSupport=1
2. https://searchsecurity.techtarget.com/definition/computer-forensics
3. https://blog.eccouncil.org/the-role-of-cyber-forensics-in-criminal-offences/
4. https://www.cyberdegrees.org/jobs/computer-forensics/
5. https://resources.infosecinstitute.com/category/computerforensics/introduction/#gref
6. https://www.sciencedirect.com/topics/computer-science/cyber-forensics
7. https://www.forensiccontrol.com/what-is-computer-forensics
8. http://crawsecurity.com/landing-page/chfi/?gclid=CjwKCAiAj-_xBRBjEiwAmRbqYmrSSR0LSB4rnWJYROK1S

DrzmOxjTmeETnQURBP2pB-h2v764IHkqBoCMmsQAvD_BwE

9. https://blog.eccouncil.org/anti-forensic-techniques-a-call-for-digital-forensics/

10. अपराधों की रोकथाम औऱ प्रौद्योगिकी का इस्तेमाल – डॉ. निशांत सिंह

11. पुलिस अन्वेषण के आधुनिक एवं वैज्ञानिक तरीके, विश्लेषण – इन्दराज सिंह (पुलिस विज्ञान)

12. https://www.cgbank.in/CyberCrimePrevention.pdf

13. https://uppolice.gov.in/article/hi/cyber-crime

14. https://shodhganga.inflibnet.ac.in/bitstream/10603/229023/5/ch-2.pdf

15. https://aajtak.intoday.in/crime/story/these-ipc-sections-impose-on-cyber-criminals-1-855373.html

16. file:///C:/Users/Dr.%20Rakesh%20Prakash/Downloads/93593094d92492e93e928%2093892e92f%2092e947902%2093893e90792c930%2093693f91594d93793e%20915940%2092d94292e93f91593e-%2092a94292892e%2092494d93093f91693e.pdf

17. https://hindime.net/cyber-crime-kya-hai-hindi/

18. https://www.bbc.com/hindi/science-42081238

19. Understanding cyber crime - http://www.itu.int/ITU-D/cyb/cybersecurity/docs/Cybercrime%20legislation%20EV6.pdf

20. Cyber crime Classification and Characteristics - Hamid Jahankhani and Amin Hosseinian

21. Cyber Crime & its Categories - Kejal Vadza

22. A to Z of Cyber Crime - Asian School of Cyber Laws

23. https://www.oas.org/juridico/spanish/cyber/cyb10_slide.pdf

24. Introduction Of Cyber Crime And Its Type – Navneet Kaur

25. https://cybercrime.gov.in/UploadMedia/MHA-CitizenManualReportOtherCyberCrime-v10.pdf

26. http://www.tezu.ernet.in/wsc/pdf/notes/W03-Cyber-crime.pdf

27. https://www.us-cert.gov/sites/default/files/publications/forensics.pdf

28. https://shodhganga.inflibnet.ac.in/bitstream/10603/204375/5/chapter%204.pdf

29. http://index-of.es/Varios-2/Computer%20Forensics%20and%20Cyber%20Crime%20An%20Introduction.pdf

30. Role of Cyber Security and Cyber Forensics in India - Gulshan Srivastave,Manju Khari, Kavita Sharma, Syeda Zohra

31. Introduction to Computer Forensics and Digital Investigation - Rauf Guney

32. https://www.certconf.org/presentations/2006/files/WD4.pdf

33. https://csusm-dspace.calstate.edu/bitstream/handle/10211.3/191085/ONeilJaja_Spring2017.pdf?sequence=3

34. http://www.isfs.org.hk/publications/ComputerForensics_part1.pdf

35. https://www.bbc.com/hindi/topics/6105fd8d-33f4-4de4-9525-abf33697324a

36. https://economictimes.indiatimes.com/news/politics-and-nation/states-to-have-cyber-forensic-labs-dna-testing-facilities-soon-to-check-crimes-against-women/articleshow/68966794.cms

पं. गोविन्द वल्लभ पंत पुरस्कार योजना के अंतर्गत ब्यूरो द्वारा प्रकाशित पुस्तकें

क्र.सं.	पुस्तक का नाम	लेखक का नाम
1.	भारतीय पुलिस का इतिहास (अतीत काल से मुगल काल तक)	डॉ. शैलेन्द्र कुमार चतुर्वेदी
2.	भारत में केन्द्रीय पुलिस संगठन	श्री एच भीष्मपाल
3.	विकासशील समाज में समसामयिक पुलिस की भूमिका	प्रो. आर.एस. श्रीवास्तव
4.	ग्रामीण पुलिस–समस्याएं एवं समाधान	श्री रामलाल विवेक
5.	ग्रामीण पुलिस–समस्याएं एवं समाधान	श्री शंकर सरोलिया
6.	मादक पदार्थ–पुलिस की भूमिका	डॉ. हरीश नवल
7.	स्वातंत्रयोत्तर भारत में जनता का उत्तरदायित्व तथा पुलिस की भूमिका	डॉ. कृष्ण मोहन माथुर
8.	सामाजिक चेतना के परिप्रेक्ष्य में पुलिस की भूमिका का उदभव	प्रो. मीनाक्षी स्वामी
9.	समग्र न्याय व्यवस्था में पुलिस का स्थान एवं भूमिका	ललितेश्वर
10.	पुलिस दायित्व एवं नागरिक जागरूकता	डॉ. सी. अशोक वर्धन
11.	मानवाधिकार एवं पुलिस एक समीक्षा	डॉ. जी एस वाजपेयी
12.	नई आर्थिक नीति एवं अपराध	डॉ. अर्चना त्रिपाठी
13.	महिलाएं और पुलिस	श्रीमती अमिता जोशी
14.	बाल–अपराध	श्री गिरिश्वर मिश्र
15.	न्यायायिक विज्ञान की नई चुनौतियां	डॉ. शरद सिंह
16.	नई सहस्त्राब्दि में पुलिस कैसी हो...	डॉ. अजय शंकर पांडेय
17.	सामुदायिक पुलिस व्यवस्था	डॉ. तपन चक्रवर्ती एवं डॉ. रवि अम्बष्ट
18.	भारत में मानवाधिकार–संरक्षण एवं पुलिस	डॉ. रामकृष्ण दत्त शर्मा एवं डॉ सविता शर्मा
19.	संगठित अपराध	श्री महेन्द्र सिंह आदिल
20.	पुलिस कार्यों का निजीकरण	डॉ. शंकर सरोलिया
21.	साइबर क्राइम	डॉ. अनुपम शर्मा
22.	अपराधों की रोकथाम और प्रौद्योगिकी का इस्तेमाल	डॉ. निशांत सिंह
23.	अपराध पीड़ित महिलाओं की समस्याएं	डॉ. उपनीत लाली एवं डॉ. ऋता तिवारी

24.	व्यावसायिक यौनकर्मियों का सुधार एवं पुनर्वास	श्रीमती नीना लाम्बा
25.	वैध समस्याओं के निदान हेतु बढ़ती हिंसा प्रवृत्ति	श्री राकेश प्रकाश
26.	बंदियों का सुधार एवं पुनर्वास	प्रो. दीप्ती श्रीवास्तव
27.	आतंकवाद एवं जन साझेदारी	श्री विश्वेश प्रकाश
28.	महिला कैदी एवं जेल व्यवस्था	श्रीमती अदिती
29.	नक्सलवाद और पुलिस की भूमिका	श्री राकेश कुमार सिंह
30.	पुलिस नेतृत्व	डॉ. प्रशांत चौबे
31.	महिला पुलिस से अपेक्षाएं	डॉ. अनुपम चौबे
32.	अपेक्षित परिवर्तन में महिलाओं की भूमिका	डॉ. मंजू देवी
33.	पर्यावरण और प्राकृतिक संसाधनों के संरक्षण में पुलिस की भूमिका	डॉ. पंकज श्रीवास्तव एवं नीतू मिश्रा
34.	अपराध नियंत्रण में न्यायपालिका की भूमिका	डॉ. अदिती मिश्र
35.	महिलाओं के विरूद्ध अपराध की रोकथाम हेतु पुलिस में परिवर्तन	श्रीमती मंजूला वर्मा
36.	वरिष्ठ नागरिकों के प्रति पुलिस का व्यवहार	श्री ललितेश्वर
37.	नई प्रौद्योगिकी और पुलिस	श्री राजेश प्रताप सिंह
38.	स्मार्ट पुलिसिंग	डॉ. प्रशान्त चौबे
39.	आर्थिक अपराध तथा पुलिस	डॉ. जालम सिंह
40.	बन्दी कल्याण एवं निःशुल्क कानूनी सहायता	डॉ. सरिता भवानी मालवीय
41.	साइबर फॉरेंसिक	डॉ. राकेश प्रकाश

officialBPRDIndia

BPRDIndia

bprdIndia

Bureau of Police Research & Development India

www.bprd.nic.in

पुलिस अनुसंधान एवं विकास ब्यूरो

गृह मंत्रालय, भारत सरकार, नई दिल्ली

NH-8, महिपालपुर, नई दिल्ली-110037