Gurukul International Multidisciplinary Research Journal (GIMRJ)*with* International Impact Factor 8.357
Peer Reviewed Journal
DOI link - https://doi.org/10.69758/GIMRJ/2503I3IIVXIIIP0055

e-ISSN No. 2394-8426
Special Issue on Cyber Crime and Social Media
Issue–III(II), Volume–XIII

भारत मे सायबर अपराध और सुरक्षा मे आने वाली चुनौतिंया

डॉ. सरला धाबेकर
सहयोगी प्राध्यापक
पुरुषोत्तम थोटे समाजकार्य महाविद्यालय
नरसाळा रोड, नागपूर.
मो. नं. ९४२२४३९७५०

Abstract

भारत में हर दिन सोशल मिडिया सें सायबर अपराध के खबरों से भरे होते हैं। इसलिये हमें सोषल मिडिया प्लॅटफॉर्म का उपयोग करते समय थोडी सावधानिंया बरतनी चाहीएं। यह थोडी जागरुक होकर सायबर हमले या सायबर अपराध के खतरे को कम कर सकते हैं। बहुतही कम प्रयास सें उन सोशल मिडिया प्लॅटफॉम से आपके व्यक्तिगत डाटा कि सुरक्षा सुनिश्चित करना संभव हैं। इंटरनेट लोगों के लिए वरदान बन गया हैं। इसके अलावा इंटरनेट कि बढती आवश्यकता कें साथ हमारी जानकारी और डेटा की सुरक्षा भी एक चुनौंवती बन गयी हैं। चाहे आप एक कंपनी में मालक हों या यदी आप केवल इंटरनेट के अभ्यासक उपयोग कर्ता हैं। तो आपको इसबातकी जानकारी होती चाहीए। इंटरनेटने मनुष्यकों एकही स्थानपर बैंठकर सबकुछ आसानी सें उपलब्ध कर दिया हैं। सोशल नेटवर्कींग, ऑनलाईन शॉपींग, डाटा स्टोर करना, गेमींग करता, ऑनलाईन पढाई, ऑनलाईन जॉब, हर वो संभव काम जो मनुष्य सोच सकता हैं।

इसमें अवैध या अनाधीकृत गतीविधीयाँ शामील हैं। जो विभिन्न प्रकारके अपराध करनेके लिए प्रधोगिकी का लाभ उठाती हैं। सायबर अपराधमें अपराधोंकी एक विस्तृत शृंखला शामील हैं। यह व्यक्ती वो संघटन के साथ साथ सरकार को भी प्रभावित कर सकती हैं। साबयर सुरक्षा यह कँप्युटर, सर्वर, मोबाईल, डिव्हाईस, इलेक्ट्रॉनिक सिस्टीम, नेटवर्क और डेटा को दुर्भावनापूर्ण हमलों से बचाने का अभ्यास है। इंटरनेट का विकास और इससे संबंधित लाभों के साथ साइबर अपराध की अवधारणा भी विकसित हुई। साइबर अपराध विभिन्न रूपों में किये जाते हैं। कुछ साल पहले, इअंटरनेट के माध्यम से होने वाले अपराधें के बारे में जागरूकता की कमी थी। साइबर अपराधें के मामले में भारत भी अन्य देशों से पीछे नहीं है, जहाँ साइबर अपराध की घटनायें दिन–ब–दिन बढती जा रही है।

Keyword : **सायबर अपराध, इंटरनेट, सायबर सुरक्षा, डाटा.**

परिचय :

थोडा सतर्क रह कर और एहततियात बरतकर आप अपने आपको इन खतरों से बचा सकते हैं और आसानी से सोशल नेटवर्किंग साइटों का प्रयोग कर सकते हैं। ऐसी धोखाधडियों से स्वयं को और अपने मित्रों को बचाने के लिए आपको सतर्क रहना होगा और कुछ सुरक्षा उपाय करने होंगे।

चलिए चर्चा करे कि आप खुदकों अपने सोशल मिडीया अकाऊंट को कैसे सुरक्षित रख सकते हो आप इन सुझाँओंको अपना परिवार और मित्रोंको शेयर करें। अपने सोशल नेटवर्किंग अकाऊंट को सुरक्षीत रखने के लिए पहेला जरुरी कदम यह हैं की यह हँक ना होना पाए या खतरे में ना पडे इसके लिए आपको एक मुश्किल पासवर्ड का प्रयोग करना चाहीए और समय समय पर इसे बदलते रहें। आप जों कुछ भी सोशल नेटवर्कींग साइड पोस्ट करते हैं वह हर किसीको दिखाई देना जब आप आपनी पोस्ट की एक्सेसको अपने मित्रों और फॉलोवर्स तक सिमित नही करेंगे। आपको आपना सोशल मिडीया अकाऊंट की प्रायव्हेसी सेटींग बदलनी चाहीए और यह सुनिश्चित करले की आपको अपडेट्स पोस्ट आपके केवल मित्र फॉलोव्हर्स ही देख सकें। साइबर अपराध विभिन्न रुपों में किये जाते है। कुढ साल पहले, इंटरनेट के माध्यम से होने वाले अपराधें के बारे में जागरुकता का अभवाव था। साइबर अपराधें के मामलों के मामलों में भारत भी उन देशें से पीढे नही है, जहाँ साइबर अपराधें की घटनाओं की दर भी दिन–प्रतिदिन बढती जा रही है। साइबर अपराध के मामलों में एक साइबर अपराधी, किसी उपकरण का उपयोग, उपयोगकर्ता की व्यक्तिगत जानकारी, गोपनीय व्यावसायिक जानकारी, सरकारी जानकारी या किसी डिवाइस को अक्षमक रने के लिये कर सकता है। उपरोक्त सूचनों को ऑनलाइन बेचना या खरीदना भी एक साइबर अपराध हैं।

इसमें कोई संशय नहीं है। कि यह एक आपराधिक गतिविधि है, जिसे कंप्यूटर और इंटरनेट के उपयोग द्वारा अंजाम दिया जाता है। साइबर जिसे इलेक्ट्रॉनिक अपराध के रूप में भी जाना जाता है।, एक ऐसा अपराध है जिसमें किसी भी अपराध को करने के लिये कंप्यूटर, नेटवर्क डिवाइस या नेटवर्क का उपयोग, एक वस्तु या उपकरण के रूप में किया जाता है। जहाँ इनके (कंम्यूटर, नेटवर्क डिवाइस या नेटवर्क) जरिये ऐसे अपराधें 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 धोरी, क्रेडिट कार्ड धोखाधडी, कंप्यूटर से व्यक्तिगत डेटा हैक करना, फिशिंग, अवैध डाउनलोडिंग, साइबर स्टॉकिंग, वायरस प्रसार, सहित कई प्रकार की गतिविधियाँ शामिल हैं। गौरतलब हौ कि सॉफ्टवेयर चोरी भी साइबर अपराध का ही एक रूप है।, जिसमें यह जरुरी नही हैं। कि साइबर अपराधी, ऑनलाइन पोर्टल के माध्यम से ही अपराध करे।

सायबर अपराध : सायबर अपराध का संबंध कॅम्पूटर द्वारा होनेवाले सुचनाओं के आदान–प्रदान एवं व्यापारिक लेनदेनसें है। इंटरनेट के माध्यम से होनेवाला अपराध सायबर अपराध कहलाता है।

प्रकार :

• ई–मेल स्पूफिंग – आपको ऐसे ई–मेल भेजकर जो वास्तविक लगे तथा विश्वसनीय ई–मेल आई डी से भेजा गया लगे किंतु वास्तव में ऐसा नहीं होता।

• द्वेषपूर्ण फाइल एप्लीकेशन : आपके स्मार्टफोन तथाि व्यक्तिगत डाटा तक पहुंच बनाने के लिए सीधे मैसेज भेजना, गगेमिंग, ई–मेल और वेबसाइट के द्वारा आपको द्वेषपूर्ण तथा बुरे एप्लीकेशन और फाइल भेजना।

• सामाजिक इंजिनिअरिंग : सामाजिक इंजीनियरिंग एक ऐसी तकनीक है जिसका प्रयोग साइबर अपराधियों द्वारा आपसे जानकारी प्राप्त करने के लिए आपका विशस जीतने के लिए किया जाता है। आपकी जानकारी प्राप्त करने तथा/अथवा आपको कुछ नुकसान पहुंचाने के लिए इस बात का प्रयोग करता है। कि आपको सबसे अधिक क्या पसंद है। मान लीजिए आपको ऑनलाइन गेम खेलना पसंद है।. बहरुपिया एक अन्य बच्चे की तरह व्यवहार करेगा तथा आपको बातचीत तथा जानकारी साझा करने के लिए आमंत्रित करेगा।

• डिस्ट्रीब्यूटेड डिनायल–ऑफ–सर्विस (DDoS) अटैक : इसका प्रयोग किसी ऑनलाईन सेवा को अनुपलब्ध बनाने और विभिन्न स्त्रोंतों से वेबसाइट पर अत्यधिक ट्रैफिक के माध्यम से नेटवर्क को बाधित करने के लिये किया जाता है।

• बॉटनेट : यह कंप्यूटर का एक ऐसा नेटवर्क हैं जिसे दूर बैठे हैकर्स द्वारा बाह्य रुप से नियंत्रित किया जाता है। रिमोट हैकर्स या तो स्पैम भेजते हैं या इन बॉटनेट के माध्यम से अन्य कंप्यूटरों पर हमला करते हैं।

• पहचान की चोरी (Identify Theft) : या सायबर अपराध तब होता है जब कोई अपराधी किसी उपयोगकर्ता की व्यक्तिगत या गोपनीय जानकारी तक पहुँच प्राप्त कर लेता है, जिसके परिणामस्वरुप वह प्रतिष्ठा धूमिल करने या फिरौती मांगने की कोशिश करता है।

• साइबर स्टॉकिंग : इस प्रकार के साइबर अपराध में ऑनलाइन उत्पीडन शामिल होता है जहाँ उपयोगकर्ता को ढेर सारे ऑनलाईन संदेशों और ईमेल का सामना करना पडता है। सामान्यत: साइबर स्टॉक किसी उपयोगकर्ता को डराने के लिये सोशल मिडिया, वेबसाइट और सर्च इंजन का उपयोग करते है।

• (जॉबफ्रॉड) नौकरी से संबंधित जालसाजी : किसी कर्मचारी अथवा भावी कर्मचारी द्वारा अपने नियोक्ता के प्रिति धोखाधडी या कपटपूर्ण निष्पण करना।

बैकिंग फ्रॉड : स्वयं कारे बैंक या अन्य वित्तीय संस्थान के रूप में प्रस्तुत करके जमाकर्ता के खाते से धोखाधडी करके धन प्राप्त करना।

• फिशिंग : यह एक प्रकार का सोशल इंजीनियरिंग हमला है जिसका उपयोग अक्सर उपयोगकर्ता का डेटा चुराने के लिये किया जाता है।, जिसमें लॉगिन क्रेडेंशियल और क्रेडिट कार्ड नंबर शामिल हैं। ऐसा तब होता है जब एक हमलावर एक विश्वसनीय संस्था के रूप में किसी पीडित को ईमेल, त्वरित संदेश या टेक्स्ट संदेश के माध्यम से धोखा देता है।

डेटा संरक्षण की आवश्यकता : • निजता की सुरक्षा • विभिन्न एजंन्सियों के द्वारा निगरानी को रोकना • वर्ष २०१८ कॅबिज एनालिटिका डेटा विवाद • आर्थिक क्षति : • सायबर अपराधोकिं बढती जटिलता

भारत में सायबर अपराधों सें निपटने हेतू सरकारकी भूमिका:

• भारतीय सायबर अपराध समन्वय केंद्र ये केंद्र पुरे देष मे सभी प्रकारके सायबर अपराधोंसे निपटने के प्रयासों का समन्वय करता है। • राष्ट्रीय सायबर फॉरेन्सीक प्रयोगशाळा यह ऑनलाईन तथा ऑफ लाईन दोनो तरीकोंसे सभी राज्य केंद्रशासीत प्रदेश पुलीस के जाँच अधिकारीयों को प्रारंभिक चरण की सायबर फॉरेंसीक सहायता प्रदान करती है • साईट्रेन पोर्टल सायबर अपराध जाँच फारेंसिक और अभियोजन के महत्वपुर्ण पहेलूंओंपर ऑनलाईन पाठ्यक्रमोकें माध्यम सें पुलीस अधिकारीयोकं न्यायीकअधिकारीयों तथा अभियोजको की क्षमता निर्माण हेतू एक विषाल ओपन ऑनलाईन पाठ्यक्रम • राष्ट्रीयश सायबर अपराध रिपोर्टिंग पोर्टल एक ऐसा मंच जहाँ जनता सायबर अपराध कि घटनाओंकी रिपोर्ट कर सकतीर है, जिसमें महिजाओं एवं बचचों के प्रति अपराधें पर विशेष ध्यान दिया जाता है। • नागरिक वित्तीय साइबर फ्रॉड रिपोटिंग और प्रबंधन प्रणाली यह वित्तीय धोखाधडी की तत्काल रिपोटिबंग और टोल–फ्री हेल्पलाईन के माध्यम से ऑनलाइन साइबर शिकायतें दर्ज करने में सहायता हेतु एक प्रणाली है। • महिलाओं एवं बच्चों के प्रति साइबर अपराध निवारण ;ब्ब्ब्द्ध योजना : साइबर अपराधें के जाँच में कानून प्रवर्तन एजेकंसियों की क्षमताओं को विकसित करने के लिये राज्यों/ केंद्रशासित प्रदेशें को वित्तीय सहायता प्रदान की जाती है। • संयुक्त साइबर समन्वय दल : राजें/केंद्रशासित प्रदेशों की कानून प्रवर्तन एजेंसियों के बीच, विशेष रूप से साइबर–अपराधें से संबंधित बहु–क्षेत्राधिकर वाले क्षेत्रों में समन्वय बढाने के लिये इस दल का गठन करना। • पुलिस के आधुनिकीकरण के लिये केंद्रीय सहायता: आधुनिक हथियार, उन्नत संचार/फोरेंसिक उपकरण तथा साइबर पुलिसिंग उपकरण करने के लिये राज्यों/केद्रशासित प्रदेशों को वित्तीय सहायता प्रदान करना।

भारत में साइबर सुरक्षा से संबंधित चुनौतियाँ:

लाभ–उन्मुख अवसंरचना की मानसिकता उदारीकरण के बाद से सूचना प्रौद्योगिकी (T), बिजली और दूरसंचार क्षेत्र में निजी क्षेत्र द्वारा वृहत निवेश किया गया है। ऑपरेटर सुरक्षात्मक बुनियादी ढाँचे में निवेश नहीं कर रहे हैं, बल्कि वे केवल लाभदायक बुनियादी ढाँचेपर ध्यान केंद्रित कर रहें हैं, क्योंकि उन्हे लगता है कि साइबर हमले की तैयारियों पर निवेश से अच्छा मुनाफा नहीं हो सकता है। सभी ऑपरेटर लाभर पर अधिक केंद्रित हैं और अवसंरचना में निवेश नहीं करना चाहते क्योंकि वहाँ उनके लिये लाभ के अवसर नहीं है। पृथक प्रक्रियात्मक संहिता का अभाव साइबर या कंप्यूटर संबंधी अपराधों की जाँच के लिये कोई पृथक प्रक्रियात्मक संहिता मौजूद नहीं है। साइबर हमलों की अंतरराष्ट्रीय (ट्रांस–नेशनल) प्रकृति :

अधिकांश साइबर अपराध प्रकृति में ट्रांस–नेशनल स साक्ष्य एकत्र करना न केवल कठिन बल्कि एक भारत में साइबर अपराधें से निपटने के लिये किये जाने वाले उपाय:

• साइबर सुरक्षा जागरूकता अभियान

सरकारों का विभिन्न स्तरों पर साइबर धोखाधडी के संबंध में बडे पैमाने पर साइबर सुरक्षा जागरुकता अभियान चलाने, मजबूत, अद्वितीय पासवर्ड एवं सार्वजनिक वायफाय का उपयोग करने आदि में सावधानीं बरतने की आवश्यकता है।

• सायबर बिमा : ऐसी साइबर बिमा पॉलीसीयाँ विकसित की जानी चाहीए जो विभिन्न व्यवसायों और उद्योग कि विशिष्ट आवश्यकता हो के अनुरुप हैं। अनुकुलित नितियाँ यह सुनिश्चित करने में सहायता करेगी की संघटनों के पास उनके सामने आनेवाली सबसे प्रासंगिक सायबर जोखिम के लिए कव्हरेज है। सायबर बिमा सायबर घटनाओंसे होनेवाले नूकसान के खिलाप

वित्तीय कव्हरेज प्रदान करता है। तथा इन घटनाओंको के वित्तीय प्रभाभाव को कम करने संघअन अधिक तेजीसें सुचारु रूपसे अपना संचालन जारी रख सकता है।

• डेटा संरक्षण कानुन :

डेटा को नई मुद्रा कहा जाता हैं। इसलिए भारत में एक सक्त डेटा सुरक्षा व्यवस्था की आवश्यकता है।डेटा संदर्भमें युरोपिय संघ का सामना सामान्य डेटा संरक्षण विनियमन और भारत का व्यक्तिगत डेटा संरक्षण अधिनियमन २०१९ सही दिशा में उठाया गया कदम है।

• सहयोगात्मक त्वरीत प्रतिक्रिया तंत्र :

भारत जैसे देश में जहाँ नागरिक सायबर अपराध के प्रती अधिक संवेदनशील हैं। एक सहयोगात्मक त्वरीत प्रतिक्रिया तंत्र की आवश्यकता है। यह तंत्र सभी पंक्षो को संघटीत करेगा तथा कानून लागू करनेवाले को तूरंत कारवाई करके तथा नागरीक एवं व्यवसायीयों को बढते खतरेंसे बचानेमें संक्षम बनाएगा। इस संदर्भ में भारतीय सायबर अपराध समन्वय केंद्र सायबर सुरक्षा जाँच को केंद्रियकृत करने प्रतिक्रीया उपकरनो के विकासीतकी प्राथमिकता इस खतरे को राकने कें लिए निजी कंपनीयों को एकसाथ लाने का सहायता करेगा।

निष्कर्ष :

सूचना साझा करने तथा साइबर सुरक्षा अनुसंधान एवं विकास में संयुक्त प्रयासों को मजबूत कर वैश्विक सहयोग सुनिश्चित करना आवश्यक हैं क्योंकि अधिकांश साइबर हमले सीमाओं के पार से होते हैं।

कॉरपोरेट्स या संबंधित सरकारी विभागों के लिये यह महत्वपूर्ण है कि वे अपने संगठनों में कतियों का पता लगाएँ और उन कमियों को दूर करें तथा एक स्तरित सुरक्षा प्रणाली बनाएँ जिसमें विभिन्न स्तर पर सुरक्षा खतरे की खुफिया जानकारी साझा की जा सकें। भारतीय संविधान की सातवीं अनुसूची के अनुसार, साइबर अपराध राज्य सूची के अंतर्गत आती है। इसमें अवैध या अनाधिकृत गतिविधियाँ शामिल हैं जो विभिन्न प्रकार के अपराध करने के लिये प्रौद्योगिकी का लाभ उठाती है। साइबर अपराध में अपराधी की एक विस्तृत शृंखला शामिल है। यह व्यक्तियों, संगठनों के साथ–साथ सरकारों को भी प्रभावित कर सकता है।

संदर्भ :

Cyber Crime @Coe Update on Council of Europe activities 04 Cyber Crime, 2017.

कुमारी सिमा, 'सोशल मिडिया आणि सायबर अपराध,' अंतरराष्ट्रीय हिंदी एवं सामाजिक विज्ञान शोध पत्रिका इशू व्हॅलून १२ इशूज ०३