Gurukul International Multidisciplinary Research Journal (GIMRJ)*with* International Impact Factor 8.357
Peer Reviewed Journal
DOI link - https://doi.org/10.69758/GIMRJ/2503I3IIVXIIIP0058

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

सायबर क्राइम आणि सोशल मीडिया मार्केटिंग

Dr. Priyanka Ambade-Ukey
Faculty of Sociology (Social Work)
(Autonomous) Department, RTMNU,
Mahatma Phule Campus, Nagpur.

गोषवारा

इंटरनेटच्या उत्क्रांती आणि त्याच्या सर्वव्यापी उपस्थितीचे वर्णन करण्याचा प्रयत्न म्हणजे या सायबर स्पेसने जगाच्या कानाकोपऱ्यात साऱ्यांप्रमाणे पाय रोवले आहेत. प्रत्येक होमो सेपियन्स स्वेच्छेने किंवा अनिच्छेने, निर्विवादपणे किंवा अप्रत्यक्षपणे या सुपर हायवेशी जोडलेले आहेत. पण पाप आणि पुण्य या एकाच नाण्याच्या इंटरनेटच्या दोन बाजू आहेत, त्यांचा सभ्यतेवर सकारात्मक आणि नकारात्मक प्रभाव पडतो. आपण या ऑनलाइन नेटवर्कचा सायबर गुन्ह्याच्या नावाने उदयास आलेल्या आणि विकसित झालेल्या सभ्यतेवर होणाऱ्या विरोधी प्रभावावर लक्ष केंद्रित करणार आहोत.

सायबर गुन्ह्यांचा सोशल मीडिया मार्केटिंग आणि बौद्धिक संपदा अधिकारावर होणाऱ्या विपरित परिणामाबद्दल चर्चा केली जाईल. सोशल मीडिया मार्केटिंग एकतर पीडित किंवा गिझमो अशी दुहेरी भूमिका बजावू शकते. दोन्ही प्रकरणांमध्ये एखाद्या व्यक्तीच्या किंवा व्यवसायाच्या बौद्धिक संपदा अधिकारांचे उल्लंघन होत आहे. भारतामध्ये सायबर गुन्ह्यांमुळे निर्माण झालेला हाहाकार, इतर राष्ट्रांच्या तुलनेत सायबर गुन्ह्यांपासून संरक्षण देण्याबाबतही ते चर्चा करेल. यात माहिती तंत्रज्ञान कायदा, 2000 द्वारे सध्या लागू होत असलेला सायबर कायदा आणि या क्षेत्रातील प्रगतीशील सुधारणा, सोशल मीडियावरील सायबर गुन्हे कमी करण्यासाठी आणि काही शिफारशी यावरही प्रकाश टाकला आहे.

परिचय

इंटरनेट किंवा सुपरहायवेने आपले पाय एका ध्रुवावरून दुसऱ्या खांबापर्यंत पसरवले आहेत आणि प्रत्येक माणसाच्या जीवनाला स्पर्श केला आहे. आपण इंटरनेटचा विरोधाभासी प्रभाव, त्याचे फायदे आणि शक्ती लक्षात घेऊन चर्चा करू. इंटरनेट हे आजकाल वर्ल्ड वाइड वेबचे समानार्थी आहे (WWW म्हणून संक्षिप्त), जे इंटरनेटचे कार्यात्मक एकक आहे. वर्ल्ड वाइड वेब हे एक जटिल नेटवर्क आहे ज्यामध्ये विविध लोकांमध्ये संवाद, सॉफ्टवेअर आणि सेवा यांचा समावेश होतो. हे त्याच्या प्रभावी कार्यासाठी विविध संप्रेषण साधने आणि नेटवर्क आणि डेटा वितरणावर अवलंबून आहे. तंत्रज्ञानातील सुपरफास्ट प्रगतीमुळे त्याच्या सहजतेमुळे, माहितीचा सुपरहायवे प्रत्येक व्यक्तीची गरज बनला आहे. व्यवसाय, सैन्य, सामान्य नागरिक आणि सरकार अशा प्रत्येक विभागात त्याच्या सेवा वापरल्या जातात. ARPANET (द ॲडव्हान्स्ड रिसर्च प्रोजेक्ट्स एजन्सी नेटवर्क) प्रदान करत असलेल्या पारदर्शकते प्रमाणेच संस्था आणि व्यक्तींना गोपनीयता आणि सुरक्षितता राखणे कठीण झाले आहे आणि ही पारदर्शकता आणि सुलभता वाढल्याने सायबर गुन्ह्यांमध्ये वाढ होईल.

शिकण्याचे परिणाम

- व्यक्ती आणि समाजावर सायबर गुन्ह्यांची व्याप्ती आणि प्रभाव समजून घेणे.
- वय आणि लिंग असमानतेसह सायबर गुन्ह्यांचा बळी घेण्याशी संबंधित लोकसंख्याशास्त्रीय नमुने ओळखणे.
- फिशिंग, ओळख चोरी आणि सायबरस्टॉकिंग यांसारख्या सायबर गुन्हेगारांद्वारे नियोजित सामान्य कार्यपद्धती ओळखणे.
- सायबर धोक्यांच्या वैविध्यपूर्ण स्वरूपाचे आणि सायबरसुरक्षेसाठी बहुआयामी दृष्टीकोनांच्या गरजेची प्रशंसा करणे.
- सायबर धोके कमी करण्यासाठी आणि सायबर गुन्ह्यांपासून संरक्षण करण्यासाठी सतत जागरूकता आणि शिक्षणाचे महत्त्व मान्य करणे.

सायबर गुन्हे

कायदेशीर चौकटीत सायबर गुन्हे ही जागतिक पातळीवरील सर्वात गुंतागुंतीची समस्या बनली आहे, जी शारीरिकरित्या गुंतल्याशिवाय केली जाऊ शकते. हे संगणक किंवा लहान बार फोन सारख्या कोणत्याही सॉफ्टवेअर डिव्हाइसवरून वचनबद्ध केले जाऊ शकते.

यामुळे सायबर गुन्हेगारांना प्रतिकारशक्ती मिळाली आहे आणि त्यांना त्यांची ओळख लपवणे सोपे झाले आहे. सायबर गुन्ह्यांना मदत करण्यासाठी आणि ते रोखण्यासाठी तंत्रज्ञान हे दोन्ही माध्यम म्हणून काम करते. हे गुन्हेगार आणि गुन्हेगारी प्रतिबंधक दोघांनाही संधी प्रदान करते. सायबर गुन्ह्यात सायबर जगतात संगणकाच्या मदतीने किंवा त्याच्या विरोधात केलेल्या सर्व नकारात्मक क्रियाकलाप, गैरवापर किंवा भ्रष्टाचार यांचाही समावेश होतो. सायबर गुन्हे हे बेकायदेशीर कृत्य आहेत जिथे संगणक एक उपकरण म्हणून काम करतो आणि यामुळे संगणक वापरून गुन्ह्याच्या नेहमीच्या पद्धतीत बदल होतो.

सायबर गुन्ह्याच्या व्याख्या :"इलेक्ट्रॉनिक ऑपरेशन्सद्वारे निर्देशित केलेले कोणतेही बेकायदेशीर वर्तन जे संगणक प्रणालींच्या सुरक्षेला लक्ष्य करते आणि त्यांच्याद्वारे प्रक्रिया केलेल्या डेटाला सायबर गुन्हा म्हणतात."

सायबर गुन्हे हे सध्याचे अद्ययावत आणि अत्यंत कार्यक्षम आहेत ज्यात साधन आणि त्याचा बळी सारखीच उपकरणे आहेत. संगणक हॅकिंग, स्पूफिंग, ई-मेल बॉम्बिंग, इंटरनेट टाइम थेफ्ट, वेब हॅकिंग, सायबर स्टॉलिंग, पोर्नोग्राफी, सॉफ्टवेअर पायरसी आणि सायबर दहशतवाद इत्यादी काही उदाहरणे आहेत.सायबर गुन्ह्यांमध्ये वाढ नुकत्याच झालेल्या ढोबळ मानाने सायबर गुन्ह्यांच्या घटनांमध्ये दरवर्षी 107% वाढ होत आहे. 2 भारतातील सायबर गुन्ह्यांमध्ये वाढ होण्याचा हा दर भयावह आहे. जरी सायबर गुन्ह्यांचा वाढीचा दर आणि वेबचा वापरकर्ता आधार सारखा नसला तरी डेटा सांगतो की ते एक निश्चित, समान पॅटर्नचे अनुसरण करतात असे दिसते, तर 2013 आणि 2014 या दोन्ही वर्षांमध्ये सायबर गुन्ह्यांमध्ये वाढ 65% पेक्षा जास्त आहे; 2 2013 मध्ये भारतामध्ये इंटरनेट फायद्याचा आधार सुमारे 18% आणि 27% पर्यंत वाढला आहे. माहिती तंत्रज्ञान कायद्यांतर्गत ७२१० प्रकरणे नोंदवली गेली आणि त्यापैकी फक्त 2013 ते 2014 या वर्षात 4246 जणांना ताब्यात घेण्यात आले. माहिती तंत्रज्ञान कायद्यांतर्गत नोंदवलेल्या गुन्ह्यांच्या संख्येत झपाट्याने आणि सतत वाढ झाल्याचे दिसून आले आहे. युनियनने हे देखील मान्य केले आहे की दररोज नवीन तंत्रज्ञान आणि उपकरणांच्या प्रगतीमुळे देशात सायबर गुन्ह्यांमध्ये वाढ होत आहे.

सोशल मीडिया

सोशल मीडियाला तृतीय पक्ष साधन म्हणून संबोधले जाऊ शकते जे सार्वजनिक आणि व्यावसायिक संस्थांना व्हर्च्युअल गट आणि नेटवर्कमध्ये विविध प्रकारची माहिती आणि कल्पनांची देवाणघेवाण आणि संवाद साधण्यासाठी व्यासपीठ प्रदान करते. सोशल मीडियाची व्याख्या करणे हे एक आव्हानात्मक कार्य आहे कारण ते त्याच्या उदयापासूनच्या अस्थिरतेमुळे, परंतु ते मानवजातीसाठी वरदान ठरले आहे कारण त्यात इंटरनेट आधारित ऍप्लिकेशन समाविष्ट आहे जे वापरकर्त्याला उर्वीरत जगाशी कनेक्ट करण्याची, माहिती तयार करण्यास आणि सामायिक करण्यास अनुमती देते.

आजच्या वर्तमान उद्देशांसाठी "सोशल मीडिया" परिभाषित करण्यासाठी, साहित्यात उपस्थित असलेल्या व्याख्यांचे संश्लेषण करतो आणि वर्तमान सोशल मीडिया सेवांमध्ये खालील समानता ओळखतो:

1) सोशल मीडिया सेवा (सध्या) वेब 2.0 इंटरनेट-आधारित अनुप्रयोग आहेत,

2) वापरकर्त्याने व्युत्पन्न केलेली सामग्री ही सोशल मीडियाचे जीवन आहे,

3) व्यक्ती आणि गट सोशल मीडिया सेवेद्वारे डिझाइन आणि देखरेख केलेल्या साइट किंवा ॲपसाठी वापरकर्ता-विशिष्ट प्रोफाइल तयार करतात,

4) सोशल मीडिया सेवा इतर व्यक्ती किंवा गटांशी प्रोफाईल कनेक्ट करून ऑनलाइन सोशल नेटवर्क्सचा विकास सुलभ करतात.

सोशल मीडियाचा विकास प्रत्यक्षात मेमरी साठवण्यासाठी, नवीन माहिती शिकण्यासाठी आणि एक्सप्लोर करण्यासाठी, जाहिराती आणि स्वत:चा प्रचार आणि जगाशी संपर्क साधण्यासाठी आधार म्हणून केला गेला. यामुळे बऱ्याच लोकांना त्यांच्या व्यवसायात उदयास येण्यास, त्यांचे कुटुंब आणि मित्रांशी जोडले जाण्यास, जगभरातील नवीन कल्पनांशी परिचित होण्यास आणि इतर अनेकांना मदत झाली आहे.

सोशल मीडिया मार्केटिंग

सोशल मीडिया मार्केटिंग (SMM) हा इंटरनेट मार्केटिंगचा एक प्रकार आहे जो सोशल नेटवर्किंग वेबसाइट्सचा विपणन साधन म्हणून वापर करतो. कंपनीला ब्रँड एक्सपोजर वाढवण्यासाठी आणि ग्राहकांपर्यंत पोहोचण्यास मदत करण्यासाठी वापरकर्ते त्यांच्या सोशल नेटवर्कसह सामायिक करतील अशी सामग्री तयार करणे हे सोशल मीडिया मार्केटिंग SMM चे ध्येय आहे.

आधुनिक काळातील व्यवसायांना सोशल मीडियाचा फायदा होत आहे कारण ते जाहिरातींसाठी एक उत्तम व्यासपीठ देते, हे उत्पादन किंवा त्यांच्या सेवांबद्दल ग्राहक पुनरावलोकनाचे विश्लेषण करण्यासाठी व्यवसायाला मदत करणाऱ्या ग्राहकांशी संपर्क साधण्यास देखील अनुमती देते.

सोशल मीडिया मार्केटिंग खूप उपयुक्त बाजार माहिती प्रदान करते. हे वापरकर्त्यांना देखील फायदेशीर ठरते कारण ते नवीन उत्पादन, नवीन सेवा, नवीन तंत्रज्ञान याबद्दल अद्यतनित होण्यास मदत करते आणि अशा प्रकारे त्यांना अधिक चांगले पर्याय निवडण्याचे स्वातंत्र्य देते. सर्व प्रकारचे व्यवसाय लहान किंवा मोठे हवामान देखील सोशल नेटवर्कचा वापर कम्युनिकेशन चॅनेल म्हणून करतात. कंपन्या त्यांच्या ग्राहकांशी थेट संवाद साधण्यासाठी फेसबुक, ट्विटर आणि लिंक्डइन हे प्रमुख व्यासपीठ म्हणून वापरतात. थिंक डिजिटलचे जस्टिन वाईज आणि सॅमसंगचे डॉ. ओह-ह्यून क्वॉन सारखे उद्योजक सोशल मीडियावर खूप सक्रिय असतात आणि नियमितपणे पोस्ट करतात. हे त्यांच्या ग्राहकांना संवाद साधण्यास आणि उत्पादनाबद्दल अधिक सूचना आणि पुनरावलोकने देण्यासाठी प्रोत्साहित करतात.

सोशल मीडिया मार्केटिगवर सायबर क्राईमचा प्रभाव

यूके मधील शीर्ष 150 वरिष्ठ विपणन अधिकारी IDM येथे भेटले (इन्स्टिट्यूट ऑफ डायरेक्ट मार्केटिंग ही युरोपमधील आघाडीची संस्था आहे प्रत्यक्ष, डेटा आणि डिजिटल मार्केटिंगचा व्यावसायिक विकास)सोशल मीडियाला संधी ऐवजी जोखीम मानतात. वेबसाइटद्वारे सोशल मीडियावर केलेले SWOT विश्लेषण त्याच्या धोक्यांची नोंद करते:

- तुमचे स्थान उघड करा
- तुमची ओळख चोरीला जाणे
- ऑनलाइन मार्केटिंगचा मंद वाढीचा दर
- कमकुवत व्यवसाय मॉडेल
- नकारात्मक टिप्पण्या मिळवणे 8

सोशल मीडिया मनोरंजक आणि मोहक दिसतो कारण प्रत्येकाला लोकप्रियता हवी असते. आजकाल फक्त एका क्लिकवर प्रसिद्धी मिळवणे खूप सोपे आहे, परंतु जे काही चमकते ते सोने नसते. सोशल मीडिया मार्केटिंगद्वारे जाहिरात आणि नफा मिळवणे सोपे आहे परंतु त्याचे स्वतःचे धोके आहेत.

सोशल मीडिया अस्पष्टता प्रदान करतो ज्याने मोठ्या प्रमाणात गर्दी आकर्षित केली आहे आणि अशा प्रकारे जगभरातील मोठ्या प्रमाणात लोक त्याचा वापर करत आहेत ज्यामुळे बनावट आणि फसव्या जाहिराती, गुंतवणूक आणि कर्ज मिळविण्याची आश्वासने किंवा बनावट किंवा बनावट सिक्युरिटीजचा व्यापार. अविश्वसनीयपणे जास्त नफा मिळवून देण्याचे आश्वासन देऊन अशा बनावट आणि फसव्या योजनांमध्ये गुंतवणूकदारांना त्यांचा पैसा लावला जातो.

माहिती तंत्रज्ञान कायदा, 2000: उदय आणि त्याची गरज

माहिती तंत्रज्ञान कायदा, 2000: उदय आणि त्याची गरज नवीन नेटवर्किंग प्रोटोकॉल आणि डिजिटल तंत्रज्ञानाची निर्मिती, डेटाचे पारंपारिक पद्धतीने कागदी दस्तऐवजीकरण बाजूला ठेवून इलेक्ट्रिक, पोर्टेबल डेटा फॉरमॅटमध्ये डेटा ट्रान्समिटन्स आणि स्टोरेजद्वारे लोकांचा व्यवसाय करण्याच्या पद्धतीमध्ये लक्षणीय बदल झाला आहे. परंतु इलेक्ट्रॉनिक स्वरूपातील माहिती असुरक्षित आहे आणि त्यात अनेक गोपनीयता आणि सुरक्षिततेच्या समस्या आहेत परंतु सायबर गुन्ह्यांपासून सुरक्षित राहण्यासाठी स्वस्त आणि स्टोरेज आणि दळणवळण सुलभतेच्या फायद्यांमुळे ती मोठ्या प्रमाणावर वापरली जाते आणि त्यामागील कारण नसणे हे देखील पाहिले जाणे ही एक मोठी जबाबदारी आहे.

माहिती तंत्रज्ञान कायदा, 2000 आणि सोशल मीडिया

सर्वसाधारणपणे, माहिती तंत्रज्ञान कायदा, 2000 परंतु कोणत्याही विशिष्ट इलेक्ट्रॉनिक रेकॉर्डच्या संदर्भात "मध्यस्थ" म्हणून कलम 2(w) अंतर्गत वर्णन केलेल्या शब्दात सोशल मीडियाचे काही भाग, म्हणजे कोणतीही व्यक्ती जी दुसऱ्या व्यक्तीच्या वतीने रेकॉर्ड प्राप्त करते, संग्रहित करते किंवा प्रसारित करते किंवा त्या रेकॉर्डच्या संदर्भात कोणतीही सेवा प्रदान करते आणि त्यामध्ये टेलिकॉम सेवा प्रदाता, नेटवर्क सेवा प्रदाते, ऑनलाइन पेमेंट सेवा प्रदाते, ऑनलाइन वेब सेवा प्रदाते, वेब सेवा प्रदाते, इंटरनेट सेवा प्रदाते. साइट्स, ऑनलाइन बाजार ठिकाणे आणि सायबर कॅफे. या व्याख्येच्या क्षमतेमध्ये सरकारने फेसबुक, ट्विटर, लिंक्डइन, इन्स्टाग्राम इत्यादी सोशल मीडिया वेबसाइट्सचा या कायद्याच्या तरतुदीनुसार समावेश केला आहे. माहितीपर तंत्रज्ञान सुधारणा कायदा, 2008 मध्ये लागू करण्यात आलेल्या इतर तरतुदींमध्ये सोशल मीडियाद्वारे होणारे गुन्हे देखील समाविष्ट आहेत.

साहित्य समीक्षा

(कुमार, 2016) उद्धृत करतात की इंटरनेटच्या आगमनाने आणि सोशल मीडिया प्लॅटफॉर्मच्या व्यापक वापरामुळे लोकांच्या संप्रेषणाच्या, माहितीची देवाणघेवाण आणि व्यवसाय चालवण्याच्या पद्धतीत बदल झाला आहे. परिणामी, सायबर गुन्हेगारांसाठी सायबर गुन्ह्यांसह त्यांचे बेकायदेशीर क्रियाकलाप करण्यासाठी सोशल मीडिया हे आवश्यक साधन बनले आहे.

(Koops, 2012) नुसार, सायबर क्राईम म्हणजे गुन्हेगारी क्रियाकलापांचा संदर्भ आहे ज्या डिजिटल नेटवर्कद्वारे आयोजित केल्या जातात किंवा संगणक तंत्रज्ञानाचा वापर करतात. भारतातील सायबर गुन्ह्यांच्या प्रसारामध्ये सोशल मीडियाची भूमिका अनेक अभ्यासांनी अधोरेखित केली आहे. या अभ्यासातून असे दिसून आले आहे की फेसबुक, ट्विटर आणि व्हॉट्सॲप सारख्या सोशल मीडिया प्लॅटफॉर्मचा वापर सायबर गुन्हेगारांकडून संशयास्पद व्यक्ती आणि संस्थांना लक्ष्य करण्यासाठी केला जातो. ते असुरक्षिततेचा फायदा घेण्यासाठी आणि वैयक्तिक माहिती आणि आर्थिक संसाधनांमध्ये अनधिकृत प्रवेश मिळविण्यासाठी फिशिंग, मालवेअर वितरण आणि ओळख चोरी यासारख्या विविध युक्त्या वापरतात.

(सिंग, 2015) सोशल मीडियावरील सायबर गुन्हे कमी करण्यासाठी खालील पावले सुचवतात:

1] पासवर्ड नियमितपणे अपडेट करा: बरेच सोशल मीडिया आणि ईमेल वापरकर्ते सोयीसाठी सोपे पासवर्ड पसंत करतात, परंतु ते नियमितपणे बदलल्याने इंटरनेट गुन्ह्यांचा धोका लक्षणीयरीत्या कमी होऊ शकतो. सर्व प्रकारच्या खात्यांसाठी केवळ अक्षरेच नव्हे तर संख्या आणि विशेष वर्णांचा समावेश असलेले जटिल पासवर्ड वापरावेत. तसेच, वैयक्तिक डेटा अधिक सुरक्षित करण्यासाठी गुप्त प्रश्न सुविधेमध्ये आव्हानात्मक उत्तर असावे.

2] घराचा पत्ता उघड करणे टाळा: विशेषत: स्त्रियांसाठी, विशेषत: प्रमुख व्यावसायिक भूमिकांशी संबंधित, घराचा पत्ता उघड करण्यापासून परावृत्त करण्याची प्रथा आहे. त्याऐवजी, कामाचा पत्ता किंवा भाड्याने दिलेला खाजगी मेलबॉक्स निवडणे सोशल मीडियामधील स्टॉलर्सना रोखण्यात मदत करू शकते. शिवाय, ऑनलाइन अपलोड केलेली वैयक्तिक माहिती कमी केल्याने अनधिकृत व्यक्तींना सहज प्रवेश करणे टाळता येते

3] मर्यादित सामाजिक मंडळे टिकवून ठेवा: मोठ्या सोशल मीडियाचे अनुसरण करण्याचे आकर्षण मोहक असले तरी, एखाद्याचे कनेक्शन आटोपशीर संख्येपर्यंत मर्यादित करणे उचित आहे, आदर्शतः सुमारे 150 व्यक्ती ज्यांच्याशी अस्सल सामाजिक नातेसंबंध जपता येतील. हा सराव खात्री देतो की वैयक्तिक माहिती केवळ ज्यांना खरोखर माहित आहे त्यांच्याशी शेअर केली जाते, अज्ञात घटकांशी संपर्क कमी करते.

4] जागरुकता मोहिमा चालवा: शाळा आणि महाविद्यालयांपासून सुरू होणाऱ्या तळागाळातील जागरुकता मोहिमा, विविध सायबर गुन्ह्यांबद्दल जसे की, स्टकिंग, फसवणूक, बदनामी आणि सायबर छळवणूक यांबद्दल लोकांना शिक्षित करण्यासाठी आवश्यक

आहेत. हे उपक्रम ऑनलाइन धोके ओळखण्यासाठी आणि त्यांचा प्रभावीपणे सामना करण्यासाठी आवश्यक ज्ञान असलेल्या लोकांना सक्षम बनवतात.

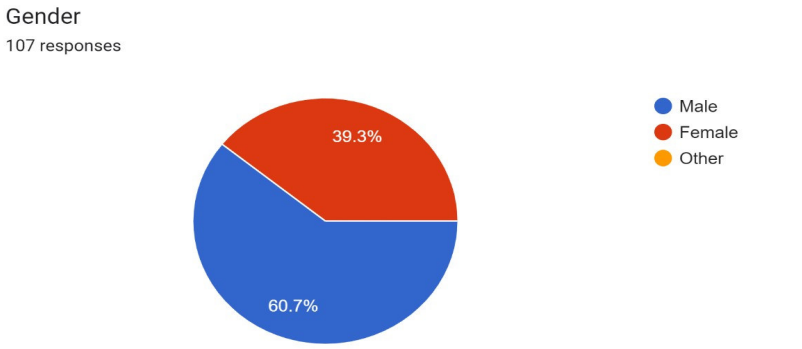
5] अवांछित संप्रेषणांपासून संरक्षण: महिलांनी अवांछित फोन कॉल्स आणि संदेशांबाबत सावधगिरी बाळगली पाहिजे, कारण ते संभाव्यतः देखरेखीच्या हेतूंसाठी वापरले जाऊ शकतात. सततच्या छळाचे दस्तऐवजीकरण केले जावे, फोन कॉल रेकॉर्ड करून अधिकाऱ्यांना कळवावे. विश्वसनीय स्त्रोतांकडून अनुप्रयोग डाउनलोड करणे आणि विश्वासार्ह व्यक्तींना गोपनीय ठेवणे देखील अतिरिक्त समर्थन प्रदान करू शकते.

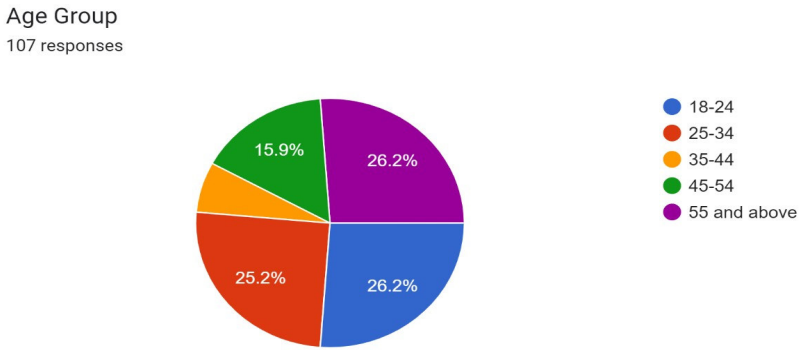
6] गोपनीयता सेटिंग्ज समजून घ्या: गोपनीयता धोरणे आणि सोशल नेटवर्क्स आणि ऑनलाइन प्लॅटफॉर्मच्या सेटिंग्जसह स्वतःला परिचित करणे महत्त्वाचे आहे. योग्य गोपनीयता सेटिंग्जचा अवलंब करून, व्यक्ती त्यांच्या जोखमींशी संपर्क कमी करू शकतात आणि संभाव्य ऑनलाइन हानीपासून स्वतःचे संरक्षण करू शकतात.

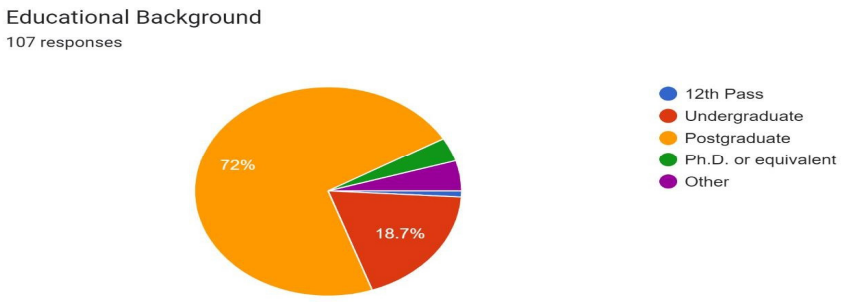
7] नियमितपणे खात्यांचे निरीक्षण करा: नियमितपणे ईमेल, ब्लॉग आणि वेबसाइट खाती तपासणे व्यक्तींना त्यांच्या ऑनलाइन क्रियाकलापांबद्दल माहिती ठेवण्यास मदत करते आणि हॅकिंग किंवा स्टॅकिंगच्या घटनांची शक्यता कमी करते. खात्यांचे निरीक्षण करण्याकडे दुर्लक्ष केल्याने जागृत राहण्याच्या महत्त्वावर जोर देऊन, व्यक्ती शोषणास बळी पडू शकतात.

भारतातील सायबर गुन्ह्यांच्या गुंतागुंतीचे निराकरण करण्यासाठी सरकारी संस्था, कायदा अंमलबजावणी संस्था, व्यवसाय आणि व्यक्ती यांच्याकडून एकत्रित प्रयत्न करणे आवश्यक आहे. राष्ट्रीय आणि वैयक्तिक अशा दोन्ही स्तरांवर सायबरसुरक्षेला प्राधान्य देऊन, भारत सायबर गुन्ह्यांमुळे निर्माण होणारे धोके प्रभावीपणे कमी करू शकतो आणि नागरिकांसाठी अधिक सुरक्षित डिजिटल वातावरण तयार करू शकतो.

लोकसंख्याशास्त्रीय विश्लेषण







एका सर्वेक्षणा अंतर्गत वयोगटानुसार केलेल्या विश्लेषणाने सायबर गुन्ह्यांचे वेगळे नमुने उघड केले. 55 आणि त्यावरील वयोगटातील 26.3%आणि 25 ते 34 या वयोगटांमध्ये 26.2% सर्वाधिक घटना दर दिसून आला, प्रत्येक गटात एकूण प्रकरणांपैकी 24.3% समावेश आहे. उल्लेखनीय म्हणजे, 18-24 या वयोगटातील 22.2% प्रकरणे आहेत, जे दर्शविते की सायबर गुन्ह्यांमुळे विविध वयोगटातील लोकसंख्येवर परिणाम होतो. याउलट, 35 ते 44 वयोगटातील सर्वात कमी घटना दर 9.4% दर्शविला. हे निष्कर्ष सूचित करतात की सर्व वयोगटातील व्यक्ती सायबर धोक्यांना संवेदनाक्षम असतात, तरुण आणि वृद्ध लोकसंख्या विशेषतः असुरक्षित असतात. लिंग-आधारित विश्लेषणातून असे दिसून आले की सायबर गुन्ह्यांमध्ये 39.3% पीडित महिला होत्या, तर बहुसंख्य, 60.7% पुरुष होते. हे वितरण सायबर गुन्ह्यांमध्ये संभाव्य लिंग असमानतेवर प्रकाश टाकते, या घटनेला कारणीभूत असलेल्या अंतर्निहित घटकांच्या पुढील तपासाची हमी देते.

बौद्धिक संपदा हक्क

"एखाद्या व्यक्तीला किंवा एखाद्या कंपनीला त्याच्या स्वत: च्या योजना, कल्पना किंवा इतर अमूर्त मालमत्तांचा वापर करण्याचा अधिकार आहे, किमान विशिष्ट कालावधीसाठी या अधिकारांमध्ये प्रताधिकार, पेटंट, ट्रेडमार्क आणि व्यापार रहस्ये यांचा समावेश असू शकतो कल्पना चोरेल आणि/किंवा त्याचे श्रेय घेईल."१०

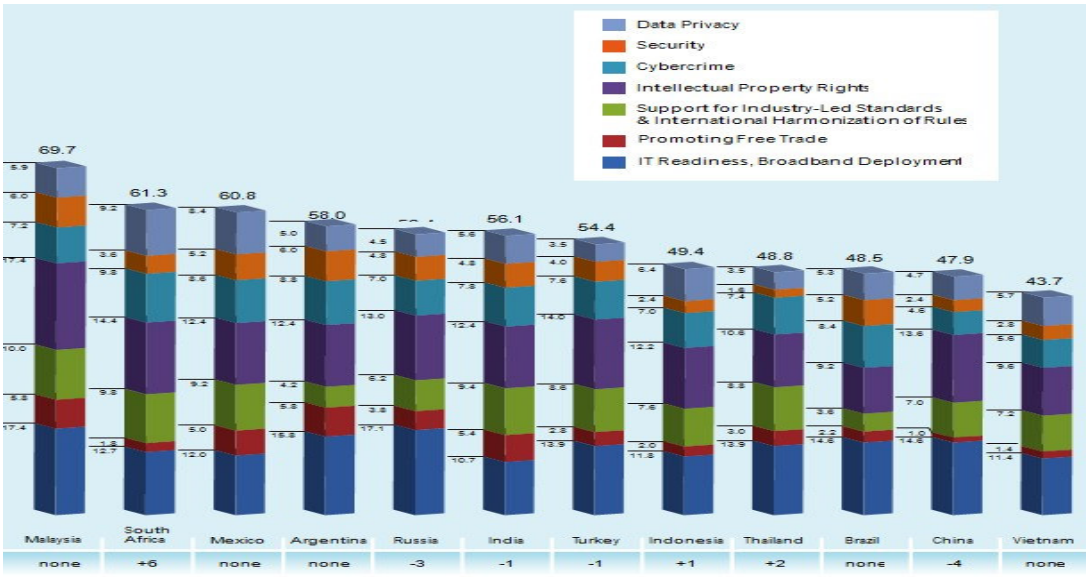
प्रतिसादकर्ता इंटरनेट आणि सोशल मीडिया मार्केटिंग व्यवसायात गुंतलेला असला तरी, दुसऱ्या पक्षाच्या ट्रेडमार्कचा गैरफायदा घेणाऱ्या भ्रामक डोमेन नावाचा वापर तक्रारीच्या दुसऱ्या घटकाच्या उद्देशाने "वस्तू किंवा सेवांच्या प्रामाणिक ऑफरच्या संदर्भात" वापर मानला जाऊ नये. 11

इंटरनेट सेवा प्रदाते संबंधित वेळेचे रेकॉर्ड जतन करण्यात अयशस्वी ठरतात या अपयशामुळे सायबर गुन्ह्यांतील अनेक सायबर गुन्ह्यांचे निराकरण न झालेले कलम 67 सी ही दुरुस्ती आता सायबर गुन्ह्यांच्या प्रकरणांमध्ये फायदेशीर ठरत आहे. या कलमानुसार केंद्र सरकारने मध्यस्थांना विहित नमुन्यात दिलेल्या कालावधीसाठी असा महत्त्वाचा डेटा जतन करणे आणि टिकवून ठेवणे बंधनकारक केले आहे. जर मध्यस्थ या निकषांचे आणि तरतुदींचे पालन करत नसेल तर ते दोन वर्षांपेक्षा जास्त नसलेल्या मुदतीसाठी तुरुंगवासासाठी दोषी ठरतील किंवा ते 1 अभाव किंवा दोन्हीच्या समान 5 पेक्षा जास्त आकारू शकतात.

2008 कलम 69B च्या दुरुस्तीनंतर, केंद्र सरकारला कोणतीही एजन्सी नियुक्त करण्याचा अधिकार देते आणि त्यावर लक्ष ठेवण्यासाठी आणि तयार केलेल्या, प्राप्त झालेल्या किंवा जतन केलेल्या गर्दीच्या डेटाचे आयोजन करण्यासाठी 11 2014 SCC ऑनलाइन WIPO 506 Beach Body, LLC v. Cornel Ungureanu /Cyberland LLC World Intellectual Property Organization WIPO, केस क्रमांक D2014-0361. त्याची सायबर सुरक्षा राखण्यासाठी आणि वाढविण्यासाठी संगणक संसाधने आणि मध्यस्थाला नियुक्त एजन्सीशी सहकार्य करण्यास बांधील बनवते आणि असे होत नसल्यास संबंधित मध्यस्थ 3 वर्षांपर्यंतचा कारावास आणि दंड किंवा दोन्ही अशी शिक्षा होऊ शकते.

सुधारणांपूर्वी IT कायदा, 2000 चे कलम नेटवर्क सेवा प्रदात्यांना तृतीय पक्ष सामग्रीसाठी जबाबदार बनवते जेव्हा ते हे सिद्ध करण्यात अयशस्वी ठरतात की गुन्हा त्यांच्या नकळत केला गेला आहे किंवा त्यांनी असे गुन्हे घडू नयेत यासाठी योग्य ती दक्षता घेतली आहे.

सायबर गुन्ह्यांपासून लढण्यासाठी भारत स्वतःमध्ये सुधारणा करत आहे=भारत - स्कोअर: 56.1 - 2012 पासून स्कोअर: +6.11 | रँक: +1



भारत एक महत्त्वाची प्रादेशिक अर्थव्यवस्था आहे, ज्याला आयसीटी सेवांच्या विकासामध्ये तीव्र रस आहे. भारतातील कायद्याने क्लाउड कंप्युटिंगमधील घडामोडींना पूर्णपणे गती दिली नाही आणि संरक्षणाच्या प्रमुख क्षेत्रांमध्ये काही अंतर आहे; विशेष म्हणजे, भारताने अद्याप प्रभावी गोपनीयता कायदा लागू केलेला नाही.

भारताच्या सायबर क्राइम कायद्याला आंतरराष्ट्रीय मॉडेल्सशी सुसंगत होण्यासाठी अपडेट करणे देखील आवश्यक आहे. भारतातील काही कायदे आणि मानके तंत्रज्ञान तटस्थ नाहीत (उदा., इलेक्ट्रॉनिक स्वाक्षरी), आणि हे इंटरऑपरेबिलिटीमध्ये अडथळा असू शकतात.

तथापि, 2012 मध्ये, भारताने शेवटी आपले कॉपीराइट कायदे आधुनिक कॉपीराइट समस्या जसे की अधिकार व्यवस्थापन माहिती आणि तांत्रिक संरक्षण उपाय समाविष्ट करण्यासाठी अद्यतनित केले. ब्रॉडबँड आणि वैयक्तिक संगणक प्रवेशाच्या कमी पातळीसह भारताच्या तंत्रज्ञान क्षेत्रांचा विकास अजूनही आव्हानात्मक आहे. एकूणच, 2016 च्या स्कोअरकार्डमध्ये भारताचे रँकिंग एका स्थानाने सुधारले आहे. 19 व्या ते 18 व्या अद्ययावत बौद्धिक संपदा कायद्यांच्या आधारे आणि पायाभूत सुविधांमध्ये केलेल्या सुधारणांवर आधारित आहे.

शिफारशी

- सामान्य सायबर धोके ओळखणे आणि कमी करणे यावर लक्ष केंद्रित करून सर्व वयोगटातील व्यक्तींना लक्ष्य करणारे सायबर सुरक्षा शिक्षण आणि जागरूकता कार्यक्रम मजबूत करणे.
- सायबर गुन्ह्यांचा प्रभावीपणे मुकाबला करण्यासाठी सरकारी संस्था, कायद्याची अंमलबजावणी आणि खाजगी क्षेत्रातील भागधारक यांच्यातील सहकार्य वाढवणे.
- वैयक्तिक आणि आर्थिक माहितीचे रक्षण करण्यासाठी बहु-घटक प्रमाणीकरण आणि एन्क्रिप्शन यासारखे मजबूत ओळख संरक्षण उपाय लागू करणे.
- नियमित सॉफ्टवेअर अपडेट, सुरक्षित पासवर्ड व्यवस्थापन आणि सावध ऑनलाइन वर्तन यासारख्या सायबरसुरक्षा सर्वोत्तम पद्धतींचा अवलंब करण्यास प्रोत्साहित करणे.

• कर्मचारी प्रशिक्षण, घटना प्रतिसाद नियोजन आणि नियमित सुरक्षा मूल्यांकनांद्वारे संस्थांमध्ये सायबर सुरक्षा लवचिकतेची संस्कृती वाढवणे.

या शिफारशींची अंमलबजावणी करून आणि सायबर सुरक्षेसाठी सक्रिय दृष्टिकोन वाढवून, व्यक्ती आणि संस्था सायबर धोक्यांपासून अधिक चांगल्या प्रकारे बचाव करू शकतात आणि संपूर्ण समाजावर सायबर गुन्ह्यांचा प्रभाव कमी करू शकतात.

निष्कर्ष

सोशल मीडियाच्या माध्यमातून 21व्या शतकात सुपरहायवेचा वापर हा एक वरदान आणि त्रासदायक दोन्ही प्रकार आहे जो सर्व काही तो कोणत्या मार्गाने वापरला जातो यावर अवलंबून आहे. विक्रेता आणि खरेदीदार यांच्यातील संबंध एकदम बदलले आहेत जेथे विक्रेते यापुढे गवत शोधत असलेल्या मेंढ्या नाहीत तर ते थेट त्यांच्या ग्राहकांवर शिकार करणारे शिकारी बनले आहेत. ते सहजपणे विश्वास संपादन करतात आणि ग्राहकांना त्यांचे इच्छित दर्जेदार उत्पादन प्रदान करतात परंतु म्हटल्याप्रमाणे. परंतु असे म्हंटले जात आहे की, प्रत्येक संस्था किंवा गट, समुदाय इत्यादीची एक काळी बाजू आहे. त्यामुळे सोशल मीडिया मार्केटच्या सकारात्मक घडामोडींचे नियमन करण्यासाठी आणि वापरकर्त्यांचे हित जपण्यासाठी काही कायद्यांची अंमलबजावणी करणे आवश्यक आहे कारण कायदा देणाऱ्यांच्या हेतूने शांतता आणि आनंदी जीवन जगणे आणि वाईट विचार करणाऱ्यांना शिक्षा हे अशा कायद्यांच्या अंमलबजावणीचे परिणाम आहेत. सायबर स्पेस अधिक सुरक्षित करण्यासाठी, खालील धोरणांचे पालन करणे आवश्यक आहे:

• एक सर्वसामान्य सुरक्षित सायबर इको-सिस्टम तयार करणे.

• माहिती तंत्रज्ञानासाठी योग्य अशी यंत्रणा निर्माण करणे.

. गुन्हेगारी सुरक्षा यंत्रणा निर्माण करणे.

• माहितीच्या पायाभूत सुविधांचे संरक्षण करणे.

• खुल्या मानकांचा उठाव करणे.

• सायबर गुन्ह्यांचा विचार करून कायद्यांच्या अंमलबजावणीत सुधारणा करणे.

References

1. As substituted by the Information Technology (Amendment) Act, 2008 (10 of 2009), section 4(H), for clause (w). [10]
2. Bamrara, Dr Atul. "The Challenge of Cyber Crime in India: The Role of Government." Pakistan Journal of Criminology 3.3 (2012): 127-134.
3. Debdutta Mitra 2024, proliferation of cybercrime via social media, international journal of novel research and development 71-93
4. Gupta Dhurv 2016ncyber crime and social media, Bharti law review 244-256
5. https://data.gov.in (Government of India initiative under digital India movement).
6. Koops, Bert-Jaap. "Criminal law and Cyberspace as a Challenge for Legal Research." SCRIPTed 9 (2012): 354.
7. Kumar, PN Vijaya. "Growing cybercrimes in India: A survey." 2016 International Conference on Data Mining and Advanced Computing (SAPIENCE). IEEE, 2016.
8. Nagarwal, Narender. "Social Media Crime in Digital World-A Critique through Law, Policy and Practice." Indian JL & Just. 10 (2019): 34.
9. Obar, J.A. and Wildman, S. (2015). Social media definition and the governance challenge: An introduction to the special issue. Tele Communications Policy, 39(9), 745-750.
10. Pew Research Center Surveys, 2005-2006, 2008-2015.
11. Report-Global Cloud Computing Scorecard (2013).
12. R.P. Kataria & S.K.P. Srinivasan, Cyber Crimes Law, Practice & Procedure along with Cyber Evidence and Information Technology Act, 2000 with Allied Rules (New ed. 2014).

13. Singh, Jaspreet. "Violence against women in cyber world: a special reference to India." International Journal of Advanced Research in Management and Social Sciences 4.1 (2015): 60-76.
14. Student, New Law College, Bharati Vidyapeeth Deemed University, Pune.1
15. www.whatis.techtarget.com. [6]
16. www.cio.com.
17. www.jeffbullas.com. [8]
18. www.adweek.com.
19. www.businessdictionary.com.
20. Varma, Dr TN, and D. A. Khan. "Curbing Cyber Crimes by Indian Law." Available at SSRN 2922365 (2017).