Gurukul International Multidisciplinary Research Journal (GIMRJ)*with*
International Impact Factor 8.357
Peer Reviewed Journal
DOI link - https://doi.org/10.69758/GIMRJ/2503I3IIVXIIIP0060

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

वाढता इ कॉमर्स आणि सायबर सुरक्षितता

डॉ. रामेश्वर एस. व्हंडकर
सहा. प्राध्यापक
कुंभलकर कॉलेज ऑफ सोशल वर्क, वर्धा
Mob. 9021204340
Email: - ram.hondkar@gmail.com

प्रस्तावना . दैनंदिन जीवनात वाढत्या इंटरनेटच्या वापरामुळे ऑनलाईन कार्यात वाढ झाल्यामुळे सायबर गुन्हे मोठ्या प्रमाणात वाढले आहे. इंटरनेटच्या माध्यमातून सोशल नेटवर्किंगच्या साह्याने अनेक लोक एकमेकांशी प्रत्यक्ष अपरिचित असूनही विविध ॲप द्वारे एकमेकांशी कनेक्टेड असतात. त्यामुळेच आपण नेहमी बोलत असतो की हे जग हे वैश्विक खेडे झाले आहे कारण जगातल्या कानाकोपऱ्यातील माहिती, फोटोज किंवा संवाद बसल्याठिकाणी आपण पाहू शकतो ऐकू शकतो पाठवू शकतो अगदी काही क्षणात तेथील संवाद आपल्यापर्यंत व आपला संवाद त्यांच्यापर्यंत पोहोचवणे अगदी सोपे झाले आहे. या धर्तीवरच अनेक कंपन्यांनी आपला व्यवसाय सुद्धा इंटरनेटच्या साह्याने विविध वेबसाईट विविध सोशल अकाउंट्स तसेच वैयक्तिक ॲप द्वारे ई–कॉमर्स मोठ्या प्रमाणात केला जात आहे. ई–कॉमर्स मुळे विक्रेता व उपभोक्ता या दोघांचाही वेळ, श्रम व पैसा वाचतो त्यामुळे ग्राहक व विक्रेता दोघेही ई–कॉमर्सला प्राधान्य देतात.

सध्या परिस्थितीत पाहिले असता असे आढळते की अगदी खेडोपाड्यापर्यंत ई-कॉमर्सद्वारे सेवा पुरवल्या जातात अनेक व्यक्तींना सोशल नेटवर्किंग द्वारे ई–कॉमर्समध्ये आकर्षिले जाते आणि अगदी कमी शिक्षित किंवा निरक्षर व्यक्ती सुद्धा याचा उपभोग घेत असल्याचे सर्वत्र पाहावयास मिळते आहे. बऱ्याच अंशी ई–कॉमर्स ग्राहकांना तसेच उपभोक्त्यांसाठी फायद्याची ठरत आहे परंतु त्याचा उपयोग करत असताना आवश्यक ती काळजी जर घेतली नाही तर त्यापासूनमोठ्या प्रमाणात हानी सुद्धा ग्राहकाची होत असल्याचे आपल्याला पाहायला मिळत आहे. हे होणारे नुकसान टाळण्याकरिता नागरिकांमध्ये सायबर साक्षरता खूप महत्त्वाची असल्याचे आढळते. दैनंदिन घडत असलेल्या वेगवेगळ्या सायबर गुन्ह्यांचे प्रमाण समजून घेऊन सायबर गुन्हेगारांच्या नवनवीन युक्त्या तात्काळ आपल्याला समजणे आवश्यक आहे. याकरिता ग्राहकांनी कोणत्या गोष्टीची काळजी घेणे आवश्यक आहे. याचे संशोधकांनी अध्ययन करून सदर संशोधन पेपर सादर केला आहे. सायबर गुन्हेगारांचे प्रमाण दिवसेंदिवस वाढत आहे आणि ते टाळण्यासाठी सायबर सुरक्षिततेचे महत्त्व सर्वसामान्यांपर्यंत पोहोचवणे आवश्यक वाटते.

सायबर सुरक्षितता म्हणजे काय:– सायबर सुरक्षा लक्षात घेत असताना इंटरनेट कनेक्टेड व्यवस्थेतून होणारे अपहरण चोरी म्हणजे सायबर गुन्हेगारी होय सायबर गुन्हेगारी हार्डवेअर सॉफ्टवेअर आणि डेटा यांच्या साह्याने होते. सायबरसुरक्षा म्हणजे संगणक सर्व्हर] मोबाईल उपकरणे] इलेक्ट्रॉनिक प्रणाली] नेटवर्क आणि दुर्भावनापूर्ण हल्ल्यांपासून डेटाचे रक्षण करणे होय. याला माहिती तंत्रज्ञान **सुरक्षा** किंवा इलेक्ट्रॉनिक माहिती **सुरक्षा** म्हणून सुद्धा ओळखले जाते.

सायबर गुन्ह्यांचे प्रकार:–

दिवसेंदिवस सायबर गुन्हे वाढतच असल्याचे दिसत आहे. एकूण सायबर गुन्ह्यांपैकी महिलांचे सायबर गुन्ह्यांचे प्रमाण खूप अधिक असल्याचे आढळून येते.

- **ई–मेल द्वारे फसवणे:– मागील काही वर्षात पत्र व्यवहार मोठ्या प्रमाणात केला जात होता परंतु त्याची जागा आता आपण पाहतोय की ई–मेलने घेतलेली आहे आणि तात्काळ**

Gurukul International Multidisciplinary Research Journal (GIMRJ)*with* International Impact Factor 8.357
Peer Reviewed Journal
DOI link - https://doi.org/10.69758/GIMRJ/2503I3IIVXIIIP0060

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

आपला संदेश समोरच्या व्यक्ती पर्यंत पोहोचवला जातो परंतु यामध्येही सायबर गुन्हे घडत असल्याचे निदर्शनास येते. यामध्ये ब्लॅकमेल करणे] धमकावणे] फसवणूक करणे] हॅक करणे] चुकीचे मेल पाठवणे अशा प्रकारचे सायबर गुन्हे घडत असतात. या प्रकारास महिला अधिक प्रमाणात बळी पडतात.

- सायबर बदनामी:– महिलांना मोठ्या प्रमाणात फसवणूक करून त्यांचे इमेजेस मोडतोड करून त्यांची बदनामी करण्याचा सुद्धा प्रकार मोठ्या प्रमाणात घडत असल्याचे आढळून येते. तसेच त्यांना विविध लिंक असणाऱ्या ईमेल पाठवून विडंबन / टवाळकी केल्याचेसुद्धा मोठ्या प्रमाणात दिसून येते.
- आधुनिक गुन्ह्यांमध्ये सायबर पोर्नोग्राफी:–आधुनिक गुन्ह्यांमध्ये सायबर पोर्नोग्राफी याचाही मोठ्या प्रमाणात वापर केला जातो तंत्रज्ञानाच्या द्वारेसोशल नेटवर्किंग मधल्या फोटोग्राफी कलेक्ट करून त्यात बदल करून पोर्नोग्राफी बनवली जाते व त्यावर धमकावून पैसे मागणे किंवा आवश्यक ती मागणी केल्या जाते या ही बाबत महिला अधिक प्रमाणात बळी पडतात.
- इंटरनेट व मोबाईलचा वाढता वापर:– सध्या परिस्थितीत इंटरनेट व मोबाईलचा वापर वाढल्यामुळे ई–कॉमर्स सुद्धा मोठ्या प्रमाणात वाढले आहे त्याचाच गैरफायदा घेऊन सायबर गुन्हेगार ग्राहकांना मोठ्या प्रमाणात फसवताना आढळून येतात. त्यामुळे सायबर सुरक्षित राहणे खूप आवश्यक झाले आहे. त्याला बळी पडण्याचे मुख्य कारण म्हणजे नागरिकांना काही गोष्टी सोप्या किंवा कमी किमतीत किंवा मोफत मिळत आहे अशा मेसेज किंवा फोनद्वारे जाळ्यात घेतल्या जाते व त्याला अनेक व्यक्ती बळी पडून आपली फसवणूक करून घेतात.
- फिशिंग:– फिशिंग यामध्ये सायबर गुन्हेगार व्हाट्सअप द्वारे किंवा मेल द्वारे लिंक पाठवतो आणि ती लिंक ओपन करण्यास ग्राहकांना सांगतो. लिंक ओपन झाल्यानंतर ठराविक काम] माहिती आहे म्हणून सांगून त्यात तुम्हाला एवढे एवढेच पैसे] बक्षीस मिळणार आहे असे सांगितले जाते त्याकरिता एवढे रुपये तुम्हाला प्रोसेस / पोस्ट चार्ज किंवा जीएसटी वगैरे म्हणून भरावी लागते असे सांगितले जाते व त्या व्यक्तींना जाळ्यात घेतले जाते. आशा आमिषास बळी पडून ठराविक अमाऊंट सायबर गुन्हेगार पाठवण्यास प्रवृत्त करतात] पैशाच्या] बक्षिसाच्या आशेने अनेक लोक ती अमाऊंट सहज पाठवतात त्याला फिशिंग म्हणतात.
- आयडेंटिटी थेफ्ट:– आयडेंटिटी थेफ्ट या प्रकारच्या सायबर गुन्ह्यांमध्ये एखाद्या व्यक्तीचे नाव] मेल आयडी] व्हाट्सअप अकाउंट वापरून समोरच्या व्यक्तींना फसवल्या जाते. एखाद्या कंपनीकडून आपला डाटा प्राप्त करून त्याद्वारे तुमच्या नावावर कर्जही घेऊ शकतो] गुन्हे करू शकतो] बेकायदेशीर खरेदी करू शकतो या प्रकारे व्यवहार करू शकतो त्यामुळे आपला डाटा देत असताना खात्रीशीर व योग्य ठिकाणी तो देणे आवश्यक आहे. कुठेही कोणत्याही कंपनीकडे आपली वैयक्तिक माहिती देऊ नये.

ई– कॉमर्स म्हणजे काय :-

ई-कॉमर्स म्हणजे उत्पादने सेव ऑनलाइन खरेदी आणि विक्री करण्याची प्रक्रिया होय. ई कॉमर्स म्हणजे इलेक्ट्रॉनिक कॉमर्स यामध्ये ऑनलाइन स्टोअर्स स्मार्टफोन ऑनलाईन मार्केटप्लेस तसेच सोशल मीडिया प्लॅटफॉर्म यांच्या साह्याने डिजिटल डिव्हाइस किंवा प्लॅटफॉर्म वर केलेली सर्व प्रकारची खरेदी आणि विक्री होय.

Gurukul International Multidisciplinary Research Journal (GIMRJ)*with* International Impact Factor 8.357
Peer Reviewed Journal
DOI link - https://doi.org/10.69758/GIMRJ/2503I3IIVXIIIP0060

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

इलेक्ट्रॉनिक वाणिज्याचा मोठा हिस्सा फक्त आभासी किंवा संकेतस्थळावर उपलब्ध असणाऱ्या अशा गोष्टींसाठी वापरला जातो. एखादी महत्त्वाची माहिती जी फक्त ई-पेमेंट केल्यावरच पाहता येते बऱ्याच वेळेला इलेक्ट्रॉनिक वाणिज्यच्या सोबतच वस्तू किंवा सेवा यांची वाहतुकी द्वारे पोहोच ही जोडली गेलेली असते. ऑनलाइन व्यवसाय वृद्धीकरिता प्रत्येक व्यवसायिक ऑनलाईन मार्केटिंग सुद्धा करत असतो त्यासाठी आवश्यक स्कीम्स देत असतो आणि त्याद्वारे ग्राहकांना आकर्षित करत असतो. अशा काही स्कीम्स वास्तविक असतात परंतु याला जोडूनच सायबर गुन्हेगार अनेक स्कीम लागू करून किंवा जोडून ग्राहकांना फसव्या ऑफर्स देत असतात या ऑफर द्वारे ग्राहकांना जाळ्यात घेणे त्यांना अनावश्यक लिंक वर नेणे त्यानंतर त्वरित नॉमिनल चार्ज म्हणून शुल्क आकारणे आणि याद्वारे त्यांची फसवणूक केल्या जाते. यासाठी ग्राहकांनी अशा फसव्या स्कीम ओळखून त्वरित त्यापासून दूर जाणे आवश्यक आहे. तेव्हा आपले होणारे नुकसान टाळले जाऊ शकते. सायबर गुन्हेगार अनेक नवनवीन युक्त्या वापरून ग्राहकांना आकर्षित करतात. ग्राहकांनी त्या युक्त्या वेळोवेळी ओळखणे आवश्यक आहे याकरिता ग्राहकांनी अनावश्यक व मूल्या पेक्षा अधिक कोणीही देणार नाही याची जाण ठेवूनच अशा आफवांण पासून दूर राहणे योग्य आहे. तेव्हा सायबर गुन्हेगारी ऑटोमॅटिक कमी होईल.

वाढते सायबर सुरक्षिततेचे महत्व:– **आधुनिक युगात जगत असताना चालू ट्रेंड्स टाळता येत नाही. जसे की ई–कॉमर्स] ई–लायब्ररी] ई– प्रशासन] ई– शासन यांच्यासह आपणही ग्रेट होऊन त्यात सहभाग घेणे आवश्यक आहे. अन्यथा आपण कालबाह्य ठरू शकतो. हे टाळण्यासाठी तंत्रज्ञानाचा वापर करता येणे तसेच नवनवीन तंत्रज्ञान] उपकरण यांची माहिती असणे हे सुद्धा महत्त्वाचे आहे. तसेच संगणक] मोबाईल] नवनवीन इलेक्ट्रॉनिक प्रणाली] सर्व्हर नेटवर्क आणि डेटा यांच्याद्वारे सायबर गुन्हेगारी घडते. आज आपण आधुनिक युगात असल्यामुळे या तंत्रज्ञानाचा उपयोग प्रत्येक व्यक्तीच्या जीवनात कमी अधिक प्रमाणात होत असतो. दिवसेंदिवस यांचा उपयोग वाढतच जाणार आहे याचा फायदा सायबर गुन्हेगार घेत असून त्याद्वारे वेगवेगळ्या युक्त्या करून उपभोक्त्यांना जाळ्यात घेऊन सायबर हल्ले केले जातात. आपल्या जीवनात काही गोष्टी संवेदनशील असतात त्या गोपनीय माहितीची सुरक्षा व्हावी म्हणून सायबर सुरक्षा असणे फार महत्त्वाचे असते.** सायबर सुरक्षितता म्हणजे आपली वैयक्तिक माहिती कोणी चोरी करणार नाही याची खात्री असते. तसेच कोणीही अनधिकृतपणे आपली साईट वापरू शकत नाही. इंटरनेटवरील धोक्यापासून संरक्षण तसेच उपकरणांची सुरक्षा होते. सायबर सुरक्षा नेटबँकिंगची कामे सुरक्षित पार पाडण्याकरिता आवश्यक आहे. आताच्या जगात आपण सर्व इंटरनेटचा वापर करतो. त्यामुळे सध्याच्या घडीला सायबरसुरक्षा ही प्रत्येकाची गरज आहे. आरोग्यसेवा] छोटे व्यवसाय] सरकारी संस्था] उत्पादन] वित्तीय संस्था] शिक्षण यांनाही आपला डेटा गोपनीय ठेवण्यासाठी सायबरसुरक्षेची गरज लागते. तसेच ती आपला बँकिंग डेटा सुरक्षित ठेवते. बँकिंग डेटा सुरक्षित नसल्यास कोणीही आपल्या खात्यांमधून पैसे काढू शकते.

सायबर सुरक्षितते करीता घ्यावयाची दक्षता:–

- तुमचे सॉफ्टवेअर वेळोवेळी अपडेट करत रहा.
- अँटी–व्हायरस सुरक्षा वापरा
- चांगला मजबूत पासवर्ड ठेवा
- कोणताही असुरक्षित किंवा सार्वजनिक ठिकाणाचा वायफाय वापरू नका
- कोणत्याही अनोळखी मेसेज किंवा लिंकवर क्लिक करू नका
- कोणत्याही अपरिचित साईटवर आपली माहिती शेअर करू नका
- सायबर हल्यास बळी पाडण्याचे मुख्य करण म्हणजे मानवी चूका होय. म्हणूनच कर्मचाऱ्यांना येणाऱ्या धोक्यांना तोंड देण्यासाठी आवश्यक असलेले ज्ञान तुम्ही त्यांना दिले पाहिजे.

- कर्मचारी जागरूकता प्रशिक्षण. कर्मचाऱ्यांना सायबर हल्या पासून वाचवण्याकरिता सुरक्षा धोक्यांचा त्यांच्यावर कसा परिणाम होतो हे दाखवावे
- व्यवसायात एप्लीकेशन ची भूमिका वाढत असताना वेब एप्लीकेशन सुरक्षेवर लक्ष केंद्रित करणे तेवढेच महत्त्वाचे आहे
- नेटवर्क सुरक्षा करणे हे आवश्यक आहे आणि डेटाची उपयुक्तता आणि अखंडता सुरक्षित करण्याची प्रक्रिया सुद्धा आवश्यक आहे. हे नेटवर्क पेनिट्रेशन चाचणी करून साध्य केले जाते जी तुमच्या नेटवर्कमधील भेदयता आणि सुरक्षा समस्यांचे मूल्यांकन करते.
- नेतृत्वाची वचन पद्धतही सायबर लवचिकतेची गुरुकिल्ली आहे. त्याशिवाय प्रभावी प्रक्रिया स्थापित करणे किंवा अमलात आणणे कठीण आहे.
- मजबूत पासवर्ड आणि नियमित पासवर्ड बदलणे यामध्ये उपयुक्त ठरते. येथे मला हे अवश्य सांगावे से वाटते की संशोधनांती हे सिद्ध झाले आहे की अनेक देशात अनेक लोक आपल्या उपकरणास पासवर्ड ठेवत असताना 'पासवर्ड'] '१२३४५६' किंवा 'क्वर्टी' हे पासवर्ड वापरतात . सायबर सुरक्षितता वाढवण्याकरिता स्ट्रॉग पासवर्ड ठेवणे व तो वेळोवेळी पासवर्ड बदलणे खूप महत्वाचे आहे.

सायबर सुरक्षिततेबाबत चेतावणी संदेश ओळखणे:–

1) सिस्टम नेहमीपेक्षा हळू चालत असेल तर
2) अनपेक्षित पॉप–अप विंडोओपन होणे
3) तुम्ही न केलेले पासवर्ड बदल
4) असामान्यपणे जास्त नेटवर्क ट्रॅफिक
5) अक्षम केलेली सुरक्षा साधने किंवा अँटीव्हायरस
6) अनधिकृत प्रोग्राम आपोआप सुरू होतात

या मूलभूत गोष्टी समजून घेतल्याने आणि अंमलात आणल्याने तुमच्या सायबर सुरक्षा धोरणाचा मजबूत पाया तयार होतो. ही मूलभूत गोष्टी अधिक प्रगत सुरक्षा उपायांना समर्थन देतात आणि सामान्य धोक्यांपासून संरक्षण करण्यास मदत करतात. वाढता ई –कॉमर्स आणि सायबर सुरक्षितता लक्षात घेत असताना दिवसेंदिवस वाढता ई – कॉमर्स वाढत जाणार आहे परंतु त्यासोबत सायबर गुन्हेगारी वाढणे अपेक्षित नाही याकरिता आपण सर्वांनी एकत्रित येऊन योग्य अयोग्य काय याची जाण ठेवून जर व्यवहार केला तर नक्कीच सायबर गुन्हेगारी आटोक्यात येईल आणि अशा गुन्हेगारांना चाप बसेल याकरिता आपणास योग्य अयोग्य काय हे ओळखता येणे आवश्यक आहे. अनावश्यक कोणीही मोफत काहीही देत नाही याची जाणीव ठेवून अशा स्कीमवर विश्वास ठेऊ नये व अनावश्यक ओटीपी किंवा चार्जेस घेणारे शुल्क अनोळखी व्यक्तीच्या सांगण्यावरून पाठवू नये. तेव्हा सायबर गुन्हेगारी नक्कीच कमी होईल.

संदर्भ:-

सिंह त्रिवेणी,दुबे अमित, 'अदृश्य जाल', (2021) युवान बुक्स पब्लिशर्स.
दुबे अमित, 'सायबर क्राईम' (2025) युवान बुक्स पब्लिशर्स.
जाचक गौरव, 'जयप्रकाश सायबर गुन्हेगारी' (2015) संस्कृती पब्लिकेशन.
द लिटल बुक ऑफ सायबर स्कॅम २.०
https://www.bigcommerce.com/articles/ecommerce/
https://www.buldhanapolice.gov.in/files/Gwork/19.pdf
https://mr.m.wikipedia.org/wiki/%E0%A4%B8%E0%A4%BE%E0%A4%AF%E0%A4%AC%E0%A4%B0_%E0%A4%97%E0%A5%81%E0%A4%A8%E0%A5%8D%E0%A4%B9%E0%A4%BE
https://www.itgovernance.co.uk/what-is-cybersecurity#:~:text=Cyber%20security%20is%20the%20application,systems%2C%20networks%2C%20and%20technologies.