Gurukul International Multidisciplinary Research Journal (GIMRJ)*with* International Impact Factor 8.357
Peer Reviewed Journal
DOI link - https://doi.org/10.69758/GIMRJ/2503I3IIVXIIIP0053

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

सायबर गुन्हे:-एक दृष्टीक्षेप

प्रा. बालाजी गणपत आडे
सहाय्यक प्राध्यापक
मातोश्री अंजनाबाई मुंदाफळे समाजकार्य
महाविद्यालय नरखेड, जि. नागपूर
मो. 8624851841
Email. balajiade.in@gmail.com

प्रस्तावना: -

2024 च्या पहिल्या चार महिन्यांत सायबर गुन्ह्यांची 740,000 हून अधिक प्रकरणे भारतीय सायबर गुन्हे समन्वय केंद्र (I4C) मध्ये नोंदवली गेली. देशातील सायबर गुन्ह्यांच्या संख्येत 2019 आणि 2020 दरम्यान मोठ्या प्रमाणात वाढ झाली आहे आणि तेव्हापासून त्यात वाढ होत आहे. 2024 मधील अंदाजे 85 टक्के अहवाल ऑनलाइन आर्थिक फसवणुकीशी संबंधित होते.

भारत स्वत:ला जगातील आघाडीच्या डिजिटल हबमध्ये बदलण्यासाठी सज्ज झाला आहे. तसेच अधिक कनेक्टिव्हिटी आणि डिजिटल अर्थव्यवस्था मोठ्या प्रमाणात प्रगतीचे आश्वासन देत असताना, ते आमच्या डिजिटल सोसायटींना नवीन असुरक्षिततेसाठी देखील मोकळे सोडताना दिसत आहे. जगातील दुसऱ्या क्रमांकाच्या इंटरनेट लोकसंख्येचे संरक्षण करण्यासाठी भारताने नुकतीच सायबर सुरक्षा फ्रेमवर्क विकसित करण्यास सुरुवात केली आहे. दरम्यान, सायबर गुन्ह्यांना कोणतीही सीमा माहित नाही आणि उदयोन्मुख तंत्रज्ञानाच्या बरोबरीने ते वेगाने विकसित झाले असून सुद्धा सायबर गुन्हे वाढलेले दिसून येतात.

1. सायबर सुरक्षा ही चिंतेची बाब.

आज इंटरनेट, संगणक, स्मार्ट फोन आणि इतर संप्रेषण तंत्रज्ञानाची उपकरणे आपल्या जीवनाचा अविभाज्य भाग बनली आहेत. कल्पना करा, आपण दररोज या स्मार्ट उपकरणांवर किती वेळ घालवतो. आपण गुगल, ईमेल, व्हॉट्सॲप, ट्विटर, फेसबुक इत्यादी इंटरनेट संप्रेषण माध्यमांना आपल्या दैनंदिन कामकाजाचा अविभाज्य भाग बनवले आहे. परंतु आपल्यापैकी बहुतेकांना स्वतःचे रक्षण करण्यासाठी आवश्यक असलेल्या सायबर सुरक्षा आणि सुरक्षेची माहिती नाही.

2. सायबर गुन्हे म्हणजे काय?

सायबर गुन्हे म्हणजे डिजिटल माध्यमांद्वारे किंवा इंटरनेटद्वारे केल्या जाणाऱ्या गुन्हेगारी कृती. यामध्ये व्यक्ती, संस्था किंवा अगदी सरकारला हानी पोहोचवण्याच्या, संवेदनशील माहिती चोरण्याच्या, आर्थिक नफ्यासाठी किंवा सामान्य कामकाजात व्यत्यय आणण्याच्या उद्देशाने लक्ष्य करणाऱ्या विविध प्रकारच्या बेकायदेशीर कृतींचा समावेश आहे.तसेच सायबर गुन्हेगार पीडितांवर हल्ला करण्यासाठी सोशल नेटवर्किंग साइट्स, ईमेल, चॅटरूम, पायरेटेड सॉफ्टवेअर, वेबसाइट इत्यादी प्लॅटफॉर्मचा वापर करतात. मुले देखील विविध प्रकारच्या सायबर गुन्ह्यांना बळी पडतात. डियन कॉम्प्युटर इमर्जन्सी रिस्पॉन्स टीम (CERT-In) नुसार, २०१७ मध्ये भारतात सायबर सुरक्षेच्या ५३००० हून अधिक घटनांची नोंद झाली.

काळजी करू नका मित्रांनो, सावधगिरी बाळगून आणि सतर्क राहून तुम्ही सायबर गुन्ह्यांपासून स्वतःचे रक्षण करू शकता. मी तुमचा सायबर मित्र आहे आणि मी तुम्हाला विविध प्रकारचे सायबर गुन्ह्यांचे आणि सायबर गुन्ह्यांचा बळी पडण्याचा धोका कमी करण्यासाठी तुम्ही घ्यावयाच्या खबरदारीचे उपाय समजून घेण्यास मदत करेन.

1. कोणालाही प्रभावित करू शकणारे सायबर धोके:-

सायबर धोके हे इंटरनेट किंवा मोबाईल तंत्रज्ञानाचा वापर करून आपल्यावर हल्ला करण्यासाठी वापरल्या जाणाऱ्या विविध संभाव्य मार्गांपैकी एक आहेत.सायबर गुन्हेगारांना आपल्या संवेदनशील माहितीवर अनधिकृत प्रवेश मिळवायचा असतो. बहुतेक प्रकरणांमध्ये, सायबर गुन्हेगार स्पष्ट उद्देशाने हल्ला करतात, त्यासाठी ते काही सर्वात प्रभावी पद्धती वापरतात.

सायबर गुन्हेगारांकडून वापरले जाणारे काही सामान्य मार्ग असे आहेत:

I. **ईमेल स्पूफिंग (Email Spoofing):** तुम्हाला असे ईमेल पाठवणे जे खरे वाटतात आणि विश्वासार्ह ईमेल आयडीवरून - .येतात परंतु प्रत्यक्षात ते खरे नसतात

II. **दुर्भावनापूर्ण फाइल्स ॲप्लिकेशन्स (Malicious Files Applications):** तुमच्या स्मार्ट फोन आणि वैयक्तिक डेटामध्ये प्रवेश मिळविण्यासाठी थेट मेसेजिंग, गेमिंग, ईमेल किंवा वेबसाइट इत्यादींद्वारे तुम्हाला दुर्भावनापूर्ण आणि वाईट ॲप्लिकेशन्स आणि फाइल्स पाठवणे .

III. **सोशल इंजिनिअरिंग (Social Engineering):** सोशल इंजिनिअरिंग ही सायबर गुन्हेगारांकडून तुमच्याकडून माहिती मिळविण्यासाठी तुमचा आत्मविश्वास मिळवण्यासाठी वापरली जाणारी एक तंत्र आहेतुम्हाला सर्वात जास्त काय करायला . आवडते यावर अवलंबून, सायबर गुन्हेगार माहिती मिळवण्यासाठी तुमच्याशी संवाद साधण्याचा आणिकिंवा तुमचे काही / समजा तुम्हाला ऑनलाइन गेम खेळायला आवडत असेल .नुकसान करण्याचा प्रयत्न करू शकतो, तर एक तोतयागिरी करणारा दुसऱ्या मुलासारखा वागतो आणि तुम्हाला त्याच्याशी बोलण्यासाठी आणि माहिती शेअर करण्यासाठी आमंत्रित करतो .

IV. **सायबर धमकी(Cyber Bullying):** संगणक, मोबाइल फोन, लॅपटॉप इत्यादी इलेक्ट्रॉनिक किंवा संप्रेषण उपकरणांच्या वापराद्वारे छळ किंवा धमकीचा एक प्रकार.

V. **ओळख चोरी (Identity Theft) :**एखाद्याच्या ओळखीचा जाणूनबुजून वापर करून आर्थिक फायदा मिळवणे किंवा दुसऱ्या व्यक्तीच्या नावाने क्रेडिट आणि इतर फायदे मिळवणे .समकक्षांचे नुकसान किंवा नुकसान करणे /

VI. **नोकरीतील फसवणूक (Job Frauds):** एखाद्या कर्मचाऱ्याने किंवा संभाव्य कर्मचाऱ्याने नियोक्त्याकडे केलेले फसवे प्रतिनिधित्व किंवा फसवे क्रियाकलाप .

VII. **बँकिंग फसवणूक (Banking Frauds):** बँक किंवा इतर वित्तीय संस्था असल्याचे भासवून ठेवीदारांकडून फसवणूक करून पैसे मिळवणे.

अनोखी आव्हाने:-

पारंपारिक गुन्हेगार संगणक तंत्रज्ञानाचा वापर करणार असल्याने, सायबर गुन्ह्यांचे स्वरूप आणि वैशिष्ट्ये भारत सरकार आणि धोरणकर्त्यांसाठी नवीन आव्हाने घेऊन येतील;

- ❖ गतिक पोहोच अधिकारक्षेत्राच्या मुद्द्यांसह), विषम गुन्हेगारी कायदे आणि मोठ्या प्रमाणावर पीडित होण्याची शक्यता(;
- ❖ ज्या वेगाने गुन्हे केले जाऊ शकतात;
- ❖ प्रत्यक्षदर्शी, फिंगरप्रिंट्स, ट्रेस पुरावा किंवा डीएनए यांसारख्या संपार्श्विक किंवा फॉरेन्सिक पुराव्यासह पुराव्याचे अस्थिरता किंवा क्षणिक स्वरूप; आणि

तपासाचा उच्च खर्च. डिजिटल युगातील आव्हाने आणि इलेक्ट्रॉनिक गुन्हे किंवा सायबर गुन्हे किंवा संगणक गुन्ह्यांच्या तपासासाठी असंख्य आणि वैविध्यपूर्ण आहेत आणि त्यात समाविष्ट आहेत; बहु-अधिकारक्षेत्रीय सीमारेषा दूर करणे;

- ❖ पुरावे टिकवून ठेवणे आणि जतन करणे;
- ❖ योग्य शक्ती प्राप्त करणे;
- ❖ डीकोडिंग एनक्रिप्शन;
- ❖ ओळख सिद्ध करणे;
- ❖ पुरावे कोठे शोधायचे हे जाणून घेणे;

- ❖ गुन्ह्याच्या साधनांचा सामना करणे आणि गुन्ह्यांचा प्रतिकार करण्यासाठी साधने विकसित करणे;
- ❖ तपासणीच्या खर्चाचा आणि प्राधान्यक्रमांचा पुनर्विचार; □ रिअल टाइममध्ये गुन्ह्याला प्रतिसाद देणे;
- ❖ अन्वेषण क्रियाकलापांचे समन्वय;
- ❖ संस्थेच्या सर्व स्तरांवर प्रशिक्षण सुधारणे;
- ❖ धोरणात्मक भागीदारी आणि युती विकसित करणे;
- ❖ इलेक्ट्रॉनिक गुन्ह्यांच्या अहवालात सुधारणा करणे;
- ❖ माहिती आणि बुद्धिमत्तेची देवाणघेवाण वाढवणे;
- ❖ प्राप्त करणेविशेषज्ञ कर्मचारी विकसित करणे आणि कायम ठेवणे .; आणि
- ❖ "टेक.(किंवा अत्याधुनिक तंत्रज्ञानात प्रवेश मिळवणे) टाळणे "लॅग-

फॉरेन्सिक आव्हाने, विशेषतः, खूप विचारात आहेत. यूएस डिपार्टमेंट ऑफ जस्टिसने एका अहवालातफॉरेन्सिक पुरावे संकलन आणि विश्लेषणाच्या संबंधात चार प्रमुख आव्हाने ओळखली आहेत;

1. 'माहिती महासागर' मध्ये पुरावे शोधणे – महत्त्वाचे पुरावे शोधणे जवळजवळ अशक्य आहे. valuablexz1 ` 1232 माहितीला असंबद्ध माहितीपासून वेगळे करण्यासाठी देखील विलक्षण तांत्रिक प्रयत्नांची आवश्यकता आहे. पुरावे कुठे साठवले जातात ते स्थान निश्चित करणे देखील खूप कठीण आहे.

2.निनावीपणा – संगणक नेटवर्क व्यक्तींना सहजपणे निनावी ठेवण्याची परवानगी देतात आणि बऱ्याच वेब सर्व्हरला "हँडल", खोटे नाव किंवा ओळख असते.

3.शोधण्यायोग्यता – निनावीपणाशी संबंधित, शोधण्यायोग्यता म्हणजे संगणक आणि संप्रेषण नेटवर्क, जसे की इंटरनेटवर संप्रेषणांचे स्रोत आणि गंतव्य स्थापित करणे किती कठीण आहे याचा संदर्भ देते. प्रसार आणि एकाधिक संप्रेषण प्रदात्यांसाठी सुलभ उपलब्धतेमुळे ट्रेसेबिलिटी आणखी कठीण होत आहे. उदाहरणार्थ, इंटरनेटवरील संप्रेषणे 10 वेगवेगळ्या इंटरनेट सेवा प्रदात्यांमधून (ISP's) सहजपणे जाऊ शकतात, ज्यापैकी प्रत्येकाने संप्रेषण शोधण्यासाठी माहिती प्रदान करणे आवश्यक आहे.

4.एनक्रिप्शन - लवकरच, बहुसंख्य डेटा आणि संप्रेषणे एनक्रिप्ट केली जातील. एन्क्रिप्शन कायद्याची अंमलबजावणी करणाऱ्या तपासात अडथळा आणू शकते आणि एन्क्रिप्शन क्रॅक करण्याशी संबंधित समस्यांमुळे खर्च वाढवू शकते

निष्कर्ष:-

इंटरनेटवरील गुन्हेगारी वर्तन, किंवा सायबर गुन्हे, हे भारत आणि आंतरराष्ट्रीय कायद्याच्या अंमलबजावणीसाठी भविष्यातील प्रमुख आव्हानांपैकी एक आहे. जसजसे ICT अधिक व्यापक होत जाईल तसतसे, इलेक्ट्रॉनिक गुन्ह्यांचे पैलू सर्व प्रकारच्या गुन्हेगारी वर्तनामध्ये वैशिष्ट्यीकृत होतील, अगदी त्या बाबी देखील ज्यांना सध्या अधिक पारंपारिक गुन्हे मानले जाते. अंमली पदार्थांची तस्करी, लोकांची तस्करी, दहशतवाद आणि मनी लाँड्रिंगचा समावेश असलेल्या अनेक आंतरराष्ट्रीय गुन्ह्यांमध्ये हे आधीच वैशिष्ट्यीकृत आहे. पारंपारिक गुन्ह्यांमध्येही डिजिटल पुरावे अधिक सामान्य होतील आणि या नवीन आव्हानाला सामोरे जाण्यासाठी आपण तयार असले पाहिजे. इंटरनेटवर सुरक्षितता आणि सुरक्षितता सुनिश्चित करण्यासाठी जगभरातील कायदा अंमलबजावणी संस्था नवीन भागीदारी, नवीन न्यायवैद्यक पद्धती आणि सायबर गुन्ह्यांना नवीन प्रतिसाद विकसित करण्यासाठी एकत्र काम करत आहेत. सायबर गुन्ह्यांचा शोध, प्रतिबंध आणि प्रतिसाद देण्यासाठी जागतिक संदर्भात लागू केलेली नवीन कौशल्ये, तंत्रज्ञान आणि तपास तंत्रे आवश्यक असतील. हा "नवीन व्यवसाय" गुन्ह्यांचे नवीन प्रकार, आक्षेपार्ह आणि पीडित होण्याचे एक विस्तृत व्याप्ती आणि प्रमाण, अधिक वेळेवर प्रतिसाद देण्याची गरज आणि आव्हानात्मक तांत्रिक आणि कायदेशीर गुंतागुंत याद्वारे वैशिष्ट्यीकृत केले जाईल.

संदर्भ:-

2. Etter B. (2002), The challenges of Policing Cyberspace, presented to the Netsafe: Society, Safety and the Internet Conference, Auckland, New Zealand.

3. Eric J. Sinrod and William P Reilly, Cyber Crimes (2000), A Practical Approach to the Application of Federal Computer Crime Laws, Santa Clara University, Vol 16, Number 2.

4. Gengler, B. (2001), Virus Cost hit $20bn, The Australian, 11 September p.36. 5. The IT Act 2000.

6. Cyber stalking India, www.indianchild.com.

7. Cybercrime a new challenge for CBI,www.rediff.com, March 12, 2003 12:27 IST

8. Richard Raysman& Peter Brown (1999), Viruses Worms, and other Destructive Forces N. Y. L. J.