Gurukul International Multidisciplinary Research Journal (GIMRJ)*with* International Impact Factor 8.357
Peer Reviewed Journal
DOI link - https://doi.org/10.69758/GIMRJ/2503I3IIVXIIIP0056

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

डिजिटल हाऊस अरेस्ट भीती, फसवणूक आणि सजगतेची गरज

अमोल दिलीप दोंड
सहाय्यक पोलीस निरीक्षक,
जनसंपर्क अधिकारी
मा.पोलीस आयुक्त, नागपूर शहर.
ईमेल: dond.amol@gmail.com
मो. क्र. 9823075006

सारांश:
आजकालच्या डिजिटल जगात आपण सर्वजण तंत्रज्ञानावर अधिकाधिक अवलंबून आहोत. पण याच तंत्रज्ञानाचा गैरफायदा घेत सायबर गुन्हेगार निष्पाप लोकांना मोठ्या शिताफीने जाळ्यात अडकवत आहेत. डिजिटल हाऊस अरेस्ट हा सायबर गुन्ह्याचा एक अत्यंत धोकादायक प्रकार आहे, जिथे लोकांना त्यांच्या मनात भीती निर्माण करून पूर्णतः गुन्हेगारांच्या ताब्यात घेतले जाते.

संकेत शब्द: तंत्रज्ञान, डिजिटल हाऊस अरेस्ट, सायबर गुन्ह्य

प्रस्तावना:

कल्पना करा, तुम्हाला अचानक एक फोन येतो. समोरचा आवाज अत्यंत गंभीर आणि धोकादायक असतो. तो तुम्हाला सांगतो की, "तुम्ही एखाद्या मोठ्या आर्थिक गैरव्यवहारात सापडला आहात, आणि आता सीबीआइ, एनआईए किंवा ईडी तुमच्यावर कारवाई करणार आहे! तुमचे बँक खाते तपासले जात आहे, तुमच्या नावावर लवकरच गुन्हा दाखल होईल" यावेळी तुम्हाला काळजी वाटते, घाबरायला होते, आणि हळूहळू तुम्ही त्याच्या शब्दांवर विश्वास ठेवायला लागता. सायबर गुन्हेगार अत्यंत हुशारीने तुमच्या मनात भीती निर्माण करतात. ते तुम्हाला सतत फोनवर ठेवतात, तुम्ही कुठेही जाऊ शकत नाही, कुणाशीही बोलू शकत नाही, कारण तुम्ही आता आमच्या तपासाअंतर्गत आहात असे बजावले जाते. तुमच्यावर मानसिक दडपण वाढवले जाते. सतत व्हॉट्सअप, स्कायप किंवा अन्य माध्यमांद्वारे व्हिडिओ कॉल करून तुम्हाला पूर्णतः बंदिस्त ठेवले जाते. त्यांच्यासोबत बोलताना तुमच्या मनात असंख्य विचार येतात. मी काही चुकीचं तर केलं नाही ना? कदाचित माझ्या बँक व्यवहारात काही चूक झाली असेल का ? मी आता काय करणार ?आणि याच गोंधळाचा फायदा सायबर गुन्हेगार घेतात. ते तुम्हाला सांगतात की, जर तुम्ही निर्दोष असाल, तर काही पैसे भरून तुमच्या नावावरील संशय दूर करू शकता. त्या भीतीतून तुम्ही पैसे पाठवता. एकदा नाही, दोनदा नाही तर पुन्हा पुन्हा! पण मग समजतं की ही तर मोठी फसवणूक होती. त्या क्षणी तुमच्या मनात अनंत भावना दाटून येतात राग, लाज, अपमान, दुख आणि आत्मग्लानी. आपण कसे काय एवढे मोठे फसवले गेलो? आपण का कोणालाही काही सांगितले नाही? हे सगळं टाळता आलं असतं का ?

"डिजिटल हाऊस अरेस्ट":

होय ! हे पूर्णपणे टाळता येऊ शकतं आजच्या आधुनिक युगात सायबर गुन्हेगारीने प्रचंड वेग घेतला आहे आणि त्यातील एक नवीन आणि अत्यंत धोकादायक स्वरूप म्हणजे "डिजिटल हाऊस अरेस्ट". हा एक असा प्रकार आहे जिथे विशेषतः ज्येष्ठ नागरिक आणि महिला यांना टार्गेट केले जाते. सायबर गुन्हेगार अत्यंत नियोजनबद्ध पद्धतीने संपर्क साधून त्यांचा विश्वास संपादन करतात आणि मोठ्या प्रमाणात आर्थिक फसवणूक करतात.

मानसिक तणाव निर्माण करणारा सायबर गुन्हा:

डिजिटल हाऊस अरेस्ट हा एक अत्यंत धूर्त आणि मानसिक तणाव निर्माण करणारा सायबर गुन्हा आहे. यात सायबर गुन्हेगार स्वतःला सीबीआइ, एनआईए, ईडी किंवा अन्य शासकीय संस्थेचा अधिकारी असल्याचे भासवतात. पीडित व्यक्तीला व्हॉट्सअप, विओआईपी, वाई फाई किंवा सिम कॉलद्वारे संपर्क केला जातो. त्यांना सांगितले जाते की ते एखाद्या मोठ्या गुन्ह्यात अडकले आहेत. बनावट वॉरंट किंवा बोगस

कागदपत्रे पाठवून विश्वास संपादन केला जातो. पिडीतेला घरातच थांबण्यास सांगून त्यांना सतत निगराणीखाली ठेवले जाते. आर्थिक माहिती मिळवून पैसे पाठवण्यास भाग पाडले जाते.सायबर गुन्हेगार पीडित व्यक्तीला कॉल करून सांगतो की, तुमचं नाव एखाद्या गंभीर गुन्ह्यात आले आहे. तो स्वतःला सीबीआइ किंवा ईडी सारख्या शासकीय संस्थेचा अधिकारी असल्याचे भासवतो. मोठ्या गुन्ह्यांमध्ये अडकण्याची भीती दाखवतो, जसे की मनी लॉन्ड्रिंग, टॅक्स चोरी, आर्थिक गैरव्यवहार इत्यादी. त्यानंतर, तो सांगतो की तुमच्या निर्दोषतेचा तपास सुरू आहे, त्यामुळे तुम्हाला सहकार्य करावे लागेल.

पीड़ित व्यक्ति घाबरते:

पीडित व्यक्तीला सांगितले जाते की, तुम्हाला कुठेही जायला किंवा कोणाशीही बोलायला परवानगी नाही. सायबर गुन्हेगार सतत संपर्कात राहतो, त्यांना सतत फोन, व्हिडिओ कॉल किंवा चॅटद्वारे गुंतवून ठेवतो. बोगस वॉरंट पाठवून मानसिक तणाव वाढवला जातो.पीडित व्यक्तीला सांगितले जाते की तुमच्या निर्दोषतेचा पुरावा द्यायचा असेल तर तुम्हाला काही प्रमाणात पैसे भरावे लागतील. पैसे पाठवण्याच्या प्रक्रिया सुरू होतात आरटीजीएस, एनईएफटी, कयुआर कोड किंवा थेट बँक ट्रान्सफर. जर पीडित व्यक्तीकडे पैसे नसतील, तर त्यांना पर्सनल लोन घेण्याचा दबाव टाकला जातो. एकदा पैसे गुन्हेगाराच्या खात्यात गेले की, ते सांगतात की ती रक्कम सरकारकडून गोठवली आहे. आणखी पैसे देण्याची मागणी केली जाते, अन्यथा मोठ्या कायदेशीर कारवाईची भीती दाखवली जाते. पीडित व्यक्ती आर्थिक आणि मानसिक तणावाखाली पूर्णतः गुन्हेगारांच्या ताब्यात येते. कोणतीही शासकीय संस्था व्हॉट्सअप किंवा सामान्य कॉलद्वारे संपर्क करत नाही. जर सीबीआई, एनआईए, ईडी किंवा कोणत्याही सरकारी संस्थेच्या नावाने कॉल आला, तर तो लगेच ब्लॉक करयला पाहिजे. सायबर गुन्हेगार भावनिक आणि मानसिक दबाव टाकण्याचा प्रयत्न करतात. घाबरून काहीही कृती करू नका, कोणालाही बँक डिटेल्स कुटुंबीय, मित्र, वकील किंवा पोलिसांशी बोलावे. गुन्हेगार नेहमीच सांगतात की, " ही गोष्ट कोणालाही सांगू नका " त्यामुळे ही माहिती त्वरित शेअर करणे गरजेचे आहे. सायबर क्राइम हेल्पलाइन नंबर (1930) वर त्वरित कॉल करा. www.cybercrime.gov.in (डब्लू डब्लू डब्लू. साइबरक्राइम.गवर्मेंट.ईन) या वेबसाइटवर ऑनलाईन तक्रार दाखल करा. सायबर गुन्हेगार तुम्हाला स्कायप, व्हॉट्सअप किंवा इतर माध्यमांतून अज्ञात अप्स डाऊनलोड करण्यास सांगतात. यामुळे तुमच्या फोनमधील सर्व माहिती हॅक होण्याची शक्यता असते. डिजिटल हाऊस अरेस्ट हा सायबर गुन्ह्याचा अत्यंत धोकादायक प्रकार आहे. हा गुन्हा फक्त तुमच्या परवानगीशिवाय होऊ शकत नाही. कोणत्याही प्रकारच्या शासकीय तपास यंत्रणा व्हॉट्सअप कॉलद्वारे संपर्क करत नाहीत, पैसे मागत नाहीत आणि तुम्हाला घरी बसून हाऊस अरेस्ट करत नाहीत. जर तुम्हाला अशा कोणत्याही संशयास्पद कॉल आला, तर घाबरू नका. त्वरित पोलिसांना कळवा, फोन ब्लॉक करा आणि सुरक्षित राहा.

भीतीचा खेळ: व्यापक उपाययोजना:

सायबर गुन्हेगार तुमच्या भीतीचा गैरफायदा घेतात. त्यामुळे सजग राहा, सावध राहा आणि कोणत्याही फसवणुकीला बळी पडू नका! , सायबर गुन्हे, विशेषतः डिजिटल अटक फसवणुकीला सामोरे जाण्यासाठी केंद्र सरकारने समन्वयित आणि व्यापक उपाययोजना केल्या आहेत. भारतीय सायबर गुन्हे समन्वय केंद्र (14सी) गृह मंत्रालयाने हे केंद्र स्थापन केले आहे, जे देशभरातील सर्व प्रकारच्या सायबर गुन्ह्यांना तोंड देण्यासाठी कार्यरत आहे. जनजागृती कार्यक्रम डिजिटल अटक फसवणुकी विरोधात लोकांना जागरूक करण्यासाठी केंद्र सरकारने वृत्तपत्रे, मेट्रोमध्ये जाहिराती, सोशल मीडिया प्रभावकांचा (इन्फ्लूएंसर्स) वापर, प्रसार भारती आणि आकाशवाणीवरील विशेष कार्यक्रमाचे आयेाजन केले जाते. याकरीता सर्वसामान्य नागरीकांनी जनजागृतीपर सहभाग घेणे आवश्यक आहे. केंद्र सरकारने सायबर गुन्हेगारांकडून पोलीस, एनसीबी, सीबीआई, आरबीआई आणि इतर कायदा अंमलबजावणी यंत्रणांची तोतयागिरी करून केलेल्या 'ब्लॅकमेलिंग' आणि 'डिजिटल अटक' घटनांबाबत सावधगिरीची सूचना जारी केली आहे. स्पूफ कॉल्स ब्लॉकिंग केंद्र सरकार आणि टेलिकॉम सेवा प्रदाते (टीएसपी एस) यांनी आंतरराष्ट्रीय बनावट कॉल

DOI link - https://doi.org/10.69758/GIMRJ/2503I3IIVXIIIP0056
e-ISSN No. 2394-8426
Special Issue on Cyber Crime and Social Media
Issue–III(II), Volume–XIII

ओळखून ब्लॉक करण्याची व्यवस्था तयार केली आहे. हे कॉल भारतातील क्रमांक दर्शवून भारतातूनच आल्यासारखे भासविले जात होते. हे कॉल सायबर गुन्हेगारांकडून डिजिटल अटक, फेडेक्स फसवणूक, सरकारी आणि पोलीस अधिकारी यांची तोतयागिरी इत्यादींसाठी वापरले जातात. राष्ट्रीय सायबर गुन्हा अहवाल पोर्टल (एच टी टी पी एस://साइबरक्राइम.गवर्नमेंट.ईन) 14सी अंतर्गत हे पोर्टल सुरू करण्यात आले असून, येथे सर्व प्रकारच्या सायबर गुन्ह्यांची, विशेषतः महिला आणि मुलांवरील गुन्ह्यांची तक्रार नोंदविता येते. पोर्टलवर नोंदवलेल्या गुन्ह्यांवर संबंधित राज्य केंद्रशासित प्रदेशातील कायदा अंमलबजावणी यंत्रणा कायद्यानुसार कारवाई करतात.नागरिक आर्थिक सायबर फसवणूक तक्रार आणि व्यवस्थापन प्रणाली 2021 मध्ये सुरू करण्यात आलेल्या या योजनेअंतर्गत आर्थिक फसवणुकीच्या घटनांची तत्काळ नोंद घेऊन पैसे हस्तांतरण थांबवता येते. 1930 हा टोल-फ्री हेल्पलाइन क्रमांक यासाठी कार्यरत आहे.

निष्कर्ष:

शेवटी कुठल्याही प्रकारचा सायबर गुन्हा असेल तो या चार प्रकारांमध्ये जर पैसे पाठवत असेल आणि आपण जर सतर्क राहिलो तर आपले पैसे बँक खात्यात सुरक्षित राहतील. ओटीपी देऊ नये, कुठल्याही लिंक ला क्लिक करू नये, खात्री केल्याशिवाय कुणाच्या खात्यात पैसे पाठवू नये आणि कार्ड डिटेल शेअर करू नये. जगाच्या पाठीवर अनेक सायबर फ्रॉड आले येत राहतील आणि पुढे पण चालू असेल परंतु वरील 4 गोष्टी जर आपण सदसदविवेकबुदधीचा वापर करुन पालन केले तर निश्चित सायबर फ्रॉड पासून आपण बचाव करू शकतो .