Gurukul International Multidisciplinary Research Journal (GIMRJ)*with* International Impact Factor 8.357
Peer Reviewed Journal
DOI link - https://doi.org/10.69758/GIMRJ/2503I3IIVXIIIP0066

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

सायबर हल्ल्याची समज
Understanding Cyber Attacks

डॉ. सुरेश एच. मिलमिले
सहाय्यक प्राध्यापक
आठवले समाजकार्य महाविद्यालय,
चिमूर, जि.चंद्रपूर
ईमेल : sureshmilmile@gmail.com
Mob. ९४२०५५४८००

सायबर गुन्हा ही गुन्हेगारी क्रिया आहे. ज्यामध्ये संगणक नेटवर्क किंवा नेटवर्क उपकरण समाविष्ट आहे. बहुतेक सायबर गुन्हे नफा कमविण्यासाठी करतात. सध्या लोक कॉम्प्युटर, लॅपटॉप, मोबाईलचा सर्रास वापर करीत आहेत. सर्व आर्थिक व्यवहार ऑनलाईन होत आहेत. भारतात ही क्रांती वेगाने होत आहे. याच बरोबर सायबर गुन्हेगारीही वेगाने वाढत आहे. अस म्हणतात किंवा आख्यायीका आहे की, धरती पुर्वी शेषनागाच्या फन्यावर उभी होती. त्यानंतर माणसाची विकासासोबत संकल्पना बदलल्या, कालांतराने ती माणसाच्या मनगटावर उभी आहे. माणसाचा पुन्हा विकास झाला आज धरती असे म्हणतात की, इंटरनेटच्या जाळयावरती उभी आहे. इंटरनेटच्या तंत्रज्ञानाने मानवाला एका सेकंदात संपूर्ण जगाची माहिती मिळू शकते. चांगल्या कामासाठी व प्रामाणिकतेने जिवन जगण्यासाठी याचा वापर केला तर स्वर्गीय सुख इथेच आहे. परंतू विकासासोबत तेवढीच कमालीची वाढ सायबर गुन्हेगारीमध्ये झालेला आहे. याचे मुख्य कारण आहे, लोकांमध्ये सायबर सुरक्षेच्या बाबतीत आवश्यक असणाऱ्या माहितीचा अभाव सायबर गुन्हाविषयी अनेक घटना कानावर येतात. भारत इंटरनेट वापरात दुसऱ्या क्रमांकावर आहे. मात्र सायबर सुरक्षेच्या बाबतीत पिछाडीवर आहे. सायबर गुन्हे हा एक प्रकारचा आर्थिक दहशतवादच आहे. सायबर गुन्हयाविषयी अनेक घटना कानावर पडतात. काही आप्तस्वकीयांसोबत फसवेगीरीच्या घटना होतांना दिसतात. मोबाईलवरून असं बोलल्या जाते, फोन येतो की, मी बॅंक मॅनेजर बोलतो आपले अकाऊंट बंद होत आहे. चालू ठेवण्याकरीता तुमच्या एटीएम चा सोळाअंकी नंबर सांगा तो सांगिल्यानंतर एक ओटीपी येईल, तो सांगा तो सांगितल्यानंतर पैसे अकाऊंट मधून काढल्या जाते. क्रेडीट कार्ड संबंधात लिंक पाठविल्या जाते. लिंक ओपन करून काही माहिती भरली, पैसे कटतात, फसवणुक होते. एखाद पार्सल आपल्याला आलेलं असतं अशी बतावणी करून त्याची रक्कम दिलेली आहे फक्त ओटीपी सांगा आणि ओटीपी सांगितला व आर्थिक फसवणुक झाल्याचे निदर्शनास आले. अशा वेगवेगळया प्रकारच्या अनेक घटना समाजात घडतांना दिसतात.

विशेषकरून लहान मुले, स्त्रिया, विद्यार्थी हेच नाही तर बुध्दीमान लोक, कंपन्या, बॅंक, संस्था, समुह या साबर गुन्हयांना बळी पडतात आणि हे या संकटापासून कसे बचाव करणार हा यक्ष प्रश्नच आहे आणि हा प्रश्न फक्त भारतापुरताच नाही तर जागतिक प्रश्न, आव्हान उभे आहेत. किमान अल्पवयीन मुलांचा लैंगिक शोषण व फसवणुक यापासून बचाव करण्यासाठी सायबर ुसरक्षेची जाणीवजागृती होणे आवश्यक आहे. जास्तीतजास्त मुले ऑनलाईन गेम खेळणे, मित्र बनविणे यासाठी नेटवर्कींग साईटचा उपयोग करतात. ऑनलाईन शॉपींग करतात व यामध्ये सायबर गुन्हेगारांची संकटे ओढावलेली दिसतात. त्यातून बचाव करावयाच्या उपायांची त्यांना खुप कमी माहिती असते व मुले प्रयोगिक वयाच्या वर्गात असतात ते प्रयोग करू इच्छितात. परंतू सायबरचे वाईट संकटाचा प्रभाव दिसून येते व स्वत:ला यातून सुरक्षीत ठेवण्यास प्रयत्न होणे आवश्यक आहे. आजच्या युगात इंटरनेट, कॉम्पुटर, स्मार्टफोन व इतर अनेक संवाद माध्यमे व उपकरणे जीवनाचा अभिन्न भाग बनले आहेत. यात गुगल, ई–मेल्स, व्हॉट्सॲप, ट्विटर, फेसबुक इ. माध्यमांना आपल्या दैनंदिन जीवनाचा एक अनभिज्ञ भाग बनविला आहे. परंतू पुष्कळ व्यक्तींना सायबर सुरक्षा आणि स्वत:ला सायबर गुन्हयापासून सुरक्षित आवश्यक असणाऱ्या उपाययोजनाची माहिती नाही. ते पुर्णत: अनभिज्ञ आहेत. सायबर गुन्हेगार सोशल नेटवर्कींग साईटस, इमेल, चॅटरूम, बनावट सॉफ्टवेअर, वेबसाईट अशा माध्यमांचा उपयोग करून सावजावर हल्ला करण्यास या गोष्टींचा उपयोग करतात.

सायबर संकटाचे विविध प्रकार आहेत. इंटरनेट वा मोबाईल तंत्रज्ञानाच्या साहयाने तुम्हाला संकटात टाकू शकतात, तुमचे नुकसान करू शकतात. हॅकर ही अशी व्यक्ती असते जी अनपेक्षीत फायद्यांसाठी संचार माध्यमांचा उपयोग/दुरूपयोग करून अनेकांचे आर्थिक नुकसान करू शकते. ज्यांच्या प्रतिष्ठेला धक्का पोहचवू शकते. हॅकर्स तुमच्या कॉम्पुटरचे नुकसान करणे व तुमच्या डाटा पर्यंत पोहचवणे यासाठी मालवेअर्स वायरस वा ट्रोजन्सचा उपयोग करू शकतात. सायबर गुन्हेगार आपल्या कार्यासाठी जास्तीत जास्त प्रभावशाली पध्दतींचा वापर करतात.

ई–मेल स्पुफिंग :–

तुम्हाला असे ईमेल पाठविले जातात जे तुम्हाला खरे वाटावेत. ज्यावर तुमचा विश्वास बसावा असे ई–मेल आयडी ने पाठविला आहे असे वाटते. परंतू हे खरे नसते ती फसवणुक असते.

व्देषपुर्ण फाईल अप्लिकेशन :–

तुमचा स्मार्टफोन व व्यक्तीगत डाटा पर्यंत पोहचण्यासाठी मॅसेज पाठविणे, गेमिंग, ईमेल आणि वेबसाईटच्या मार्फत तुम्हाला व्देषपुर्ण व घाणेरडे अप्लिकेशन आणि फाईल पाठविणे.

सामाजिक संबंधाचे व्यवस्थापन :–

सामाजिक संबंधाचे व्यवस्थापन असे तंत्रज्ञान आहे. त्याचा उपयोग सायबर गुन्हेगार तुमची माहिती मिळविण्यासाठी आपला विश्वास संपादन करण्यासाठी केला जातो व तुमचे काही नुकसान करण्यासाठी केला जातो व तुमचे काही नुकसान करण्यासाठी सायबर गुन्हेगार आपल्याशी संपर्क साधण्यास प्रयत्न करण्यास हा प्रयत्न करतात की तुम्हाला काय आवडते, यातून तुमच्याशी संपर्क साधुन तुमची माहिती तुमच्याकडून काढून घेतात.

सायबर बुलिंग :–

इलेक्ट्रॉनिक व संचार माध्यमे जसे संगणक, मोबाईल फोन, लॅपटॉप इत्यादिंचा वापर करून कोणता मनस्ताप देणे (त्रास देणे) एक प्रकार आहे. अश्लिल व्हिडीओ पाठविणे, भिती दाखविणे, धमकी देणे, संदेश देणे इ.

ओळख चोरण :–

आर्थिक लाभासाठी कोणादुसऱ्या व्यक्तीच्या नावावर बनावट कर्ज घेणे किंवा दुसरा फायदा घेण्यास एखाद्या व्यक्तीची ओळख चोरणे वा नुकसान पोहचविणे.

नोकरीसंबंधी फसवणुक :–

नोकरी देणार अशांच्या मदतीने आपल्या नियुक्तीसाठी फसवणुक व कपटी नियोजन करणे.

बॅकींग फ्रॉड :– स्वत: बॅकेचा वा अन्य वित्तीय संस्थेचा प्रतिनिधी असल्याचे दाखवून दुसऱ्याच्या बॅकेच्या खात्यावरून फसवून पैसे काढणे.

दुरसंचार फसवणुक :–

एखादा मित्र वा नातेवाईक अडचणीत असल्याचा फोन येतो.

नॉन डिलीव्हरी फसवणुक :–

यात अत्यंत मागणी असलेल्या वस्तुंचे आश्वासन देतात. पेमेंट स्विकारतात, नंतर काही वितरीत करीत नाही.

गुंतवणुक/बॉयलर रूम फसवणुक :– फसव्या किंवा नालायक शेअर्समध्ये गुंतवणुकीसाठी पिडीतांवर दबाव आणला जातो.

छेडछाड :– नग्न व्हिडीओ चॅटमध्ये सहभाग करून घेऊन गुप्तपणे रेकॉर्ड केले जाते व ब्लॅकमेल करतात.

सॉफ्टवेअर पायरसी कॉपीराईट उल्लंघन आणि पेटंटचे उल्लंघन इ.

सायबर हेरगिरी :– व्यक्ती व गटावर टेहाळणी करण्यास इमेल मजकुर संदेश आणि इंन्स्टंट यासह संप्रेषणाचे निरीक्षण करतात.

ऑनलाईन व्यवहार फसवणुक, सायबर बदनामी, बाल पोर्नोग्राफी, क्रेडीटकार्ड फसवणुक इ. मोठी कमाई करण्यास, सोपा मार्ग निवडतात. नौकरी वैवाहीक फसवणुक, विमा, रासायनिक बिया, ऑनलाईन खरेदी, लॉटरी बक्षिस फसवणुक, टॉवर इंन्स्टालेशन फसवणुक, इमेल हॅकींग, सिम स्वॅपिंग, ग्राहकसेवा इमेल स्पुफिंग, ई–कॉमर्स, रन्समवेअर हल्ला डेटा चोरी, व्हायरस, सेवा नाकारणे, मालवेअर हला.

महिलांना सामना करावा लागत असलेले सायबर गुन्हे

- ई–मेलव्दारे होणारा छळ
- सायबर स्टॉकिंग सायबर विश्वातून होणारा पाठलाग
- सायबर पोर्नोग्राफी सायबर विश्वातून परसविली जाणारी अश्लिलता
- सायबर बदनामी (डिक्रीमेशन)
- मॉर्फिंग संगणकाच्या माध्यमातून इंटरनेटवरील मजुकरामध्ये किंवा छायाचित्रामध्ये फेरफार करणे.
- ई–मेल स्फुपिंग (ईमेलव्दारे होणारे विबंडन/टवाळी)

ब्लॅकमेल करणे, धमकावणे, दंडेली करणे किंवा फसवणुक इ. प्रकारच्या छळवणुकीच्या समावेश होतो. हे बहुतेकदा बनावट खात्यावरून केले जाते, ईमेल पाठविले जाते हे अधिक त्रासदायक असते. आधुनिक काळातील हा सर्वाधिक चर्चीत सायबर गुन्हा म्हणावा लागेल. यामध्ये सातत्याने एखाद्यावर लक्ष ठेवल्या जाते किंवा त्याचा पाठलाग केल्या जातो. मॅसेजेस

पाठविणे, ईमेल पाठविणे किंवा ते वापरत असलेल्या चॅटरूममध्ये प्रवेश करणे. बरेचदा इंटरनेटच्या दुनियेत नविन असलेल्या आणि इंटरनेट सुरक्षिततेची माहिती नसलेल्यांना याचा सामना करावा लागतो. बहुतेक प्रकरणात महिला, मुले किंवा भावनिकदृष्टया कमजोर व्यक्ती गुन्हेगारांचे बळी पडतात. हे गुन्हे करण्यामागचे चार कारणे किंवा मानसिकता दिसतात. लैंगिक छळ, प्रेमात पिसाळलेले, बदल्याची किंवा व्देषाची भावना, इगो, मोफत उपलब्ध असलेले ईमेल्स तसेच चॅटरूम्स किंवा इतर व्यासपिठावर उपलब्ध असलेल्या अनामिकत्व (जिथे तुम्ही तुमची खरी ओळख लपवून ठेवू शकता) यामुळे या गुन्हेगारीमध्ये वाढ झालेली दितसे. इंटरनेट कनेक्टिव्हीटीच्या आवश्यकतेमुळे सायबर क्राईम क्रियाकल्पामुळे प्रमाण आणि गती वाढली आहे. कारण गुन्हा करतांना शारीरिकरीत्या उपस्थित राहण्याची गरज नाही. इंटरनेटचा वेग सुविधा, निनाविपणा आणि सिमा नसल्यामुळे आर्थिक गुन्हयाची संगणक आधारित भिन्नता फसवणुक, मनी लॉड्रींग, पाठलाग, गुंडगीरी गुन्हे वाढलेली आहेत.

सायबर हल्ल्याचे सर्वात हानिकारक प्रकार :–

मालवेअर हल्ला, रन्समवेअर, पासवर्ड हल्ला, डिस्ट्रीब्युटेड डिनायल ऑफ सर्व्हीस, फिशिंग (एसएमएस फिशिंग किंवा स्मिशिंग, व्हाईस फिशिंग किंवा विशिंग), SQL इंजेक्शन हल्ला, रूटकिट, ट्रोजन – स्पायवेअर, शब्दकोष हल्ला, सामाजिक अभियांत्रिकी, किलॉगिंग, पासवर्ड स्लिपींग, पासवर्ड डाटाबेस चोरणे किंवा विकत घेणे, क्रॉस – साईट स्क्रिप्टींग, मॅन–इन–द मध्यम हल्ला, URL व्याख्या/ URL विषबाधा, DNS स्पुलिंग, DNS टनेलिंग, बोटनेट हल्ला, वाटरिंग होल अटॅक, अंतर्गत धमकी, इन्हस्ट्रॅपिंग हल्ला, वाढदिवस हल्ला.

मालवेअर म्हणजे काय?

मालवेअर म्हणजे संगणकाला हानी पोहचविण्यासाठी विकसीत केलेले दुर्भावना पुर्ण सॉफ्टवेअर, सायबर गुन्हेगार मालवेअरचा डाटा चोरण्यासाठी करतात. मालवेअरमुळे संगणकाच्या कामगिरीत व्यत्यय येऊ शकतो आणि संवेदनशिल माहितीची सुरक्षा धोक्यात येऊ शकते. हे हल्ले संगणक, सर्व्हर किंवा संगणक नेटवर्कला हानी पोहचविण्यसाठी डिझाईन केलेले असते. आर्थिक फायद्यासाठी, डेटा मिळविण्यास सायबर गुन्हे करतात.

मालवेअरचे प्रकार :–

व्हॉयरस, वर्म्स, ट्रोजन व्हायरस, सॉफ्टवेअर, ॲडवेअर, रन्समवेअर.

मालवेअर कसा पसरतो :–

ईमेल व्दारे, वेबसाईटव्दारे, फोन्सकॉल्सव्दारे, सॉफ्टवेअर किंवा ॲप डाऊनलोडव्दारे.

एकदा आत गेल्यावर मालवेअर, किबोर्ड, इनपुटचा मागोवा घेतो. माऊस ॲक्टीव्हिटीचे अनुकरण करतो, स्क्रनिंग शेअर करतो आणि भ्रामक पॉप–ॲप प्रदर्शित करतो. वापरकर्ता नावे, ऑपरेटींग सिस्टम माहिती डिव्हाइस रनटाईम आणि सर्वात महत्वाचे म्हणजे बॅक आयडेंटीफायर यासारखा डेटा गोळा करतो. पिडीताच्या बॅक खात्यावर पुर्णनियंत्रण ठेऊन गुन्हेगार ते रिकामे करतात.

व्यवसायावर होणारे परिणाम :–

- कंपनीच्या मुल्यात घट होते.
- भांडवल उभारण्यास अडचण.
- डेटाच्या उल्लंघनामुळे व्यवसायांवर देखील खटला भरला जाऊ शकते.

सायबर हल्ल्यानंतर खराब झालेली ब्रॅड ओळख आणि प्रतिष्ठा गमावल्यामुळे ग्राहकांचा कंपनीवरील विश्वास आणि त्या कंपनीची आर्थिक डेटा सुरक्षीत ठेवण्याची क्षमता कमी होते. सायबर हल्ल्यानंतर कंपनी सध्याचे ग्राहक गमावू शकतात आणि नविन ग्राहक मिळविण्याची क्षमता गमावू शकतात इ.

धोके कसे कमी करावे :–

- व्यवसाय आणि कर्मचाऱ्यांसाठी स्पष्ट धोरणे आणि कार्यपध्दती विकसीत करा.
- सायबर सुरक्षा घटना प्रतिसाद योजना तयार करा.
- सुरक्षा व उपायांची रूपरेषा द्या
- ॲप्स किंवा भौतिक सुरक्षा की वापरा
- शक्य असेल तेव्हा प्रत्येक ऑनलाईन खात्यावर MFA मल्टीफॅक्टर ॲथेंटीफिकेशन सक्रीय करा.
- आर्थिक व्यवस्थापकाशी बोलून त्यासंबंध सत्यता पडताळा

- घुसखोरी शोधप्राली नियम तयार करा.
- निधी हस्तांतरणासाठी सर्व ईमेल विनंत्या तपासा
- कर्मचाऱ्यांना सायबर सुरक्षा धोरणे आणि कार्यपध्दती भंग झाल्यास काय करावे याचे प्रशिक्षण द्या.
- सर्व सॉफ्टवेअर रिलीस अपडेट्स किंवा पॅचसह वेबसाईटस एंडपाईंट (डेन्टाइसेस आणि सिस्टिम चालू ठेवा)
- डेटा भंग झाल्यास होणारे नुकसान कमी करण्यास डेटा व माहितीचा नियमीत बॅकअप घ्या.

आपण काळजी कशी घेणार?

आपल्यावर हल्ला होण्यास आपणही तितकेच जबाबदार असतो. त्यासाठी काही काळजी घेण्याची आवश्यकता आहे.

- गरज असेल तेव्हाच इंटरनेट चालू करावे. कोणतीही लिंक खोलू नका.
- अनोळखी आणि फेक वेबसाईट्स पासून दुर रहावे.
- प्रलोभने दाखवणाऱ्या वेबसाईट्स टाळाव्यात.
- गाणे किंवा व्हिडीओ किंवा एखादे सॉफ्टवेअर डाऊनलोड करण्यासाठी अधिकृत वेबसाईटसचा वापर करावा.
- पायरेटेड वेबसाईटसवर हमखास मालवेअर असतात.
- अनोळखी ई–मेल वरील कोणत्याही लिंकवर क्लिक करू नये. कोणतीही वस्तु घेतांना पडताळणी करा.
- बोगस वेबसाईटसपासून सावध राहा.
- कोणतीही वस्तू खरेदी करतांना ऑनलाईन पुनरावलोकन तपासा.
- आपल्या लॅपटॉप किंवा मॉनिटरचा वेबकॅमेरा नेहमी झाकुन ठेवावा.
- तुम्ही फसवणुकीचे बळी झाल्यास बॅकेला त्वरीत कळवा.
- असा कोणताही ईमेल असल्यास त्वरीत सायबर तज्ञाशी संपर्क करावा व सायबर पोलीसात तक्रार द्यावी. जेणेकरून यात उशीर होणार नाही. काहीही झाले तरी अशा हल्लेखोराला पैसे देऊ नये. यातूनही गुन्हेगारी अशीच फोफावते.
- विनंत्याबाबत सावध राहा.
- कामाच्या ठिकाणी सायबर सुरक्षा संस्कृती लागु करा आणि कर्मचाऱ्यांसाठी समस्या आणि घटनांवर मार्गदर्शन करा.
- ऑनलाईन नातेसंबंध तयार करतांना सावधगिरी बाळगा. विशेषत: जेव्हा पैसे गुंतलेले असते.
- प्रगत डावपेचाची माहिती ठेवा.

सायबर पोलीस ठाणे :–

ही शाखा वेबसाईट हॅकिंग, सायबर स्टॉलिंग, सायबर पोर्नोग्राफी, ईमेल, क्रेडीट कार्ड गुन्हे, सॉफ्टवेअर पायरसी ऑनलाईन फसवणुक आणि इंटरनेट क्राईमच्या तपासाशी संबंधीत आहे. हे विशेष माहिती तंत्रज्ञान कायदा (२००८) अंतर्गत IPC आणि इतर कायद्यासह नोंदणीकृत प्रकरणची चौकशी करते.

हल्लेखोर सापडल्या जाऊ शकतो. इंटरनेटवरील 'फुटप्रिंट' नाहीसे करतात तसेच आय.पी. लपवलेला किंवा बदललेला असतात. सायबर तज्ञांच्या मदतीने काही टुल्स वापरून ते शोधता येते. तसेच सायबर पोलीसांच्या आणि दुरसंचार विभागाच्या मदतीने बदल अधिक सखोल आणि कायदेशिररित्या माहिती मिळविता येते.

सायबर गुन्हेगार अधिकाधिक चपळ आणि संघटीत होत आहे. नवनविन तंत्रज्ञानाचा वापर करत आहे. सायबर गुन्हयांना राष्ट्रीय सिमा नाही ते अनेक क्षेत्रामध्ये गुन्हे करतात. ज्यामुळे तपास आणि खटल्यांमध्ये अनेक आव्हाने येतात. इंटरपोल मध्ये कायद्याची अंमलबजावणी करणाऱ्या ऑपरेशन्समध्ये समन्वय साधणे आणि सायबर धोके कमी करण्यास सुरक्षित डेटा शेअरिंग प्लॅटफार्म विश्लेषण आणि प्रशिक्षा देणे. सायबर गुन्हा प्रतिबंध, शोध तपास आणि व्यत्यय आणण्यास सदस्य देशाची क्षमता वाढवून सुरक्षित जगासाठी समुदायाचे संरक्षण करण्यास मदत करू शकतो.

यात सायबर क्षमता प्रशिक्षण कार्यक्रम, प्रकल्प साधने आणि प्लॅटफार्मव्दारे सर्वच पोलीसांकडे सायबर गुन्हयाचा प्रभावीपणे सामना करण्याची क्षमता आहे आणि ही घडयाळाच्या विरूध्दची शर्यत आहे. यशस्वी खटला चालविण्यास पुरेसा पुरावा गोळा करण्यासाठी वेळ व मर्यादा देण्यात आली आहे. गुन्हेगार त्यांच्या पिडीतांच्या अज्ञानाचा आणि असुरक्षिततेचा फायदा घेतात. स्मार्टफोन्स आणि टॅबलेटपासून वेबकनेक्ट केलेल्या उपकरणापर्यंत शोध घेतल्यास गुन्हेगार सापडतात. तरीही व्यक्तींनी

सामान्यज्ञान नियमांचे पालन करून तुम्ही तुमचा संपर्क आणि या फसवणुक करणाऱ्यांचा धोका कमी करू शकता. सायबर गुन्हयामध्ये दरवर्षी १५ टक्के वाढ होते. २०२५ पर्यंत ५१०.५ ट्रिलीयनपर्यंत पोहचण्याची अपेक्षा आहे.

एक साधा क्लिक सर्व फरक करू शकतो. ऑनलाईन क्रिमीनल रियल क्राईम या मोहीमेने अधोरेखित केले आहे की, ऑनलाईन गुन्हा इतर कोणत्याही प्रकारच्या गुन्हयाइतका गंभीर आहे. ऑनलाईन स्वच्छता वैयक्तिक स्वच्छतेइतकीच महत्वाची आहे. बि–केअरफुल असणे आवश्यक आहे.

भारतात तेलंगणा राज्यात सायबर फसवणुकांच्या उद्देशाने मानवी तस्करीच्या पहिला गुन्हा नोंदविला.

डिपार्टमेट ऑफ जस्टीस (DOJ) सायबर क्राईमला तिन भागात विभागते.

१) ज्या गुन्हयामध्ये संगणकीय उपकरण लक्ष्य आहे. उदा. नेटवर्क प्रवेश मिळविण्यासाठी.

२) ज्या गुन्हयामध्ये संगणकाचा वापर शस्त्र म्हणून केला जातो. उदा. डिनायल ऑफ सर्व्हिस (DOS) हल्ला सुरू करण्यासाठी.

३) ज्या गुन्हयामध्ये संगणकाचा वापर एखाद्या गुन्हयासाठी एक्सेसरी म्हणून केला जातो. उदा. बेकायदेशिरपणे मिळविलेला डेटा संचयीत करण्यास संगणक वापरणे.

विविध पोलीस एजन्सीशी संवाद साधण्यासाठी IRU हा एक स्टॉप सोल्युशन असेल जेणेकरून पिडीतांना FIR दाखल करता येईल. सायबर क्राईम तक्रारीकरीता १९३० वर कॉल करून तक्रार देऊ शकता. हा राष्ट्रीय हेल्पलाईन नंबर आहे तसेच भारतीय सायबर अपराध समन्वय केंद्र (14C) च्या वेबसाईटवर दर्ज करू शकता.

राष्ट्रीय हेल्पलाईन नंबर १५५२६०

टोल फ्री नंबर १८००–११–४००० किंवा १९१५ कॉल करून एजेंट सोबत बोलून आपली तक्रार देऊ शकतो. यात ७ वर्षाची शिक्षा आहे व हा जमानती अपराध आहे.

चोरी गेलेले पैसे वापर होऊ शकतो. ऑनलाईन आर्थिक फसवणुक झाल्यास https://www.cybercrime.gov.in किंवा पोलीसठाणेत गुन्हा दाखल करता येते व ही तक्रार तीन दिवसाच्या आत करावी.

कायदा :–

इलेक्ट्रॉनिक दस्तऐवजांना कायदेशिर मान्यता आणि ई–फायलिंग आणि ई–कॉमर्स व्यवहारांना समर्थन देण्यासाठी एक फ्रेमवर्क प्रदान करते आणि सायबर गुन्हे कमी करण्यासाठी तपासण्यासाठी कायदेशिर फ्रेमवर्क देखील प्रदान करते माहिती तंत्रज्ञान कायदा २००० (IT Act 2000) आणि त्यात ९ सप्टेंबर २०२४ मध्ये सुधारणा करण्यात आली. सायबर गुन्हयाविरूध्दच्या लढयात राष्ट्रीय स्तरावर नोडल पाईंट म्हणून काम करण्यासाठी गृहमंत्रालयाच्या (MHA) अंतर्गत इंडियन सायबर क्राईम कोआर्डिनेशन सेंटर (14C) ची स्थापना करण्यात आली. समन्वित आणि सर्वसमावेशक पध्दतीने सायबर गुन्हयांचा सामना करण्यासाठी व्यासपीठ उपलब्ध करून देणे हे उद्दिष्ट आहे.

सायबर गुन्हयास शिक्षा :–

कलम ५०४ IPC – २ वर्ष कारावास दंड किंवा दोन्ही

कलम ५०६ – २ वर्ष कारावास दंड किंवा दोन्ही. मृत्यू किंवा गंभीर दुखापत इ. धमकी असल्यास ७ वर्षापर्यंत दंड किंवा दोन्ही

भारत सरकारच्या गृहमंत्रालयातर्फे मोबाईल वरती जनजागृती सुरू केलेली असून हेल्पलाईन नंबर दिल्या जाऊन सावधानतेच्या सुचना दिलेल्या आहे. १९३० राष्ट्रीय सायबर सेल नंबर असून अनोळखी व्हिडीओ कॉल किंवा फोन येत असल्यास सावधानतेच्या सुचना दिल्या जातात व मोठया स्तरावर सायबर गुन्हेगारीवर संशोधन सुरू आहे.

संदर्भ ग्रंथ सूची :–

१) भारतातील महिलांविरूध्दचे सायबर गुन्हे, देबारती हालदर, के. जयशंकर https://mr.wikipedia.org

२) सायबर सुरक्षा पुस्तिका, प्रकाशक– बुलढाणा जिल्हा पोलीस दल

३) सायबर गुन्हे कथा – कविता दातार