'RESEARCH JOURNEY' International E- Research Journal
Issue - 291C : Recent Trends in Humanities, Commerce & Management and Science & Technology. Peer Reviewed Journal
E-ISSN : 2348-7143
April : 2022

सायबर गुन्हेगारी : दक्षता व उपाययोजना

प्रा. डॉ. दिलीप आर. चव्हाण
समाजशास्त्र विभाग
ज.जि.म.वि.प्र.सह समाजाचे कला, वाणिज्य व विज्ञान महाविद्यालय, जळगाव

प्रस्तावना –

आजचे युग हे माहिती व तंत्रज्ञानाचे युग आहे. आपण 'इन्फॉरमेशन (Information) युगात' रहातो. संगणक, मोबाईल, फोन, डिजिटल कॅमेरे आणि इतर इलेक्ट्रोनिक्स गॅझेट आपल्या दैनंदिन जीवनाचा अविभाज्य भाग बनले आहेत. दररोजच्या जीवनातील विविध पैलूंमधील तंत्रज्ञानाचा आणि इंटरनेटचा वाढता वापर यामुळे सायबर अपराधी बऱ्याच मोठ्या प्रमाणावर नागरिकांवर हल्ले करत आहेत. माहिती तंत्रज्ञानाचा वापर गैरप्रकारासाठी आणि गुन्हेगारीसाठी केला जातो. त्यास 'सायबर गुन्हा' असे म्हणतात पांढरपेशीय गुन्हेगारीतील हा एक नवा प्रकार आहे. आधुनिक काळात संपूर्ण जगात सायबर गुन्ह्यांच्या संख्येत प्रचंड वाढ होत आहे. भारतात देखील या गुन्हेगारीचे प्रमाण वाढलेले आहे. सायबर गुन्ह्यात दुसऱ्याच्या बेकायदेशीर फाईल्स, प्रोग्रॅम, माहिती चोरणे, पासवर्ड मिळवून पैसे कमविणे, माहिती आणि ज्ञान चोरणे याचा अंतर्भाव होतो. सायबर गुन्हे हे उच्च वर्गातील लोक करतात. आधुनिक काळात तर क्रीप्टोकरन्सी सारखे घोटाळे होत आहेत. हा देखील सायबर गुन्हेगारीचाच प्रकार आहे.

उद्दिष्ट्ये – प्रस्तुत संशोधन पेपरच्या अनुषंगाने खालील उद्दिष्ट्ये निश्चित करण्यात आले आहे.

१) सायबर गुन्हेगारीबाबत व सुरक्षेबाबत माहिती जाणून घेणे.
२) सायबर गुन्ह्यांच्या संदर्भात समकालीन गुन्ह्यांचे स्वरूप जाणून घेणे.
३) सायबर गुन्ह्यांचे स्वरूप लक्षात घेवून त्यानुसार उपाययोजना राबविणे.

शोधनिबंधाचे गृहीतके –

१) सायबर गुन्हेगारी विघातक स्वरूपात वाढत आहे.
२) तंत्रज्ञानाच्या वाढत्या वापरामुळे व माहितीच्या अभावामुळे गुंतागुंतीचे गुन्हे निर्माण होत आहेत.
३) उच्च शिक्षित आणि संगणकाचे ज्ञान आहे, असे उच्च वर्गातील लोक हे गुन्हे करतात.

संशोधन पद्धती – प्रस्तुत शोधनिबंध लेखनासाठी वर्णनात्मक व विश्लेषणात्मक अभ्यास पद्धतीचा अवलंब करण्यात आला आहे. तसेच दुय्यम स्त्रोतांचा वापर करण्यात आलेला असून विविध विचारवंतांनी आपापल्या ग्रंथात व्यक्त केलेल्या विचारांचा आधार घेतलेला आहे. याशिवाय वर्तमानपत्रे, नियतकालिके व इंटरनेटवर उपलब्ध असणाऱ्या प्रकाशित माहितीचा आधार घेतला आहे.

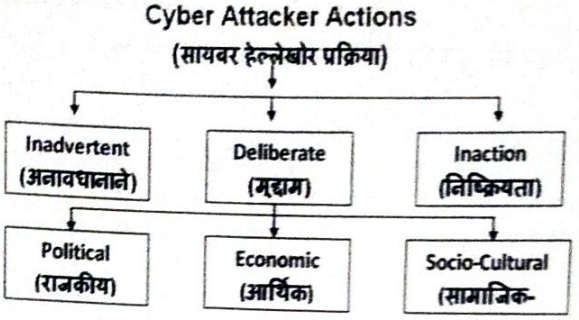
सायबर गुन्ह्याचा अर्थ व स्वरूप – सायबर गुन्हा किंवा संगणकीय गुन्हा ही संज्ञा संगणक व इंटरनेटशीअसणाऱ्या या प्रत्यक्ष गुन्ह्यात संगणकाचा प्रामुख्याने वापर असणाऱ्या गुन्ह्याला उद्देशून वापरला जातो. सायबर गुन्हे विशेष करून हॅकिंग, प्रताधिकार, बाललैंगिक चित्रण इ. स्वरूपात दिसून येतात. याशिवाय व्यक्तिगत किंवा गोपनीय माहिती चोराने किंवा फोडणे हे देखील सायबर गुन्ह्यात मोडते. माहिती तंत्रज्ञानाच्या प्रकाराबरोबर सायबर गुन्हेगारीमध्ये लक्षणीय वाढ झालेली दिसून येते.

अर्थ –

१) इंटरनेटद्वारे केल्या जाणाऱ्या गैरवापरास सायबर क्राईम म्हटले जाते.
२) सायबर स्पेसचे साधन वापरून केलेले कोणतेही बेकायदेशीर कृत्य म्हणजे सायबर गुन्हा होय.

इंटरनेट आणि सोशल मिडीयाने आपल्या दैनंदिन जीवनात मोठ्या प्रमाणात आक्रमण केले आहे. संगणकीय क्षेत्रात सायबर क्राईमचा झालेला शिरकाव हा अनेक अनर्थ व संकटाना आमंत्रण देणारा आहे. साधारणतः सर्वसामान्य नागरिकांचा असा समज आहे की, सायबर क्राईमशी आपला काही संबंध नाही. या समजुतीमुळे नागरिक सायबर क्राईमबाबत अनभिज्ञ आहेत. परंतु जरा सूक्ष्म विचार करून पाहिले तर आपल्याला रोजच या सायबर क्राईमचा सामना करावा लागतो. आपल्या ई-मेलवर सॅम मेल येत असतात, मोबाईलवर अनावश्यक कॉल, मेसेजेस येतात. नेट बँकिंग अकाउंट असेल तर त्याचा पासवर्ड, आय. डी. हॅक होतो. हे सर्व प्रकार सायबर गुन्हेगारीशी मोडतात. संगणक, इंटरनेट यांच्या माध्यमातून एखाद्या व्यक्ती, संस्था आदींच्या संगणक प्रणालीमध्ये शिरून त्यातील माहिती चोरणे, त्याचा गैरवापर करणे, व्हाटसअप पाठविणे, मेलद्वारे फसवणूक, धमकी देणे, खंडणी मागणे अशा कारवायांना सायबर क्राईम म्हणता येईल. परंतु सायबर क्राईमची व्याप्ती व तंत्र हे रोज बदलत असल्याने त्याला विशिष्ट अशा रचनेत वा संकल्पनेत बसविणे थोडे जिकरीचे आहे.

सारांश, आज जगातील प्रत्येक क्षेत्र, व्यवसाय इंटरनेटने प्रभावित झालेला दिसून येतो. इंटरनेटच्या या मायाजालाचा हॅकर अतिशय क्लुप्तीने गैरवापर करतात. सायबर क्राईममधील आजची व उद्याची आव्हाने रोज नव्या स्वरूपात, नव्या आकारात व नव्या शस्त्रासह पुढे येत आहे. आज भारतात हॅकिंग, पोर्नोग्राफी व डाटा थेफ्ट स्वरूपाचे गुन्हे आयटी सेक्शनखाली नोंदवले जातात. तथापि यात व्यापकता येऊन सायबर क्राईमखाली येणारे सर्व गुन्हे आयटी सेक्शनखाली नोंदविणे महत्वपूर्ण ठरेल.



सायबर गुन्ह्याचे प्रकार (Types of Cyber Crime) – सायबर गुन्हे करण्याचे अनेक प्रकार आहेत. वैयक्तीक स्वरूपातील संवेदनशील माहितीची चोरी किंवा परस्पर देवाणघेवाण, आर्थिक फसवणूक (फिशिंग, स्पूर्फिंग), हॅकिंग (डीनायल ऑफ सर्व्हिस), अश्लील मजकूर म्हणजे सायबर गुन्हेगारीच्या भाषेत पोर्नोग्राफी, कॉपीराईट व बौद्धिक संपदा हक्कांचे उल्लंघन असे सायबर गुन्ह्याचे प्रकार आहेत. यांची सविस्तर चर्चा पुढीलप्रमाणे –

१) हॅकिंग (Hacking) – **ही एक सोपी संज्ञा आहे. जी इतर कोणत्याही संगणकावर किंवा नेटवर्कला बेकायदेशीर सुचना पाठवण्याची व्यवस्था करते** – कोणत्याही संगणक, संगणक प्रणालीमध्ये अनधिकृत केलेला प्रवेश म्हणजे 'हॅकिंग' आणि तो करणारा 'हॅकर' सायबर गुन्ह्यामध्ये हॅकिंग किंवा हॅकर या दोन संज्ञा वारंवार पुढे येतात. ई-कॉमर्स साईटवर हॅकिंगचे प्रमाण अधिक आहे. इंटरनेटचा चुकीचा वापर करून अनधिकृत माहिती मिळवली जाते. उदा. एखादी वेबसाईट किंवा कंप्युटर सिस्टम हॅक करून अनधिकृत माहिती चोरणे, खराब करणे, हॅकर्स नेहमी मोबाईल नेटवर्क हॅक करतात. प्रयेक वेळी हॅकिंग हे पैशांसाठीच केले जाते असे नव्हे तर अनेकदा समाजात निव्वळ अस्वस्थता निर्माण करण्यासाठी किंवा विकृत आनंद मिळविण्यासाठी केला जातो. काही वेळा राजकीय हेतूने एखाद्या नेत्याच्या घरी बेहिशेबी मालमत्ता सापडण्याची पोस्ट व्हायरल केली जाते.

२) बाल अश्लीलता आणि गैरवर्तन किंवा अनुचित गोष्टींचा किंवा अश्लील गोष्टींचा प्रादुर्भाव – जगभरात मुलांचा लैंगिक अत्याचार करण्यासाठी इंटरनेटचा वापर केला जात आहे. हा एक सायबर गुन्हेगारीचा प्रकार आहे. ज्यात बाल अश्लीलतेच्या उद्देशाने गुन्हेगार अल्पवयीन मुलांना चॅट रूम्सद्वारे विनवणी करतात. यालाच पोर्नोग्राफी असेही म्हणतात. अश्लील चित्रफिती, छायाचित्रे, मजकूर इंटरनेटद्वारे डाऊनलोड करणे, प्रसारित करणे, पाहणे असे प्रकार पोर्नोग्रफीमध्ये मोडतात. थोडक्यात, सोशल मिडीयावर किंवा वेबसाईटद्वारे कायद्याने बंदी असलेल्या गोष्टी दाखविणे यामध्ये चाईल्ड पोर्नोग्राफीचा क्सामावेश जास्त आहे. या बाबींमुळे लहान मुलांच्या मनावर विपरीत परिणाम होतात आणि यामुळे मुले चुकीच्या वळणार जातात.

३) चाची किंवा चोरी किंवा डेटा थेफ्ट – या प्रकारात सायबर गुन्हेगार एखाद्या संगणकातील माहिती पेनड्राईव्ह, डेटा बँक, सीडीचा वापर करून चोरतो. या माहितीचा गैरवापर होतो किंवा विकला जातो. जेव्हा एखादा व्यक्ती कॉपीराईटचे उल्लंघन करतो आणि संगीत, चित्रपट, गेम्स किंवा सॉफ्टवेअर डाऊनलोड करतो. तेव्हा हा गुन्हा होतो. चित्रपट निर्माते आणि दिग्दर्शक बऱ्याचदा या गुन्ह्याचा बळी ठरतात. कॉर्पोरेट क्षेत्रात अशा प्रकारचे गुन्हे वारंवार घडतात. दुसऱ्याच्या एटीएमचा वापर करून पैसे काढणे किंवा खरेदी करणे तसेच अकाऊन्टचा पासवर्ड चोरणे आणि त्याचा गैरवापर करणे.

४) व्हायरस अटॅक – एखाद्या संगणक प्रणालीत ई-मेल, चॅटींग याद्वारे व्हायरस पाठवून संगणक प्रणाली हॅकरच्या नियंत्रणाखाली आणली जाते. व्हायरसचे विविध प्रकार आहे. संगणक यंत्रणा बिघडवणे, ठप्प करणे, नियंत्रण बाह्य करण्यासाठी हे व्हायरस कार्यरत असतात. ट्रोजनसारख्या व्हायरसद्वारे जगाच्या कोणत्याही कोपऱ्यात बसून जगभरातील कोणत्याही संगणकावर नियंत्रण ठेवणे शक्य आहे. इतके याचे स्वरूप गंभीर आहे. प्रतिस्पर्धी राष्ट्रांतर्गत व्हायरस अटॅकचे प्रमाण वाढलेले आहे.

५) ई-मेल, एसएमएस, चॅटींग याद्वारे फसवणूक किंवा ई-मेलद्वारे त्रास देणे (Harassment via Emails) – या प्रकारच्या सायबर गुन्ह्यात आपल्याला ई-मेल येतो की, तुम्ही मोठी रक्कम जिंकली आहात तसेच आपणास लॉटरी लागली आहे आणि ती रक्कम तुमच्या पर्यंत पोहचवण्यासाठी काही खर्च (प्रोसेसिंग फी) आहे. ती तुम्ही आम्हाला तुमच्या बँक अकाउंटसह पाठवा. परंतु हे सर्व खोटे असते. अशा प्रकारचे मेल किंवा एसएमएस आपल्याला वारंवार येतात. हा 'नायजेरियन सायबर फ्रॉड' समजाला जातो.

६) सायबर स्टॉकिंग – इतरांच्या कामकाजावर ऑनलाईनरीत्या पाळत ठेवणे. हा एक प्रकारचा ऑनलाईन Pi आहे. ज्यामध्ये पिडीतेला ऑनलाईन संदेश किंवा ई-मेलच्या बॅरेजचा सामना करावा लागतो. तुमच्यावर लक्षपूर्वक पाळत ठेवून तुम्हा ई-मेल मोबाईल, वेब कॅमेरा, विडीयोद्वारे इंटरनेटचा वापर करून धमकी देण्यात येऊ शकते. ई-मेल अथवा फेसबुक, सोशल साईटद्वारा चॅटींग व सर्फिंगच्या माध्यमातून गुन्हेगार आपली संगणकीय ओळख (आय. डी.) पासवर्ड हॅक करतात. विशिष्ट व्हायरस आपल्या संगणकात डाऊनलोडसाठी पाठवून आपली संपूर्ण वैयक्तिक माहिती, संगणकात केल्या जाणाऱ्या सर्व क्रिया, बँक अकाउंट नंबर, पासवर्ड चोरून नागरिकांना मोठ्या प्रमाणात आर्थिक भुर्दंड सोसावा लागतो.

७) सायबर दहशतवाद – याला माहिती युद्ध म्हणूनही ओळखले जाते. ज्यात संगणक व्हायरस वापरून संगणक नेटवर्कमध्ये जाणीवपूर्वक आणि मोठ्या प्रमाणात हल्ले करणे किंवा मालवेयर वापरून शारीरिक हल्ले करणे, व्यक्ती, सरकार आणि संस्था यांच्यामध्ये दहशतीची भावना निर्माण करणे हे दहशतवादाचे उद्दिष्ट असते. २६/११ चा मुंबईतील अतिरेक्यांनी केलेला हल्ला सायबर तंत्राचा वापर करून केला होता. रशियाने जॉर्जियावर केलेला हल्ला हा देखील दहशतवादाचाच प्रकार होता इ.

८) मानहानी, निंदा (Defaniation) – ई-मेलद्वारे एखाद्या व्यक्तीचे नाव खराब केले जाते तेव्हा हा गुन्हा मानला जातो. सार्वजनिक ठिकाणचा फोटो एखाद्याने तुमच्या संमतीविना व जाणीवपूर्वक वाईट पद्धतीने फोटो काढला तर व तो फोटो सन्मानजनक नसेल आणि तुमची प्रतिष्ठा घालवणारा असेल तर तुमच्या गुप्ततेचा भंग होतो. तसेच एखाद्याचे मेल अकाउंट हॅक करून त्या अकाउंटमधून दुसऱ्या व्यक्तीला खराब किंवा अश्लील ई-मेल पाठविणे हा सायबर गुन्हा ठरतो.

९) क्रॅकिंग (Cracking) – एखाद्याच्या कंप्युटरमधील खाजगी माहिती किंवा फाईल्स चोरणे.

१०) उरीवळपस – दुसऱ्याच्या TMचा वापर करून त्यातून पैसे काढणे किंवा खरेदी करणे.

११) Cheating Fraud - दुसऱ्याच्या अकाउंटचा पासवर्ड चोरणे आणि त्याचा वापर करणे.

सायबर गुन्ह्याची कारणे – माहिती तंत्रज्ञानाच्या प्रसाराबरोबर सायबर गुन्ह्यांमध्ये लक्षणीय वाढ होताना दिसून येते. या गुन्ह्यांची कारणे पुढीलप्रमाणे

१) पैसा मिळवण्यासाठी किंवा कमी वेळात श्रीमंत होणे – सायबर गुन्हेगार नेहमीच पैसे कमविण्याचा सोपा मार्ग निवडतात. ते श्रीमंत लोक किंवा बँक, कॅसिनो किंवा वित्तीय संस्था सारख्या श्रीमंत संस्थांना लक्ष करतात.आर्थिक व्यवहार होतात व संवेदनशील माहिती हॅक करतात आणि त्याबदल्यात पैसे कमवतात किंवा माहिती विकतात. अशा गुन्हेगारांना पकडणे अवघड आहे. म्हणूनच जगभरातील सायबर गुन्ह्यांची संख्या वाढत आहे.

२) समाजात अस्वस्थता निर्माण करण्यासाठी – प्रत्येक वेळी हॅकिंग हे पैशांसाठीच केले जाते असे नव्हे तर अनेकदा समाजात निव्वळ अस्वस्थता निर्माण करण्यासाठी किंवा विकृत आनंद मिळविण्यासाठी केला जातो. काही वेळा राजकीय हेतूने एखाद्या नेत्याच्या घरी बेहिशेबी मालमत्ता सापडल्याची पोस्ट व्हायरल केली जाते. विविध आक्षेपार्ह व गुन्हेगारी स्वरूपाच्या पोस्ट टाकून समाजमन दुषित केले जाते.

३) चिथावणी देण्यासाठी – सोशल मीडियावर आक्षेपार्ह मजकूर फोटो किंवा चित्राची पोस्ट टाकणे, हा गुन्हा आहे. त्याशिवाय अन्य कोणीतरी पोस्ट टाकली आणि त्यामुळे कोणाच्या तरी भावना दुखावल्या जाऊ शकतात. त्यातून दोन समाजात तेढ निर्माण केले जाते. देशाची एकता आणि अखंडता सुरक्षितेच्या दृष्टीने व सार्वभौमत्वाला धक्का पोहोचणारी अथवा लोकांमध्ये दहशत पसरवणारी माहिती अनेकांना शेअर करणे गुन्हा आहे.

४) पेटीएम केवायसी करण्यासाठी – पेटीएम अद्ययावत करण्यासाठी केवायसीचा बहाणा करून सायबर गुन्हेगारांकडून नागरिकांना फोन, मेसेज व लिंक पाठवून आर्थिक फसवणूक केली जाते. दैनंदिन व्यवहारांसाठी पेटीएम व अन्य ई-वॅलेटचा सर्रास वापर होत असल्याने फोन, मेसेज किंवा लिंक पाठवून बँक खात्याची गोपनीय माहिती मिळवली जाते. त्यानंतर तुमच्या खात्यातील लाखो रुपये काही मिनिटातच लंपास केले जातात.

५) n **अपडेट करणे** – ॲप अद्यावत करावयाचे सांगून सायबर गुन्हे घडतात. जसे एनी डिस्क,टीमव्हीवर, क्विक सपोर्ट यासारखे मोबाईल प्लिकेशन डाऊनलोड करण्यास सांगून नंतर यूपीआयपीनसह एटीएम, क्रेडिट कार्डची गोपनीय माहिती विचारून आर्थिक फसवणूक केली जाते.

६) एखाद्या व्यक्तीची प्रतिष्ठा कमी करण्यासाठी – एखाद्या व्यक्तीच्या नकळत सार्वजनिक ठिकाणी फोटो काढून तिची छेडछाड करून त्या व्यक्तीला बदनाम करणे किंवा एखाद्या राजकीय व्यक्तीला बदनाम करण्यासाठी त्यांच्याकडे बेहिशेबी मालमत्तेचे घबाड सापडले, अशी पोस्ट टाकून राजकीय करिअर नष्ट करणे, यात त्याची समाजात प्रतिष्ठा कमी व्हावी हा हेतू असतो.

७) त्रास देण्यासाठी – ई-मेल किंवा फेसबुकवर मैत्री करून नंतर त्या व्यक्तीला त्रास दिला जातो. यात विशेष करून स्त्रियांना लक्ष्य केले जाते. त्यांचे इ-मेल अकाऊंट हॅक करून त्या अकाउंटमधून दुसऱ्या व्यक्तीला खराब किंवा अश्लील फोटो किंवा इमेल पाठविले जातात किंवा इतरांच्या कामकाजावर ऑनलाइनरित्या पाळत ठेवली जाते तसेच तुम्ही रक्कम जिंकला आहात लॉटरी लागली आहे.

८) सुरक्षा प्रणाली मिळवण्यासाठी – हॅकर क्सेस कोड, रेटिना प्रतिमा, प्रगत बोईस रेकॉर्डर इत्यादी चोरू शकतात. जे बायोमेट्रिक सिस्टीम सहजपणे मूर्ख बनवू शकतात. फायर वॉललाबायपास करून अनेक सुरक्षा प्रणाली मिळवण्यासाठी वापरता येऊ शकतात.

९) लापरवाही – दुर्लक्ष हे मानवी आचरणातील एक वैशिष्ट्य आहे. आपण संगणकाचा किंवा फेसबुकचा वापर करताना बऱ्याच वेळा अकाउंट बंद करण्याचे राहून जाते किंवा बऱ्याच वेळा आपण इतर कामात असल्यामुळे इतरांना आयडी व पासवर्ड देतो. त्याचा फायदा सायबर गुन्हेगार घेत असतात. तेव्हा संगणक प्रणालीकडे दुर्लक्ष करू नये.

१०) डेटा चोरणे व स्वतःच्या फायद्यासाठी वापरणे – संगणकात डेटा अगदी लहान जागेत संग्रहीत करण्याचे वैशिष्ट्य आहे. हे इतर कोणत्याही संचयनातून डेटा चोरणे आणि स्वतःच्या फायद्यासाठी त्याचा वापर करणे लोकांना अधिक सुलभ होतो. संशोधन कार्यामध्ये असे वांग्मयचौर्य मोठ्या प्रमाणात केले जाते.

११) दहशतवादी कारवाया घडवून आणण्यासाठी – आज माहिती तंत्रज्ञानामुळे जग फार जवळ आले आहे. आपला विचार किंवा प्रभाव निर्माण करण्यासाठी काही गुन्हेगार हे संगणकाचा किंवा संगणकप्रणाली व सॅटॅलाइटचा वापर करून आपल्या देशात बसून दुसऱ्या देशात आत्मघाती कृत्ये करतात. त्यामुळे माहिती तंत्रज्ञानाचा मानवाला जसा उपयोग झाला तसा काहींनी मानवी समाजाला धोका करण्यासाठी याचा वापर सुरू केलेला दिसून येतो. या सायबर दहशतवादातून अमेरिका देखील सूटली नाही .

अशा प्रकारे सायबर गुन्हेगारीची कारणे सांगता येतील.

दक्षता – शासन लोकांची फसवणूक होऊ नये म्हणून मोबाईलवर आणि टीव्हीवर वेळोवेळी सायबर सुरक्षेच्या बाबतीत सुचना देते. त्या सूचनांचे जनतेने काटेकोरपणे पालन केल्यास सायबर गुन्ह्यांचे प्रमाण कमी होऊन जनतेची होणारी फसवणूक टळू शकेल. डिजिटल व्यवहार करताना सजग राहणे आवश्यक आहे. कोणतीही बँक आपल्या खातेदारांकडून त्यांच्या बँक खात्याबद्दलची गोपनीय स्वरूपाची माहिती कधीही मागवीत नाही. आपण सावध राहिले पाहिजे. सायबर गुन्हेगाराला शिक्षा करण्यासाठी 'माहिती तंत्रज्ञान कायदा २००२' या कायद्यात विशेष तरतूद केली आहे.

सायबर सुरक्षेचे सात स्तर (7 Layers of Cyber Security)

१)	मानवी स्तर	The Human Layer
२)	परिमिती सुरक्षा	Perimeter Security
३)	नेटवर्क सुरक्षा	Network Security
४)	अंतिम विंदू सुरक्षा	Endpoint Security
५)	अनुप्रयोग सुरक्षा	Application Security
६)	डेटा सुरक्षा	Data Security
७)	मिशन क्रिटीकल असेटस	Mission Critical Assets

उपाययोजना –

१) आपला पिन व आयडी किंवा ओटीपी व पासवर्ड कोणत्याही व्यक्तीशी शेअर करू नका.
२) लॉग-इन करताना रिमेंबर पासवर्ड हे ऑप्शन अनचेक करा.
३) सार्वजनिक ठिकाणी किंवा कॉमन कॉम्प्युटरवरून तुमचे ई-मेल किंवा अन्य संकेतस्थळांना भेट दिल्यानंतर ब्राउझिंग हिस्ट्री आणि कुकीज डिलीट करण्यास विसरू नका.
४) चॅट करताना कुठलीही महत्त्वाची माहिती टाईप करू नका. वेब कॅमेरा काम झाल्यानंतर बंद करा किंवा झाकून ठेवा.
५) दर दोन ते तीन आठवड्यांनी तुमचे पासवर्ड बदला. पासवर्डमध्ये तुमचा फोन नंबर, जन्मतारीख घरातल्या लोकांची नावे यांचा वापर टाळावा.
६) सर्वात महत्त्वाचे म्हणजे आपल्या बँक खात्यासंदर्भातील कोणतीही माहिती मोबाईल डिव्हाइसमध्ये स्टोअर करू नका.जसे खाते क्रमांक, डेबिट आणि क्रेडिट कार्ड पिन आपल्या मोबाईलमध्येस्टोअर करू नये.
७) मोबाईलच्या 'स्क्रीन लॉक'चा वापर करा. ऑनलाईन बँकिंगचा वापर करताना स्क्रीन लॉकचा वापर करावा.
८) इंटरनेट वापरताना आपला आयडी क्रमांक, नेट बँकींग अकाऊंट क्रमांक, पासवर्ड क्रमांक अथवा आपली वैयक्तिक माहिती उघड करताना सावधानता बाळगावी.
९) आपली संगणक सिस्टीम ऍन्टी व्हायरस, फायरवॉलने सुरक्षित ठेवावी. स्पॅम मेल,फसवे मेल यावर डबल क्लिक करून उघडण्याचा प्रयत्न करू नये. फसवे मेल डिलीट करणे हाच मोठा प्रतिबंधात्मक उपाय ठरतो.
१०) ऑनलाइन बँकिंग करताना संकेतस्थळे सुरक्षित असल्याची खात्री करा. ऑनलाईन व्यवहार होताक्षणी लॉग आऊट करा.
११) जातीय द्वेष, हिंसा, निंदानालस्ती, अपप्रचार, टिंगल, अफवा अशा स्वरूपाचे व आशयाचे मेसेजेस पोस्ट करू नका. अथवा फॉरवर्ड देखील करू नका. कोणाबद्दलही आक्षेपार्ह पोस्ट सोशल मीडियावर प्रदर्शित करू नका.
१२) डेटा सुरक्षेसाठी पीन लॉक किंवा फिंगर प्रिंट लॉकचा वापर करा.
१३) जो ईमेल आयडी बँक खाते, पैशाचे देवाणघेवाणीसाठी वापरतात,त्याचा वापर सोशल मीडियावर करू नका
१४) डेटा सुरक्षित ठेवण्यासाठी कोणतीही वेबसाईट वापरल्यानंतर लॉग आऊट नक्कीच करा.
१५) ब्राउजरचा वापर केल्यानंतर तुमची माहिती ब्राउजरमधून डिलीट करत चला. शिवाय पासवर्ड कधीही सेव करू नका.

अशाप्रकारे सायबर गुन्हेगारी संदर्भात दक्षता घेता येईल व आपली होणारी फसवणूक टाळता येईल.

संदर्भ

१) Nina Godbole Sumit Belpure, Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives, Wiley.
२) Cyber Security R180521
३) Anti Hacker Tool Kit (Indian Edition) by Mike Shema, Publication MC Graw Hill.
४) Computer Forensics Kruse, Warren and Jay Heiser Addison Wesley, 2002.
५) भारतीय समाज : प्रश्न आणि समस्या, प्रा. डॉ. प्रदीप आगलावे, श्री साईनाथ प्रकाशन, नागपूर
६) दै. लोकमत, दै. दिव्य मराठी, दै. सकाळ वर्तमानपत्रे
७) www.cybercellmumbai.gov.in