eISSN 3139-2377

RESEARCH WORK
A Monthly, Open Access, Peer Reviewed International Research Journal
Volume 02, Issue 01, January 2026

साइबर अपराध की डरावनी उपस्थिति

डॉ0 ऋचा सिंह राठौर[1], डॉ0 कुमारेन्द्र सिंह सेंगर[2]
सहायक प्राध्यापक, रक्षा अध्ययन विभाग, गांधी महाविद्यालय, उरई (जालौन)
सहायक प्राध्यापक, हिन्दी विभाग, गांधी महाविद्यालय, उरई (जालौन)

Received: 20 Jan 2026 Accepted & Reviewed: 25 Jan 2026 Published: 30 Jan 2026

Abstract

आज कम्प्यूटर, इंटरनेट का उपयोग बहुत तेजी से हो रहा है। व्यक्तिगत कार्यों से लेकर शासकीय कार्यों तक में इसकी सहायता ली जाती है। इंटरनेट की इस दुनिया में अपराधियों के द्वारा न केवल व्यक्तिगत अपराध किये जा रहे हैं बल्कि वे सरकारी तंत्र पर भी हमलावर हैं। सामान्य भाषा में हम इंटरनेट के ज़रिए किए जाने वाले अपराधों को साइबर क्राइम कह सकते हैं। कोई भी ऐसा आपराधिक कार्य, अवैध कार्य, अवांछनीय कार्य जो कम्प्यूटर, इंटरनेट अथवा संचार माध्यम से सम्बद्ध है, वह साइबर क्राइम है। कम्प्यूटर, इंटरनेट के माध्यम से वित्तीय धोखाधड़ी, हैकिंग, सॉफ़्टवेयर की चोरी, किसी अन्य कम्प्यूटर नेटवर्क पर हमला, पोर्नोग्राफी को बढ़ावा, आंतरिक सूचनाओं और बौद्धिक संपदा की चोरी, डिजिटल अरेस्ट आदि को साइबर अपराध कहा जाता है। साइबर अपराध और अपराधी बहुत ही ख़ामोशी से हमारे बीच अपनी घुसपैठ बनाने में लगे हैं। जहाँ हमारी एक लापरवाही हमें साइबर अपराधी का शिकार बना सकती है वहीं हमारी सतर्कता ही इससे बचाव है। ऐसे ही साइबर अपराध, उनके रूपों और उनसे बचने के लिए अपनाई जा रही अनेक विधियों, तरीकों आदि के बारे में प्रस्तुत शोध–पत्र में प्रकाश डालने का प्रयास किया गया है।

कीवर्ड– साइबर क्राइम, कम्प्यूटर, इंटरनेट, साइबर कानून, धोखाधड़ी, सुरक्षा, साइबर सुरक्षा नीति

Introduction

वर्तमान में कम्प्यूटर और इंटरनेट के माध्यम से काम बहुत आसान हुआ है। सूचना प्रौद्योगिकी के विकास के साथ–साथ साइबर अपराधों में वृद्धि से इनकार नहीं किया जा सकता है। कम्प्यूटर और इंटरनेट ने सूचना एवं प्रौद्योगिकी में अपराधियों का प्रवेश करा दिया है। तकनीकी क्षमता से संपन्न इस दौर में अपराधियों ने अपराध करने का नया तरीका साइबर माध्यम को बनाया है। सामान्य भाषा में इंटरनेट के ज़रिए किए जाने वाले अपराधों को साइबर अपराध अथवा साइबर क्राइम कहते हैं। कोई भी ऐसा आपराधिक, अवैध, अवांछनीय कार्य जो कम्प्यूटर, इंटरनेट अथवा संचार माध्यम से सम्बद्ध है, वह साइबर अपराध है। उदाहरणार्थ यदि कम्प्यूटर, इंटरनेट के माध्यम से वित्तीय धोखाधड़ी, बैंक खाते से धन चुराना, हैकिंग, अश्लीलता का प्रसार, वायरस का फैलाव, सॉफ़्टवेयर की चोरी, दोषपूर्ण सॉफ़्टवेयर भेजकर कम्प्यूटर को ख़राब करना, किसी अन्य कम्प्यूटर नेटवर्क पर हमला, पोर्नोग्राफी को बढ़ावा, आंतरिक सूचनाओं और बौद्धिक संपदा की चोरी, डिजिटल अरेस्ट आदि को साइबर अपराध कहा जाता है।

साइबर अपराध के रूप– सामान्य रूप में 'साइबर अपराधों में हैकिंग, चोरी, साइबर स्टॉकिंग, पहचान चुरा लेना, वायरस सॉफ्टवेयर, साइबर स्पाइंग, सोशल मीडिया से फोटो चुराना, साइबर बुल्लयिंग'[1] आदि को माना जाता है। इसके पीछे अपराधी का मंतव्य सूचनाओं की चोरी, वित्तीय धोखाधड़ी, कम्प्यूटर सिस्टम को

eISSN 3139-2377
RESEARCH WORK
A Monthly, Open Access, Peer Reviewed International Research Journal
Volume 02, Issue 01, January 2026

नष्ट करना आदि होता है। कॉपीराइटेड फिल्में, गेम, सॉफ्टवेयर अथवा गाने आदि डाउनलोड करके व्यक्तिगत कार्यों में उनका उपयोग करना भी साइबर अपराध है। इसी तरह किसी व्यक्ति द्वारा अपने लक्षित व्यक्ति को उसके नम्बर पर फोन करके, उसका पीछा करके, उसे मैसेज करके तंग करना साइबर स्टॉकिंग कहा जाता है। यह भी एक तरह का साइबर अपराध है।

साइबर अपराध के रूप में सबसे महत्त्वपूर्ण और रोचक तथ्य ये है कि इंटरनेट का उपयोग करने वाले लगभग प्रत्येक व्यक्ति द्वारा कभी न कभी, कोई न कोई साइबर अपराध अवश्य किया गया होता है। ये और बात है कि कई बार ऐसा अपराध कानूनी नहीं तो नैतिक अपराध में शामिल हो जाता है। आश्चर्यजनक ये है कि हममें से अधिकतर को ऐसे अपराध करने के बाद भी इसका अंदाजा तक नहीं होता है। कहीं से कोई भी चित्र, लेख या वीडियो को कॉपी–पेस्ट करना ऐसे अपराध की श्रेणी में आता है। इंटरनेट पर ऐसे तमाम काम हैं, जो साइबर क्राइम के तहत आते हैं।[2] किसी लेख, कहानी, कविता, फोटो, संगीत की धुन, सॉफ्टवेयर, वीडियो, किताब, ई–बुक को बिना इजाजत के इंटरनेट पर डालना अपराध की श्रेणी में आता है। इसी तरह किसी और का फोटो उसकी लिखित मंजूरी के बिना अपने फेसबुक प्रोफाइल पर पोस्ट करना भी साइबर अपराध है। गूगल इमेज या दूसरी इमेज होस्टिंग वेबसाइट से अपनी पसंद का कोई फोटो लेकर उसे अपने ब्लॉग, सोशल नेटवर्किंग, वेबसाइट या पत्र–पत्रिका में इस्तेमाल करना भी साइबर अपराध में आता है। किसी लोगो की चोरी करना, वाई–फाई का दुरुपयोग करना, किसी दूसरे का अकाउंट खोलकर देखना, पायरेटेड सॉफ्टवेयर का उपयोग करना, गूगल पर फ्रॉड क्लिक करना भी साइबर अपराध समझा जाता है। साइबर अपराध मामलों में इधर एक अलग तरह का अपराध दिखाई देने लगा है। यह एक तरह का घोटाला है जिसमें जिसमें धोखेबाज खुद को पुलिस या सरकारी अधिकारी बताकर लोगों को डराते हैं कि उन्होंने कोई अवैध गतिविधि की है। धोखेबाज वीडियो कॉल पर नकली गिरफ्तारी वारंट और सबूत दिखाकर, पीड़ित को पैसे ट्रांसफर करने या संवेदनशील जानकारी देने के लिए मजबूर करते हैं। अपराध की दुनिया में इसे डिजिटल अरेस्ट के नाम से जाना जाता है।

साइबर युद्ध अथवा साइबर वारफेयर अन्य देशों के खिलाफ युद्ध के कार्यों को संचालित करने के लिए साइबरस्पेस का उपयोग है। 'भूमि, महासागर, वायु और अंतरिक्ष के बाद साइबरस्पेस को युद्ध का पाँचवाँ आयाम माना जाता है। दरअसल, पेंटागन और नाटो ने हवा, जमीन और समुद्र की तरह ही साइबरस्पेस को भी 'ऑपरेशनल डोमेन' के रूप में नामित किया है।'[3]

भारत में साइबर अपराध – दुनिया में इंरटनेट उपयोग में लगातार वृद्धि है, जिसके चलते साइबर अपराध में भी वृद्धि हो रही है। भारत भी इससे अछूता नहीं रहा है। 'झारखंड राज्य में स्थित एक जिले का नाम जामताड़ा है। इस जिले को भारत में होने वाले प्रत्येक साइबर क्राइम का गुनाहगार माना जाता है। भारत में 80 प्रतिशत साइबर क्राइम का कारण इस जिले में रहने वाले लोगों को माना जाता है। ऐसा बताया जाता है कि जामताड़ा में रहने वाले इन लोगों ने साइबर क्राइम की शुरुआत साल 2013 से की थी। यह लोगों को एक फोन कॉल के जरिए ठग लिया करते थे।'[4]

'भारत में इंटरनेट उपयोगकर्ताओं की संख्या 560 मिलियन से अधिक है जो पूरे विश्व में दूसरा सबसे बड़ा इंटरनेट और ऑनलाइन नेटवर्क है और भारत इस मामले में केवल चीन से पीछे है।'[5] 'राष्ट्रीय अपराध रिकॉर्ड ब्यूरो के अनुसार वर्ष 2021 में भारत में साइबर अपराध के 52,974 मामले दर्ज किये गए जो वर्ष

eISSN 3139-2377
RESEARCH WORK
A Monthly, Open Access, Peer Reviewed International Research Journal
Volume 02, Issue 01, January 2026

2020 (50,035 मामले) की तुलना में 5 प्रतिशत से अधिक की और वर्ष 2019 (44,735 मामले) की तुलना में 15 प्रतिशत से अधिक की वृद्धि को दर्शाते हैं।'[6] राष्ट्रीय अपराध रिकॉर्ड ब्यूरो की 2023 में जारी रिपोर्ट के अनुसार भारत में कुल अपराधों में 7.2 प्रतिशत की वृद्धि (वर्ष 2022 की तुलना में 6.24 मिलियन से अधिक मामले) दर्ज की गई।[7]

'सीईआरटीइन (इंडियन कम्प्यूटर इमरजेंसी रिस्पांस टीम) के आँकड़ों के अनुसार 2022 में भारत में सबसे अधिक साइबर क्राइम के मामले दर्ज किए गए हैं। सीईआरटी साइबर सुरक्षा हमलों से निपटने के लिए केन्द्र सरकार की एक नोडल एजेंसी है जो सूचना प्रौद्यौगिकी मंत्रालय के तहत काम करती है। 2022 के पहले दो महीनों में 2,12,285 मामले दर्ज किए गए हैं।'[8]

भारत में तीन चौथाई इंटरनेट उपभोक्ता किसी न किसी तरह साइबर अपराध का शिकार होते हैं और इस लिहाज से भारत को सर्वाधिक प्रभावित देश माना जाता है। सुरक्षा समाधान उपलब्ध कराने वाली फर्म 'सिमैन्टक ने अपने एक अध्ययन में निष्कर्ष निकालते हुए बताया है कि वैश्विक स्तर पर लगभग 65 फीसदी इंटरनेट उपयोक्ता साइबर क्राइम के शिकार होते है। जबकि भारत में यह संख्या 76 प्रतिशत है।'[9] भारत में साइबर अपराध की घटनाएं वर्ष 2022 में 10.29 लाख से बढ़कर वर्ष 2024 में 22.68 लाख हो गई।[10] भारत के सबसे पसंदीदा डिजिटल भुगतान मोड यूनिफाइड पेमेंट्स इंटरफेस (यूपीआई) को भी धोखाधड़ी वाले मोबाइल नंबरों का उपयोग करने वालों द्वारा निशाना बनाया गया है।

डिजिटल अरेस्ट साइबर स्कैम का सबसे नवीन रूप है जिससे वर्ष 2024 में 92,000 से अधिक भारतीय प्रभावित हुए हैं। पिछले कुछ वर्षों में शिकायतों की संख्या में उल्लेखनीय वृद्धि हुई है, वर्ष 2021 में 1,35,242, वर्ष 2022 में 5,14,741 और वर्ष 2023 में 11,31,221 शिकायतें दर्ज की गई हैं।[11] अभी हाल ही में देश के सर्वोच्च न्यायालय ने डिजिटल अरेस्ट के मामलों में सख्ती से निपटने का आदेश दिया है। इसे एक चौंकाने वाला बताते हुए जस्टिस सूर्यकांत ने कहा, 'यह चौंकाने वाली बात है कि देश भर में पीड़ितों, जिनमें वरिष्ठ नागरिक भी शामिल हैं, से 3000 करोड़ रुपये से ज्यादा वसूले गए हैं।'[12] भारतीय साइबर अपराध समन्वय केंद्र ने डिजिटल अरेस्ट के लिए इस्तेमाल किए गए 3,962 से अधिक स्काइप आईडी और 83,668 व्हाट्सएप अकाउंट को सक्रिय रूप से पहचाना और उन्हें ब्लॉक किया।[13]

साइबर विधि– वैश्विक स्तर पर सभी देशों ने साइबर अपराधियों को नियंत्रित करने के संबंध में अनेक कानून बनाये हैं जिससे साइबर अपराधियों को पकड़ने और उन्हें दंडित करने की प्रक्रिया तेजी से विकसित हो रही है। भारत सरकार ने साइबर अपराधों से निपटने के लिए सूचना प्रौद्यौगिकी अधिनियम 2000 पारित किया था, साथ ही आईपीसी की धाराओं में भी कुछ प्रावधान किए गए हैं। 'सूचना प्रौद्यौगिकी अधिनियम 2000 की धाराएँ 43, 43ए, 66, 66बी, 66सी, 66डी, 66ई, 66एफ, 67, 67ए, 67बी, 70, 72, 72ए हैकिंग तथा साइबर क्राइम से संबंधित हैं।'[14]

'सूचना तकनीक क़ानून के अंतर्गत मामलों के निष्पादन के लिए धारा 46 का प्रावधान किया गया है। मामलों के निष्पादन का अधिकार सचिव, सूचना प्रौद्योगिकी को दिया गया है, जो इस क़ानून की धारा 46 और 47 के अंतर्गत मुआवज़े या क्षतिपूर्ति की राशि का निर्धारण करेगा।'[15] देश में विभिन्न साइबर अपराधों के लिए अलग–अलग कानूनी धाराएँ और उन्हीं के अनुसार सजा का प्रावधान किया गया है।

eISSN 3139-2377
RESEARCH WORK
A Monthly, Open Access, Peer Reviewed International Research Journal
Volume 02, Issue 01, January 2026

'भारत में सूचना प्रौद्योगिकी अधिनियम 2000 की विविध धाराओं के तहत साइबर अपराधियों के खिलाफ कार्यवाई की जा रही है। सूचना प्रौद्योगिकी अधिनियम 2000 की कुछ धाराओं में संशोधन भी किया गया है ताकि अपराधियों के विरुद्ध और सहजतापूर्वक कार्यवाही की जा सके। 'धारा 69ए के तहत पुलिस को अधिकार है कि किसी भी वेबसाइट को ब्लॉक कर सकती है।'[16] 'भारत में जुलाई 2009 में दिल्ली में देश के प्रथम साइबर रेग्यूलेटरी कोर्ट का सुभारंभ किया गया।'[17] यहाँ साइबर अपराधियों की सुनवाई होगी।

इसके अलावा 2013 में सरकार ने राष्ट्रीय साइबर सुरक्षा नीति जारी की, जिसमें अतिसंवेदनशील मुद्दों के संरक्षण को लेकर मसौदा तैयार किया गया। इसके तहत 'दो वर्ष की सजा से लेकर उम्रकैद, दंड और जुर्माने का प्रावधान है। वर्ष 2020 में गृह मंत्रालय ने साइबर अपराधों से निपटने के लिए भारतीय अपराध समन्वय केन्द्र का उद्घाटन किया।'[18] राष्ट्रीय साइबर सुरक्षा नीति का उद्देश्य भारतीय साइबरस्पेस को सुरक्षित करना और सभी क्षेत्रों में साइबर खतरों से इसको मजबूत करना है। इसके द्वारा साइबर सुरक्षा प्रदान करते हुए कंप्यूटर, सर्वर, मोबाइल डिवाइस, इलेक्ट्रॉनिक सिस्टम, नेटवर्क और डेटा को साइबर हमलों से बचाया जाता है।

देश में विभिन्न साइबर अपराधों के लिए अलग–अलग कानूनी धाराएँ और उन्हीं के अनुसार सजा का प्रावधान किया गया है। 'हैकिंग, डेटा की चोरी, वायरस–स्पाईवेयर फैलाना, पहचान की चोरी, ई–मेल स्पूफिंग और फ्रॉड, पोर्नोग्राफी, चाइल्ड पोर्नोग्राफी, बौद्धिक संपदा उल्लंघन, तंग करना आदि को साइबर अपराध माना जाता है। अपराध साबित होने पर उसके प्रकार और गम्भीरता के अनुसार तीन साल से लेकर दस साल तक की कारावास और/या पचास हजार रुपये से लेकर दस लाख रुपये तक जुर्माने का प्रावधान है।'[19]

साइबर अपराध को कम करने हेतु सुझाव

वर्तमान दौर में इंटरनेट, मोबाइल, कंप्यूटर आदि ने ऐसी व्यवस्था निर्मित कर दी है कि बिना इनके किसी काम के बारे में विचार भी नहीं किया जा सकता है। बैंकिंग हो, व्यापार हो, शिक्षा हो, सेवा हो, संचार हो अथवा कोई अन्य क्षेत्र हो सभी में इनका उपयोग सहजता के साथ हो रहा है। ऐसे में साइबर अपराध होने की सम्भावना इसलिए भी और बढ़ जाती है क्योंकि इंटरनेट के अत्यंत विशाल और सबके लिए खुले नेटवर्क में प्रविष्ट होने से किसी को रोका नहीं जा सकता है। इसी स्वतंत्रता के चलते आपराधिक, आतंकी मानसिकता के लोगों द्वारा न केवल व्यक्तियों को परेशान किया जाता है बल्कि सरकारों के लिए भी संकट उत्पन्न कर दिया जाता है।

व्यक्तियों को अपने सिस्टम को लगातार अपडेट करते रहने की आवश्यकता है। इसके लिए अपने सॉफ्टवेयर और ऑपरेटिंग सिस्टम को नवीनतम स्थिति में बनाये रखा जाना चाहिए। इसके साथ–साथ कंप्यूटर अथवा मोबाइल में एंटी–वायरस का भी उपयोग करना चाहिए। इसके द्वारा अवांछित रूप से वायरस के हमले को रोका जा सकता है। साइबर अपराध के क्षेत्र में बैठा अपराधी तकनीकी ज्ञान से समृद्ध होता है। उसके द्वारा लगातार प्रयास किया जाता है कि लक्षित व्यक्ति के खातों, सेवाओं आदि के पासवर्ड को तोड़ा जा सके। ऐसे में व्यक्ति की जिम्मेवारी बनती है कि वह अपने खातों, सेवाओं से सम्बंधित पासवर्ड मजबूत बनायें। अपने निकट परिचित का नाम, जन्मतिथि आदि को पासवर्ड बनाये जाने से बचना चाहिए। इसके अलावा अपने पासवर्ड को समय–समय पर बदलते भी रहना चाहिए।

eISSN 3139-2377
RESEARCH WORK
A Monthly, Open Access, Peer Reviewed International Research Journal
Volume 02, Issue 01, January 2026

साइबर अपराधियों द्वारा विभिन्न तरह की ई–मेल भेजकर भी आकर्षक उपहार, योजनाओं, सेवाओं आदि के बारे में बताते हुए प्रलोभन दिए जाते हैं। उनसे बचाव ही सुरक्षा है। किसी अनजान ई–मेल को, स्पैम ई–मेल को खोलने से बचना चाहिए। इसी तरह वित्तीय संस्थानों की, शैक्षिक संस्थानों की, वाणिज्यिक संस्थानों की तरह से दिखने वाली वेबसाइट के द्वारा भी साइबर अपराधी अपना काम कर जाते हैं। जल्दबाजी अथवा लापरवाही में हर एक वेबसाइट को क्लिक करने से बचना चाहिए।

वर्तमान दौर में छोटे से छोटा अथवा बड़े से बड़ा वित्तीय लेनदेन डिजिटल माध्यम से होने लगा है। इसे लेकर भी अतिशय जागरूकता की आवश्यकता है। सार्वजनिक वाई–फाई का उपयोग करने से बचना चाहिए। डिजिटल लेनदेन करने के समय सुरक्षित नेटवर्क को वरीयता देनी चाहिए। स्वयं अपने वाई–फाई नेटवर्क को अथवा सिस्टम के नेटवर्क को सार्वजनिक बनाये जाने से बचना चाहिए। इसके माध्यम से भी साइबर अपराधी सिस्टम तक पहुँच बनाकर नुकसान पहुँचा सकते हैं।

यह बात सभी को समझना चाहिए कि कानून में डिजिटल अरेस्ट जैसी कोई अवधारणा नहीं है। लोगों के साथ ऐसी स्थिति उनके स्वयं के घबराने के कारण उत्पन्न होती है। यदि किसी भी तरह से कोई कहता है कि आप अब डिजिटल अरेस्ट में हैं तो व्यक्ति को तत्काल फोन काट देना चाहिए, कम्प्यूटर बंद कर देना चाहिए और पुलिस से शिकायत करनी चाहिए। इसके लिए 1930 नंबर पर भी रिपोर्ट की जा सकती है।

साइबर अपराधों को रोकने के लिए सरकारें लगातार प्रयत्नशील हैं। उनकी द्वारा अनेक कदम उठाकर न केवल सरकारी संगठनों, सेवाओं की सुरक्षा की जा रही है बल्कि व्यक्तिगत स्तर पर भी आम जनमानस को भी सहायता प्रदान की जा रही है। चूँकि वर्तमान दौर में प्रत्येक हाथ में मोबाइल है, इंटरनेट है और उसका उपयोग भी बहुत तेजी से हो रहा है, ऐसे में आम जनसामान्य को बहुत अधिक सतर्क, समझदार होने की आवश्यकता है। सामान्य व्यक्ति की एक लापरवाही, एक गलती से साइबर अपराधी को अवसर मिल जाता है और वह किसी भी स्तर का संकट पैदा कर देता है, किसी भी तरह का नुकसान कर देता है। सरकारी स्तर पर राष्ट्रीय सुरक्षा के लिए अनेकानेक राष्ट्रीय एजेंसियाँ कार्यरत हैं मगर व्यक्तिगत स्तर पर एक–एक व्यक्ति स्वयं सजग रहकर ही साइबर अपराध से बच सकता है।

नागरिकों के साथ–साथ प्रशासन को भी आवश्यक कदम उठाये जाने चाहिए, जिससे कि नागरिकों के हितों की सुरक्षा हो सके और साइबर अपराधियों के हौसले पस्त हों। इसके लिए ई–वाणिज्य और ई–प्रशासन को बढ़ाने देने के लिए पुलिस एवं उपकरणों को प्रशिक्षित करके इस योग्य बनाया जाये कि वे साइबर अपराध की जाँच कर सकें। पुलिस में कम्प्यूटर के क्षेत्र अधिकारियों एवं कर्मचारियों को प्रशिक्षित करके इस अपराध से निपटने के योग्य बनाना चाहिए। उनको शोषित व्यक्ति के प्रति सहानुभूति दर्शाते हुए दोस्ताना एवं मधुर वार्तालाप बनाये जाने को भी प्रेरित किया जाना चाहिए।

साइबर अपराधों से सम्बंधित मामलों के निपटारे के लिए ई–अदालत का गठन किया जाना चाहिए, जिसमें कम्प्यूटर सम्बन्धी अपराध के जानकारों का सहयोग लिया जाना चाहिए। कानून के साथ ही साथ कम्प्यूटर, प्रौद्योगिकी के क्षेत्र में वकीलों को भी प्रशिक्षित किया जाना चाहिए, ताकि वे इन अपराधों से निपटने की अच्छी तरह से पैरवी कर सकें। व्यावहारिकता के सन्दर्भ में, सामाजिक क्षेत्र में सक्रिय रहते समय अथवा किसी तरह का फीडबैक देते समय अपना ई– मेल, मोबाइल नंबर प्रत्येक व्यक्ति को नहीं दिया जाना चाहिए। यदि इस सम्बन्ध में किसी भी प्रकार की कोई परेशानी हो तो तत्काल पुलिस को जानकारी देना

eISSN 3139-2377
RESEARCH WORK
A Monthly, Open Access, Peer Reviewed International Research Journal
Volume 02, Issue 01, January 2026

चाहिए। असंदिग्ध ईमेल या अपराध का स्वरूप दर्शाते हुए ऑनलाइन अथवा आवेदन पर अपना विवरण देते हुए पुलिस को शिकायती आवेदन–पत्र देना आवश्यक है। इस प्रकार के ईमेल के जबाव देने से बचना चाहिए।

इंटरनेट हमारे दैनिक जीवन का एक अभिन्न अंग बन गया है। सरकारी, गैर–सरकारी, सामाजिक, सांस्कृतिक, साहित्यिक, व्यापारिक, राजनैतिक आदि सहित रोजमर्रा के छोटे–छोटे कार्य इसके माध्यम से संपन्न किये जा रहे हैं। यह व्यक्ति के दैनिक जीवन का अभिन्न अंग बन गया है। यह भी एक तरह का समाज बन गया है जहाँ प्रत्येक मानसिकता के लोग रह रहे हैं। यहाँ भले लोग भी हैं तो आपराधिक प्रवृत्ति के लोग भी हैं। ऐसे में साइबर अपराधियों से बचने के हम सबको ही सतर्क रहने की आवश्यकता है। लापरवाही से बचने की जरूरत है। कुछ सुरक्षात्मक उपायों को अपनाये जाने की आवश्यकता है। यदि प्रशासन एवं आम जनता इस सन्दर्भ में दिए जाते सुझावों पर अमल करती है तो निश्चित ही इन अपराधों और समस्याओं से बचा जा सकेगा।

सन्दर्भ सूची

1- deepawali.co.in/cyber-crime-kya-hai-hindi-types.html
2- http://navbharattimes.indiatimes.com/tech/tips-and-tricks/cyber-crime/articleshow/16195432.cms
3- idsa.in/jds/cybersecurity-and-threats-15-2-2021
4- deepawali.co.in/cyber-crime-kya-hai-hindi-types.html
5- societalaffairs.com/bharat-mein-cyber-apradh
6- pravakta.com/bells-growing-cyber-crime
7- https://www.drishtiias.com/hindi/daily-updates/prelims-facts/crime-in-indiaA2023-report
8- patrika.com/Bhopal-news/highest-cyber-crime-in-india-7549350
9- drishtiias.com/hindi/daily-updates/daily-news-editorials/indias-cyber-ecosystem
10- https://www.pib.gov.in/PressReleasePage.aspx?PRID=2176342
11- https://www.drishtiias.com/hindi/daily-updates/daily-news-analysis/rising-digital-arrests
12- https://navbharattimes.indiatimes.com/india/digital-arrest-scam-supreme-courts-strict-stance-concern-over-3000-crore-fraud/articleshow/125059834.cms
13- https://www.pib.gov.in/PressReleasePage.aspx?PRID=2111002
14- patrika.com/Bhopal-news/highest-cyber-crime-in-india-7549350
15- http://www.chauthiduniya.com
16- pravakta.com/e-governance-in-the-era-of-the-growing-impact-of-cyber-crime
17- lbid
18- patrika.com/Bhopal-news/highest-cyber-crime-in-india-7549350
19- navbharattimes.indiatimes.com/techarticleshow/16312721.cms