

# साइबर क्राइम : एकांतता का अंत का अंतरजाल



पृथ्वी, जल और आकाश तीनों क्षेत्रों में अपराधों का विस्तार हुआ है। अपराधियों की पहुँच सभी स्थानों पर है। सरकार कोई कानून बनाती है, उसके पहले उसका 'तोड़' निकाल लिया जाता है। कम्प्यूटर के विकास होने से सूचना एवं प्रौद्योगिकी का क्षेत्र भी अपराधों और अपराधियों की पहुँच से बाहर नहीं है। यह चोरी प्रकाश में होने लगी है। की- बोर्ड पर बैठा व्यक्ति हाथ में एक 'माऊस' लेकर उतना नुकसान पहुँचा सकता है जितना 'बम और तोप' भी नहीं पहुँचा सकते हैं।

साइबर क्राइम क्या है ?

-----

आज मानव जीवन कम्प्यूटर से जुड़ा हुआ है। इस क्षेत्र के अपराध क्या-क्या हो सकते हैं, इसे जानना प्रत्येक व्यक्ति के लिए आवश्यक है। कोई भी आपराधिक कृत्य जो कम्प्यूटर अथवा संचार साधनों से जुड़ी है, साइबर क्राइम की श्रेणी में आता है। उदाहरण के लिये 'कम्प्यूटर के माध्यम से वित्तीय धोखाधड़ी, पहचान की चोरी, हैकिंग, अश्लील संदेश संप्रेषण, टेलिफोन तकनीक का दुरुपयोग, राष्ट्रविरोधी गतिविधियाँ, वायरस का फैलाव, निजी हित में कम्प्यूटर का उपयोग, कंपनी नीति के विरुद्ध गतिविधि, कम्प्यूटर नेटवर्क पर आक्रमण को प्रोत्साहन, आंतरिक और गुप्त सूचनाओं की चोरी, बौद्धिक संपदा की चोरी, आदि गतिविधियाँ व कार्यकलाप साइबर अपराध की श्रेणी में आती हैं।

डाटा और सूचना दो चीजें हैं। डाटा कम्प्यूटर में भंडारित रहते हैं और सूचना डाटा के आधार पर संप्रेषित रिपोर्ट की जाती है। साइबर आपराधिक गतिविधियाँ डाटा से जुड़ी होती हैं और वे अपने पीछे इलेक्ट्रॉनिक साक्ष्य छोड़ जाती है। साइबर क्राइमों की जांच के लिये 'कम्प्यूटर फॉरेंसिक' एक सक्षम विधा है जो विश्वस्तर पर विकसित हो रही है। इसमें आई.टी. और कम्प्यूटर क्षेत्र के विशेषज्ञ लोग रहते हैं।

कम्प्यूटर नेटवर्क से संबंधित अपराध : इस श्रेणी में मुख्य रूप से हैकिंग, सेकिंग, ई-मेल के माध्यम से धमकी देना, अज्ञात ई-मेल, मोबाइल फोन पर अश्लील संदेश देना, वायरस, आदि शामिल हैं। वित्तीय धोखाधड़ी : इस श्रेणी में डिजिटल डाटा से खिलवाड़, वित्तीय संस्थाओं जैसे बैंक, कार्यालय आदि की डाटा को गलत ढंग से प्राप्त करना मुख्यतः इस अपराध में आते हैं। बौद्धिक संपदा की चोरी : इस श्रेणी में पेटेंट प्रोडक्ट की चोरी, साफ्टवेयर पाइरेसी, म्यूजिक पाइरेसी आदि शामिल है। गैर साइबर अपराधों में कम्प्यूटर का उपयोग : इस श्रेणी में वैसे अपराध आते हैं जो मुख्य रूप से प्रोनोग्राफी से संबंधित है। इसमें कम्प्यूटर के माध्यम से राष्ट्रविरोधी व समाज विरोधी कार्यकलाप भी शामिल हैं। मोबाइल और टेलिफोन के माध्यम से जो वायरस या गलत संदेश प्रसारित किये जाते हैं वे भी साइबर क्राइम की श्रेणी में आते हैं।

बहुत से साइबर अपराध, कंप्यूटर का प्रयोग करके किये जाते हैं पर उनका लक्ष्य कंप्यूटर या सर्वर नहीं होता है। इस तरह के अपराधों को मुख्यतः निम्न श्रेणी में बांटा जा सकता है –

### साइबर आतंकवाद

---

साइबर गतिविधियों के द्वारा धार्मिक, राजनैतिक उन्माद पैदा करना साइबर आतंकवाद के अन्दर आता है। यह किसी भी देश की आंतरिक सुरक्षा को समाप्त कर सकता है।

### आर्थिक अपराध

---

इस समय अधिकतर बैंक का काम अन्तरजाल पर हो रहा है। व्यापार भी अन्तरजाल पर हो रहा है। क्रेडिट कार्ड से गलत तरह से पैसा निकाल लेना। ऑनलाइन व्यापार या बैंकिंग में धोखाधड़ी करना – यह सब आर्थिक अपराध की श्रेणी में आता है।

### फिशिंग

---

अक्सर कुछ ऐसे ईमेल मिलते हैं जिससे प्रतीत होता है कि वे किसी बैंक में या किसी अन्य संस्था की वेब साइट से हैं। यह आपके बैंक के खाते या अन्य व्यक्तिगत सूचना पूछने का प्रयत्न करते हैं। ये सारी ई-मेल फर्जी हैं और यह आपकी व्यक्तिगत सूचना को जानकर कुछ गड़बड़ी पैदा कर सकते हैं। इसे फिशिंग कहा जाता है। इस तरह की ईमेल का जवाब न दें।

### साइबर छल

---

अक्सर ई-मेल, एसएमएस मिलते हैं कि भेजने वाली विधवा है जिसके पति का बहुत सारा पैसा फंसा हुआ है और वह पैसा निकालने में आपकी सहायता चाहती है। इस तरह के भी ईमेल या एसएमएस आते हैं कि आपके ई-मेल या फोन नम्बर ने करोड़ों की लॉटरी जीत ली है, जिसे पाने के लिए सम्पर्क करें। यह सब फर्जी होता है। यह धोखाधड़ी कर, आपको फसाना चाहते हैं। यह साइबर अपराध है और इस पर कभी भी अमल नहीं करना चाहिए।

### साइबर जासूसी

---

इसे एडवेयर या स्पाईवेयर भी कहा जाता है। आपके कंप्यूटर में कभी आपकी अनुमति से कभी बिना अनुमति के स्थापित हो जाते हैं। यह आपकी गतिविधियों की आपकी व्यक्तिगत सूचना एकत्र कर, अन्य को देते हैं। जिसके द्वारा वे स्थापित किये जाते हैं। यह हमेशा आपके कंप्यूटर को धीमा भी कर देते हैं।

### पहचान की चोरी

---

किसी व्यक्ति द्वारा किसी व्यक्ति की पहचान चोरी करना या उसका इलेक्ट्रॉनिक हस्ताक्षर को हैक करना

या किसी अन्य के नाम से फर्जी काम करना ,पहचान की चोरी कहलाता है। अपने पास वर्ड में नम्बर तथा तथा वर्णमाल दोनो का प्रयोग करें। उसे बदलते रहें। किसी को न बतायें।

## स्पैम

---

स्पैम माने अनचाही ई-मेल। यह भी साइबर अपराध है। हिन्दी चिट्ठाजगत में, यह काफी है। अक्सर चिट्ठाकार बन्धु आपको अपनी चिट्ठी भेज कर उनकी चिट्ठियों को पढ़ने के लिये कहते हैं। यह गलत है। आप इस तरह का ईमेल तभी किसी व्यक्ति को भेजें जब उस व्यक्ति से आप उस चिट्ठी में कुछ करने के लिये कहते हैं या उसके बारे में लिखते हैं। यह न केवल अन्तरजाल शिष्टाचार के विरुद्ध है पर साइबर अपराध भी है।

## स्पिम

---

यदि स्पैम अनचाहे ई-मेल है तो स्पिम अन्तरजाल के बातों के दौरान अनचाही बातें।

## अन्तरजाल पर पीछा करना

---

पीछा करना, तंग करना, इस हद तक घूरना कि दूसरा खीज जाये, डर जाय। यही काम जब अन्तरजाल पर हो तो साइबर स्टॉकिंग कहलाता है।

## अश्लीलता

---

अश्लील ईमेल, अश्लील चित्र, चित्रों को बदल कर किसी अन्य का चित्र लगा देना, यह सब अश्लीलता के अन्दर आता है। इस तरह के साइबर अपराध सबसे अधिक हैं। विचारणीय है कि क्या अन्तरजाल, एकांतता का अन्त है ?

## साइबर विधि

---

साइबर अपराधियों को पकड़ने और दंडित करने की प्रक्रिया भी तेजी से विकसित हो रही है। सभी देशों में कानून बनाये गये हैं। भारत में इनफारमेशन टेक्नोलॉजी एक्ट 2000 की विभिन्न धाराओं के तहत साइबर अपराधियों के विरुद्ध कार्रवाई की जा रही है। आई.टी.एक्ट 2000 की कुछ धाराओं में 2008 में संशोधन भी किया गया है ताकि अपराधियों के विरुद्ध और सहजतापूर्वक कार्रवाई की जा सके। धारा 69-ए के तहत पुलिस को यह अधिकार है कि किसी भी वेबसाइट को ब्लाक कर सकती है। इंडियन कॉपीराइट एक्ट के तहत भी साइबर अपराधियों के विरुद्ध कार्रवाई की जा रही है। साइबर फारसेनिक विशेषज्ञों को और भी सशक्त करने की दिशा में चिंतन भी किया जाना चाहिए क्योंकि इस क्षेत्र के अपराधी अपराध के नये-नये तरीके अपना लिये हैं। देश के कई बड़े शहर जैसे बैंगलुरु, हैदराबाद, लखनऊ, मुंबई, दिल्ली, चेन्नई आदि में साइबर थाने खोले गये हैं। पुलिस को उचित प्रशिक्षण देने के उपरान्त इन थानों में पदस्थ किया जाता है।

भारत में जुलाई 2009 में दिल्ली में देश के प्रथम साइबर-रेग्युलेशन कोर्ट का शुभारम्भ किया गया जहाँ साइबर अपराधों की सुनवाई होगी। साइबर अपराधों की रोकथाम की दिशा में यह उल्लेखनीय कदम है। साइबर क्राइम में भारत, चीन, ब्राजील, कनाडा आदि देशों में बेतहाशा वृद्धि हुई है। भारत में 'कॉल सेंटर' के कारण साइबर क्राइम की संख्या में वृद्धि हो रही है। सन् 2000 में साइबर क्राइम में भारत का स्थान विश्व में 14वां था। इन अनंत अपराधों पर नियंत्रण आवश्यक है। इसके लिये आवश्यक है कि साइबर लॉ का पालन कठोरता से किया जाये और दंड के प्रावधानों का प्रचार-प्रसार किया जाये।

साइबर क्राइम में कंप्यूटर का प्रयोग या तो हथियार के रूप में किया जाता है या वह टारगेट रहता है। इसे टूट कंप्यूटर और वाई द कंप्यूटर भी कहा जा सकता है। इन अपराधों के पीछे मुख्य मूल उद्देश्य है लालच, बदला और गुप्त सूचनाओं को प्राप्त करना होता है। कई बार स्टाकर्स ई-मेल संख्या प्राप्त कर तरह-तरह के प्रलोभन देकर अपना जाल फैलाते हैं और ब्लेमेल भी करते हैं। अतः अपना नाम, ई-मेल, दूरभाष संख्या हर किसी को नहीं देना चाहिए। यदि परेशानी आये तो पुलिस को सूचित करना चाहिए। कई बार 'लॉटरी' के माध्यम से भी निजी जानकारियां मांगी जाती हैं। कई बार नौकरी और वित्तीय लाभ देने का भी प्रलोभन अपराधियों द्वारा दिया जाता है। उस प्रकार के ई-मेल के रिसपाण्ड करने से बचना चाहिए। यदि किसी के एकाऊंट में कहीं से पैसा आता है तो तत्काल सम्बन्धित वित्तीय संस्था से संपर्क करना चाहिए। प्राप्त ई-मेल अथवा अपराध का स्वरूप दर्शाते हुए ऑन लाइन अथवा आवेदन पत्र पर अपना विवरण देते हुए पुलिस को शिकायती आवेदन पत्र देना आवश्यक है, जिसमें प्राप्त संदेश का पूर्ण विवरण हो।

---

प्राध्यापक, शासकीय दिग्विजय कालेज  
राजनांदगांव, मो.9301054300