

एकूण पृष्ठे: २१

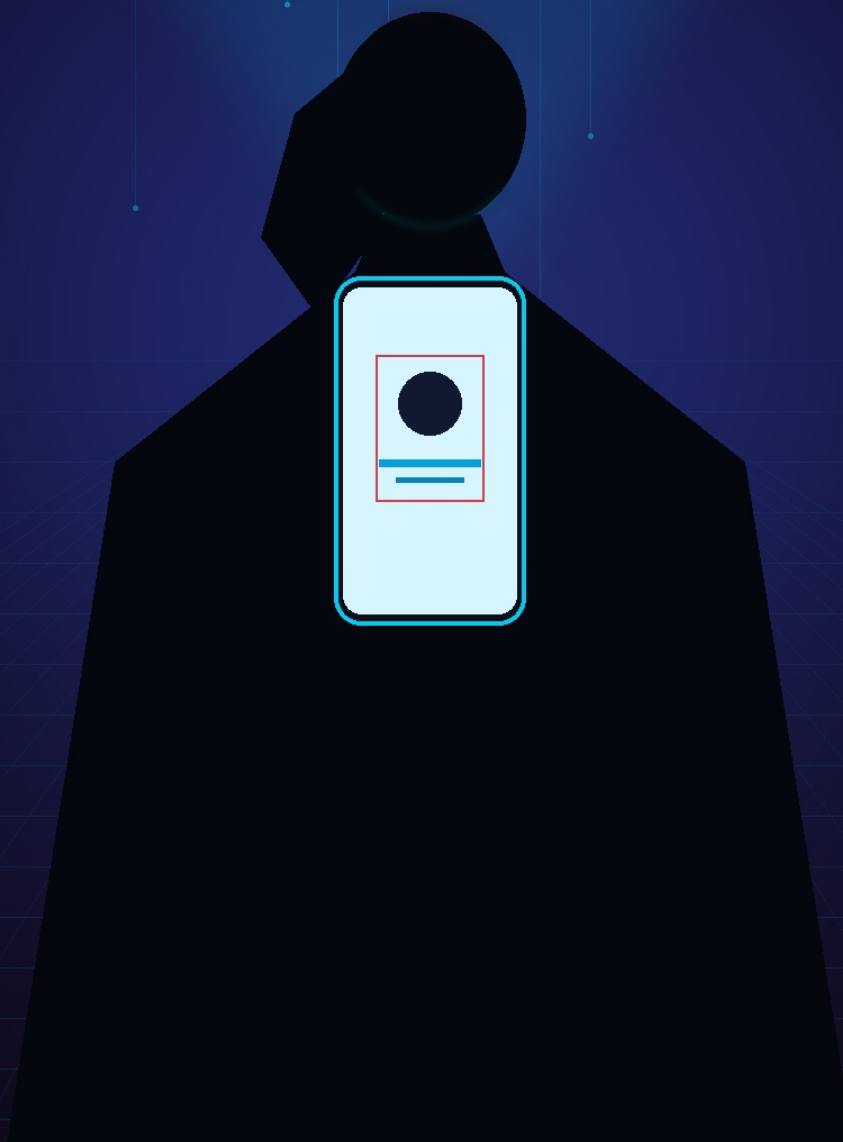
निःशुल्क जनहित आवृत्ती

सायबर-गुन्हेगारी व मानसशास्त्रीय सस्पेन्स कादंबरी

अनफॉलो

स्क्रीनमागचा अदृश्य चेहरा

एका चुकीच्या क्लिकने बदललेलं संपूर्ण आयुष्य...



लेखक

धवल हिरपरा

एकूण पृष्ठे: २१ | निःशुल्क जनहित संस्करण | २०२६

लेखक धवल हिरपरा यांचा परिचय व शोध-प्रक्रिया

धवल हिरपरा (Dhaval Hirapara) हे आधुनिक डिजिटल विश्वातील गुन्हेगारी, मानसिक संघर्ष, सोशल मीडियाचा मानवी वर्तनावरील प्रभाव आणि सायबर-सुरक्षा विषयांचे प्रदीर्घ अभ्यासक व लेखक आहेत. गेली अनेक वर्षे त्यांनी भारतीय तरुणाईमधील वाढत्या इंटरनेट व्यसनाधीनतेचा आणि सायबर गुन्हेगारांकडून रचल्या जाणाऱ्या आधुनिक जाळ्यांचा सखोल अभ्यास केला आहे. त्यांचे लेखन केवळ कल्पनाविलास नसून, वास्तविक फॉरेंसिक तपास, सायबर क्राईम सेलच्या नोंदी आणि प्रत्यक्ष पीडितांच्या मनोविश्लेषणावर आधारलेले असते.

'अनफॉलो: स्क्रीनमागचा अदृश्य चेहरा' या थरारक कादंबरीचे लेखन करण्यासाठी लेखकाने मुंबई, नवी मुंबई आणि पुण्यातील विविध सायबर सेलच्या गोपनीय तपासांचा संदर्भ घेतला आहे. आधुनिक काळात कृत्रिम बुद्धिमत्ता (AI), डीपफेक अल्गोरिदम आणि डार्क वेब हॅकिंग टूल्सचा गैरवापर करून निष्पाप कॉलेज तरुणींना प्रेमाच्या खोट्या आभासात कसे ओढले जाते, याचे धक्कादायक वास्तव मांडणे हा या पुस्तकाचा मुख्य उद्देश आहे.

लेखकाचा प्रामाणिक उद्देश:

"जेव्हा एखादी मुलगी स्मार्टफोनच्या स्क्रीनवर हसते, तेव्हा तिच्या एका क्लिकवर तिचे आयुष्य उध्वस्त करण्याचे षडयंत्र रचले जात असते. हे पुस्तक केवळ मनोरंजनासाठी नसून प्रत्येक तरुणाईसाठी आणि पालकांसाठी एक संरक्षणात्मक डिजिटल ढाल ठरावे, हीच माझी भावना आहे."

लेखकाचे अधिकृत संपर्क व माहिती स्रोत:

सदर पुस्तकाचे अधिकृत पोर्टल: <https://dhavalhirapara.com/>

ई-बुक डाउनलोड अधिकृत लिंक: <https://dhavalhirapara.com/ebook>

सोशल मीडिया कम्युनिटी: Instagram / Facebook @dhavalhirapara1995

माहितीचे अधिकृत स्रोत: CERT-In सायबर मार्गदर्शक तत्त्वे, राष्ट्रीय सायबर गुन्हे नोंदणी पोर्टल (cybercrime.gov.in), फॉरेंसिक अभ्यास अहवाल.

कायदेशीर अस्विकरण व वैधानिक सूचना (Mandatory Legal Disclaimer)

१. ऐतिहासिक, सायबर व तपासात्मक माहितीची स्थिती:

प्रस्तुत पुस्तक हे सायबर गुन्हेगारी आणि मानसोपचारशास्त्रावर आधारलेले एक नाट्यमय सादरीकरण (Dramatic Adaptation) आहे. या पुस्तकातील पात्रे, संवाद, ठिकाणे आणि संस्थांची नावे ही संपूर्णपणे काल्पनिक स्वरूपात मांडण्यात आली आहेत. प्रत्यक्ष घडलेल्या कोणत्याही जिवंत अथवा मृत व्यक्तीशी, तसेच चालू असलेल्या पोलीस तपासाशी याचा संबंध आढळल्यास तो केवळ योगायोग समजावा. सायबर गुन्हेगारीची कार्यपद्धती समजावून सांगताना गुन्हेगारी कृत्यांना प्रोत्साहन देणे हा हेतू नसून, नागरिकांना सतर्क करणे हाच सर्वोच्च हेतू आहे.

२. तांत्रिक, कायदेशीर व आर्थिक धोरणांची व्याप्ती:

या कादंबरीमध्ये उल्लेख करण्यात आलेली तांत्रिक माहिती, डिजिटल सुरक्षा टिप्स आणि कायदेशीर उपाय (उदा. IT Act 2000 च्या तरतुदी) हे केवळ सामान्य जनजागृती आणि माहितीच्या उद्देशाने दिलेले आहेत. वाचकांनी कोणतीही सायबर फसवणूक अथवा ब्लॅकमेलिंग झाल्यास स्वतः कायदेशीर सल्लागार, अधिकृत पोलीस यंत्रणा किंवा स्थानिक सायबर क्राईम सेलशी संपर्क साधावा. पुस्तकातील घटनांच्या आधारे घेतलेल्या कोणत्याही वैयक्तिक वा न्यायालयीन निर्णयाची जबाबदारी लेखक किंवा प्रकाशकावर राहणार नाही.

३. गोपनीयता, संवेदनशील डेटा व ओळख संरक्षण:

या पुस्तकात कोणत्याही व्यक्तीचा वास्तविक संवेदनशील डेटा, गोपनीय पासवर्ड, अधिकृत ओळख क्रमांक, बँक खाते क्रमांक अथवा व्यक्तिगत संपर्क क्रमांक छापण्यात आलेला नाही. पुस्तकात उदाहरणादाखल वापरण्यात आलेले सर्व आयडी व कोड डमी (उदा. [XXXX-XXXX-XXXX]) स्वरूपाचे आहेत. वाचकांच्या गोपनीयतेचा आदर राखणे आणि माहिती तंत्रज्ञान कायद्याच्या सर्व नियमांचे पालन करणे हे लेखकाचे सर्वोच्च कर्तव्य मानले गेले आहे.

४. बौद्धिक संपदा आणि पुनर्प्रकाशन हक्क:

या पुस्तकातील सर्व साहित्य, कथानक, मांडणी आणि रचना यावर लेखक धवल हिरपरा यांचे संपूर्ण बौद्धिक संपदा हक्क (Copyright © 2026) राखीव आहेत. कोणत्याही व्यक्तीस, संस्थेस अथवा डिजिटल मंचास लेखकाच्या पूर्वपरवानगीशिवाय या पुस्तकाचा कोणताही भाग व्यावसायिक कारणांसाठी वापरता येणार नाही. मात्र, शैक्षणिक आणि जनजागृतीच्या उद्देशाने विनामूल्य वाटप करण्यास पूर्ण अनुमती आहे.

वैधानिक दक्षता सूचना:

सायबर गुन्हेगारी संबंधित कोणत्याही संशयास्पद हालचाली आढळल्यास त्वरित भारत सरकारच्या राष्ट्रीय सायबर क्राईम हेलपलाइन १९३० वर संपर्क साधावा किंवा cybercrime.gov.in वर रीतसर तक्रार नोंदवावी.

प्रस्तावना: डिजिटल दुनियेतील सावल्या आणि ६ मोठे लाभ

आपण अशा एका युगात जगत आहोत जिथे माणसाचा श्वास जेवढा महत्त्वाचा आहे, तेवढाच त्याचा स्मार्टफोन आणि इंटरनेट कनेक्शन! सकाळी उठल्यापासून रात्री झोपेपर्यंत आपण हजारो अनोळखी चेहऱ्यांना लाईक्स देतो, त्यांच्या रील्स पाहतो आणि कधीकधी नकळतपणे अशा अनोळखी खात्यांशी भावना जोडतो. मुंबईच्या एका नामांकित कॉलेजमध्ये शिकणाऱ्या अनघा नावाच्या निष्पाप मुलीची ही कहाणी आहे, जिने सोशल मीडिया इन्फ्लुएन्सर बनण्याच्या नादात एका अज्ञात प्रोफाईलवर आंधळा विश्वास ठेवला.

हे पुस्तक वाचल्यानंतर वाचकांच्या जीवनात घडणारे ६ प्रमुख सकारात्मक बदल व लाभ:

- १. **सोशल मीडियाच्या मायाजाळाची खरी ओळख:** बनावट प्रोफाईल्स, बॉट्स आणि हॅकर्सची छुपी कार्यपद्धती ओळखण्याची अचूक दृष्टी मिळेल.
- २. **सायबर ग्रुमिंग (Cyber Grooming) पासून पूर्ण संरक्षण:** प्रेमाच्या गोड बोलण्यातून तरुणाईला कसे जाळ्यात अडकवले जाते, याचे मानसशास्त्रीय विश्लेषण समजेल.
- ३. **डीपफेक आणि मॉर्फिंगचा धोका ओळखणे:** एआय टूल्सद्वारे एखाद्याचे छायाचित्र किंवा व्हिडिओ कसा बनावट बनवला जातो आणि त्यापासून स्वतःचा डेटा कसा सुरक्षित ठेवावा, याचे ज्ञान.
- ४. **ब्लॅकमेलिंगच्या संकटात घाबरण्याऐवजी लढा देण्याचे धैर्य:** सायबर गुन्हेगारांच्या धमक्यांना बळी न पडता डिजिटल पुरावे गोळा करून कायदेशीर कारवाई कशी करावी, याची माहिती.
- ५. **डिजिटल प्रायव्हेसी आणि ट्रॅफॅक्टर सुरक्षेचे नियम:** वैयक्तिक सोशल मीडिया खाती हॅक होण्यापासून वाचवण्यासाठी अत्यंत आवश्यक तांत्रिक पायऱ्या समजतील.
- ६. **नातेसंबंधांमधील भावनिक परिपक्वता:** आभासी जगातील खोट्या कौतुकापेक्षा प्रत्यक्ष मानवी नातेसंबंध आणि सुरक्षिततेचे महत्त्व पटवून देणारे प्रबोधन.

✨ लेखकाचा प्रेरणार्थक संकल्प संदेश:

"तुमचा डेटा हीच तुमची खरी प्रतिष्ठा आहे. एका क्षणाच्या भावनिक मोहापायी संपूर्ण आयुष्य पणाला लावू नका. जागे व्हा, सजग राहा आणि डिजिटल दुनियेत निर्भयपणे जगा!"

विषय सूची (Table of Contents)

पुस्तकातील सर्व अध्यायांची व पानांची अचूक रचना खालीलप्रमाणे आहे:

पृष्ठ	अध्याय / विभागाचे नाव	विषय स्वरूप
पृष्ठ १	मुद्रित मुखपृष्ठ (Cover Page)	प्रिमियम डिझाईन व मेटाडेटा
पृष्ठ २	लेखक परिचय व संशोधन पार्श्वभूमी	अधिकृत स्रोत व संकेतस्थळ
पृष्ठ ३	कायदेशीर अस्वीकरण (Mandatory Disclaimer)	वैधानिक ४-परिच्छेद धोरण
पृष्ठ ४	पुस्तकाचा उद्देश आणि ६ महत्वाचे लाभ	प्रस्तावना व लेखक संकल्प
पृष्ठ ५	अनुक्रमणिका (विषय सूची)	रचनात्मक कोष्टक
पृष्ठ ६	अध्याय १: ग्लॅमर, फॉलोअर्स आणि मुंबईचे स्वप्न	कादंबरी भाग - १
पृष्ठ ७	अध्याय २: इनबॉक्समधील तो अनोळखी 'मिस्टर कबीर'	कादंबरी भाग - २
पृष्ठ ८	अध्याय ३: आभासी प्रेमाचा भूलभुलैया	कादंबरी भाग - ३
पृष्ठ ९	अध्याय ४: संशयाची पहिली ठिणगी आणि गुप्त कोड	कादंबरी भाग - ४
पृष्ठ १०	अध्याय ५: डीपफेकचा काळोख आणि पहिला धक्का	कादंबरी भाग - ५
पृष्ठ ११	अध्याय ६: ब्लॅकमेलिंगचे विषारी चक्रव्यूह	कादंबरी भाग - ६
पृष्ठ १२	अध्याय ७: तोडफोडीची रात्र आणि अश्रूंचा बांध	कादंबरी भाग - ७
पृष्ठ १३	अध्याय ८: सायबर सेलचा दरवाजा: इन्स्पेक्टर विक्रम	कादंबरी भाग - ८
पृष्ठ १४	अध्याय ९: डिजिटल फॉरेंसिक आणि IP चा माग	कादंबरी भाग - ९
पृष्ठ १५	अध्याय १०: स्क्रीनमागचा खरा चेहरा उघडा पडतो!	कादंबरी भाग - १०
पृष्ठ १६	अध्याय ११: अनफॉलो आणि नव्याने जगण्याची सुरुवात	कादंबरी भाग - ११
पृष्ठ १७	सायबर सुरक्षा सुवर्ण नियमो (Digital Armor)	टेक्निकल गाईडलाईन्स
पृष्ठ १८	कायदेशीर संरक्षण, IT कायदा आणि हेल्पलाइन	कलमे, अधिकार व सुरक्षा
पृष्ठ १९	वारंवार विचारले जाणारे प्रश्न (FAQs - भाग १)	प्रश्न १ ते १० सविस्तर
पृष्ठ २०	वारंवार विचारले जाणारे प्रश्न (FAQs - भाग २)	प्रश्न ११ ते २० सविस्तर
पृष्ठ २१	अंतिम लेखक संदेश, प्रतिज्ञा व ई-बुक डाउनलोड CTA	संकल्प व अधिकृत दुवे

[अध्याय १]

ग्लॅमर, फॉलोअर्स आणि मुंबईचे स्वप्न

दक्षिण मुंबईतील मरीन ड्राईव्हवर संध्याकाळचा वारा वाहत होता. अथांग अरबी समुद्राच्या लाटा किनाऱ्यावर आदळत असताना, वीस वर्षांची अनघा देशपांडे आपल्या आयफोनचा कॅमेरा सेट करण्यात मग्न होती. तिच्या चेहऱ्यावर एक अस्वस्थ स्मितहास्य होते. ती मुंबईतील नामांकित सेंट झेव्हियर्स कॉलेजमध्ये मास मीडियाच्या दुसऱ्या वर्षात शिकत होती.

अनघाचे एकच स्वप्न होते—तिला इन्स्टाग्रामवर लाखो फॉलोअर्स असलेली एक आघाडीची 'फॅशन इन्फ्लुएन्सर' बनायचे होते. तिच्या वर्गमित्रांचे प्रोफाईल्स व्हेरिफाईड होत होते, त्यांना ब्रँड्सकडून स्पॉन्सरशिप मिळत होती, आणि अनघा मात्र पन्नास हजार फॉलोअर्सवरच अडकून पडली होती.

"अनघा, तू अजून किती वेळ त्या फोनच्या स्क्रीनमध्ये डोकं घालून बसणार आहेस? जरा समुद्राकडे बघ, किती सुंदर सूर्यास्त आहे!" तिची मैत्रीण तन्वीने चिडून म्हटले.

"तन्वी, तुला नाही समजणार! आजकालच्या जगात जर तुमच्या प्रोफाइलवर निळी टिक (Blue Tick) नसेल, तर समाजात तुमचं काही अस्तित्वच नाही. आज रात्री मला कोणत्याही परिस्थितीत नवीन रील पोस्ट करायची आहे," अनघाने उत्तरादाखल डोळे फिरवत म्हटले.

घरी परतताना अनघाच्या डोक्यात फक्त एकच विचार होता: लाईक्स, शेअर्स आणि व्ह्यूज. तिने त्या रात्री तिचा सर्वोत्तम लूक असलेला व्हिडिओ एका ट्रेंडिंग गाण्यावर एडिट केला आणि हॅशटॅग्स लावून पोस्ट केला.

सायबर मानसशास्त्र निरीक्षण:

आधुनिक तरुण पिढीमध्ये 'व्हॅलिडेशन सिंड्रोम' (Validation Syndrome) नावाचा मानसिक आजार झपाट्याने पसरत आहे. अनोळखी लोकांकडून मिळणाऱ्या लाईक्सच्या आधारे स्वतःचे आत्मसन्मान ठरवणे हा एका मोठ्या सायबर संकटाची पहिली पायरी ठरतो.

घड्याळात रात्रीचे १२:३० वाजले होते. अनघा फोन उशाशी ठेवून झोपी जाण्याच्या तयारीत असतानाच अचानक तिच्या फोनवर एकापाठोपाठ एक नोटिफिकेशन्सचा पाऊस पडू लागला. अवघ्या दहा मिनिटांत तिची रील व्हायरल झाली होती!

[अध्याय २]

इनबॉक्समधील तो अनोळखी 'मिस्टर कबीर'

दुसऱ्या दिवशी सकाळी अनघा उठली तेव्हा तिच्या इन्स्टाग्रामवर फॉलोअर्सची संख्या एका रात्रीत थेट ऐंशी हजारांच्या पुढे गेली होती. अनघाचा आनंद गगनात मावेनासा झाला होता. तिच्या पोस्टवर हजारो कमेंट्स होत्या. पण त्या शेकडो कमेंट्सच्या गर्दीत एका विशिष्ट कमेंटने तिचे लक्ष वेधून घेतले.

त्या युझरचे नाव होते **@kabir_singh_official**. प्रोफाईल फोटोमध्ये एक देखणा, सूट घातलेला आणि आत्मविश्वासू भासणारा तरुण दिसत होता. त्याच्या बायोमध्ये लिहिले होते: 'आंतरराष्ट्रीय फॅशन फोटोग्राफर, लंडन-मुंबई. नव्या टॅलेंटचा शोधक.'

"तुझ्या डोळ्यांमध्ये एक अद्भुत तेज आहे अनघा. तुझा स्क्रीनवरील वावर लंडनच्या टॉप मॉडेलसनाही लाजवेल असा आहे. जर तुला जागतिक स्तरावर काम करायचे असेल, तर डीएम (Direct Message) कर."

अनघाचे हृदय जोरात धडधडू लागले. तिने कोणताही विचार न करता त्या प्रोफाईलच्या इनबॉक्समध्ये मेसेज टाकला: "खूप खूप धन्यवाद सर! तुमचे शब्द माझ्यासाठी खूप मोलाचे आहेत."

अवघ्या दोन सेकंदांत पलीकडून रिप्लाय आला. कबीर अतिशय सभ्य, आदराने आणि मोहक भाषेत बोलत होता. त्याने अनघाला सांगितले की तो सध्या लंडनमध्ये एका आंतरराष्ट्रीय प्रोजेक्टवर काम करत आहे आणि पुढील महिन्यात मुंबईत येऊन एका मोठ्या लवझरी ब्रँडसाठी नवीन चेहऱ्याचे ऑडिशन घेणार आहे.

डिजिटल तपासाचे सत्य:

सायबर गुन्हेगार सुरुवातीला कधीही थेट वैयक्तिक गोष्टी मागत नाहीत. ते प्रथम पीडितेच्या अहंकाराला आणि महत्वाकांक्षेला खतपाणी घालतात. या प्रक्रियेला मानसोपचारशास्त्रात '**लव्ह बॉम्बिंग**' (Love Bombing) आणि सायबर भाषेत '**युर्मिंग**' म्हटले जाते.

कबीरच्या संभाषणातील गोडवा इतका प्रभावी होता की अनघाला वाटू लागले, देव तिच्या स्वप्नांना पूर्ण करण्यासाठीच कबीरच्या रूपाने धावून आला आहे.

[अध्याय ३]

आभासी प्रेमाचा भूलभुलैया

आठवडे सरत गेले. अनघा आणि कबीर यांच्यातील संभाषण आता केवळ कामापुरते उरले नव्हते. रोज रात्री उशिरापर्यंत चॅटिंग सुरू झाले होते. कबीर अनघाला तिच्या दिवसातील प्रत्येक लहान-सहान गोष्टी विचारू लागला—ती काय खाते, तिचे कुटुंब कसे आहे, तिचे जुने मित्र कोण आहेत, आणि ती कुठे फिरायला जाते.

अनघाने कबीरवर इतका विश्वास टाकला होता की तिने तिच्या कॉलेजचे वेळापत्रक, घराचा पत्ता, अगदी तिच्या वैयक्तिक डायरीतील विचारही त्याच्याशी शेअर केले होते. कबीरने तिच्या मनात हळूहळू एक आभासी प्रेमाचे जग निर्माण केले होते.

"अनघा, मी लंडनच्या धकाधकीच्या आयुष्यात खूप एकटा होतो. पण तुझ्याशी बोलल्यानंतर मला जाणवले की माझं आयुष्य तुझ्याशिवाय अपूर्ण आहे. मी मुंबईत आलो की थेट तुझ्या आई-बाबांशी आपल्या लग्नाबद्दल बोलणार आहे," कबीरने व्हॉट्स नोट पाठवली होती.

त्या व्हॉट्स नोटमधील आवाज अतिशय गंभीर आणि भारदस्त होता. अनघा पूर्णपणे त्याच्या प्रेमाच्या जाळ्यात गुरफटून गेली होती. तिने तिच्या मैत्रिणी तन्वीशीही बोलणे कमी केले होते, कारण कबीरने तिला समजावले होते की, "तुझे मित्र तुझ्या यशावर जळतात. आपल्या नात्याबद्दल कोणालाही सांगू नकोस."

⚠ धोक्याची मोठी घंटा (Red Flag):

जेव्हा एखादी ऑनलाइन व्यक्ती तुम्हाला तुमच्या कुटुंबापासून आणि जिवाभावाच्या मित्रांपासून तोडण्याचा प्रयत्न करते, तेव्हा १००% सावध व्हा! ही सायबर भक्षकाची (Cyber Predator) पहिली आणि सर्वात धोकादायक खेळी असते.

अनघाने स्वतःभोवती कबीरच्या शब्दांचे एक काल्पनिक कवच तयार केले होते. तिला अजिबात कल्पना नव्हती की, ज्या कबीरवर ती आंधळेपणाने प्रेम करत होती, त्याचा खरा चेहरा किती भयंकर आणि विकृत होता!

[अध्याय ४]

संशयाची पहिली ठिणगी आणि गुप्त कोड

एके दिवशी कबीरने अनघाला सांगितले की तो तिच्यासाठी एक खाजगी क्लाउड सर्व्हर आणि पोर्टफोलिओ वेबसाईट तयार करत आहे. यासाठी त्याने तिला एका लिंकवर क्लिक करून एका अज्ञात ॲप्लिकेशनला गुगल अकाउंटचा ॲक्सेस देण्यास सांगितले.

"अनघा, या ॲपमुळे तुझे सर्व हाय-रिझोल्यूशन फोटो सुरक्षित राहतील आणि थेट लंडनच्या एजन्सीला दिसतील. त्वरित गुगलने लॉगिन करून मला ओटीपी (OTP) सांग," कबीरने फोनवर अतिशय घाईगडबडीत सांगितले.

अनघाने संकोच न करता लिंकवर क्लिक केले. तिच्या मोबाईल स्क्रीनवर एक लाल रंगाचा वॉर्निंग मेसेज झळकला: '*Unverified Developer App - High Risk Permission Requested*'. अनघाचे बोट एका क्षणासाठी थबकले. तिने कबीरला विचारले, "कबीर, हा मेसेज धोकादायक दाखवतोय..."

"अनघा! तू माझ्यावर संशय घेतेस का? जर तुझा माझ्यावर विश्वास नसेल तर आपण हे नाते इथेच संपवूया!" कबीरच्या आवाजात अचानक प्रचंड राग आणि आक्रमकता जाणवली.

त्याच्या रागाच्या भीतीने अनघा घाबरली. 'कबीर आपल्यावर नाराज होईल' या एकाच भीतीने तिने सर्व वॉर्निंगज दुर्लक्षित करून 'Allow All Permissions' वर क्लिक केले आणि आलेला ६-अंकी कोड कबीरला देऊन टाकला.

**सायबर सुरक्षेचा नियम क्र. १:**

कधीही, कोणत्याही परिस्थितीत कोणत्याही ॲपला आपल्या गुगल ड्राईव्ह, फोटो गॅलरी किंवा कॅमेरा-मायक्रोफोनचा अनियंत्रित ॲक्सेस देऊ नका. ओटीपी (OTP) हा तुमचा डिजिटल स्वाक्षरीसारखा असतो; तो कोणाशीही शेअर करणे म्हणजे स्वतःच्या घराची चावी चोराच्या हातात देण्यासारखे आहे!

जसा तिने तो कोड दिला, तसा कबीरचा फोन अचानक कट झाला. अनघाच्या फोनची स्क्रीन काही सेकंदांसाठी काळी पडली, आणि तिच्या गुगल ड्राईव्हमधील सर्व खाजगी डेटा, बालपणीचे फोटो आणि कुटुंबियांचे व्हिडिओ बॅकग्राउंडमध्ये अज्ञात सर्व्हरवर अपलोड होऊ लागले.

[अध्याय ५]

डीपफेकचा काळोख आणि पहिला धक्का

त्या रात्रीनंतर दोन दिवस कबीरचा कोणताही मेसेज आला नाही. त्याचा फोन सतत 'स्विच ऑफ' येत होता. अनघा प्रचंड मानसिक तणावाखाली होती. तिला वाटत होते की कबीर तिच्यावर रागवला आहे. तिने त्याला शंभरहून अधिक मेसेज केले, पण सर्व 'अनडिलीव्हर्ड' राहिले.

तिसऱ्या दिवशी संध्याकाळी अनघाच्या व्हॉट्सअॅपवर एका अज्ञात आंतरराष्ट्रीय क्रमांकावरून (+४४...) एक व्हिडिओ फाईल आली. सोबत एक लहान मेसेज होता: 'हा व्हिडिओ नीट बघ अनघा... तुझा खरा चेहरा कसा वाटतो?'

अनघाने थरथरत्या हातांनी ती व्हिडिओ फाईल उघडली. पुढील दृश्य पाहताच तिच्या पायाखालची जमीनच सरकली! तिच्या डोळ्यांसमोर अंधारी आली, आणि तिच्या तोंडातून किंवाळी बाहेर पडली.

त्या व्हिडिओमध्ये अनघाचे हुबेहूब तोंड एका अत्यंत अश्लील आणि विवस्त्र महिलेच्या शरीरावर चिकटवण्यात आले होते! तिच्या चेहऱ्याचे हावभाव, ओठांची हालचाल, अगदी पापण्यांची उघडझाप इतकी अचूक होती की कोणीही तो व्हिडिओ खराच आहे असे मानले असते!

हा आधुनिक **डीपफेक (Deepfake AI)** तंत्रज्ञानाचा अतिशय क्रूर आणि विकृत नमुना होता. अनघाने कबीरला दिलेल्या अॅक्सेसमधून त्याने तिचे सर्व हाय-डेफिनिशन फोटो चोरले होते आणि एका प्रगत एआय सॉफ्टवेअरद्वारे हा बनावट अश्लील व्हिडिओ तयार केला होता.

⚠ डीपफेक म्हणजे काय?

डीपफेक हे आर्टिफिशियल इंटेलिजन्स (Deep Learning) चे असे अल्गोरिदम आहे जे एका व्यक्तीचा चेहरा दुसऱ्या व्यक्तीच्या शरीरावर अथवा व्हिडिओवर १००% हुबेहूब बसवते. आजकाल सायबर गुन्हेगार सोशल मीडियावरील पब्लिक फोटोंचा वापर करून असे ब्लॅकमेलिंग व्हिडिओ तयार करतात.

अनघाला रडू कोसळले. ती खोलीत एकटी बसून ओक्साबोक्सी रडू लागली. तिचा ज्या कबीरवर देवासारखा विश्वास होता, तो प्रत्यक्षात एक राक्षस निघाला होता!

[अध्याय ६]

ब्लॅकमेलिंगचे विषारी चक्रव्यूह

अनघा अजून त्या धक्क्यातून सावरलीही नव्हती तोच त्याच अज्ञात क्रमांकावरून ऑडिओ कॉल आला. अनघाने भीतीने थरथरत कॉल उचलला.

पलीकडून तोच परिचित आवाज आला, पण आता त्या गोडव्यात एक भयानक विष भरलेले होते:

"कशी आहेस अनघा? व्हिडिओ आवडला का? जर हा व्हिडिओ तुझ्या कॉलेजच्या ग्रुपवर, तुझ्या वडिलांच्या फेसबुकवर आणि इन्स्टाग्रामवर व्हायरल होऊ नये असे वाटत असेल, तर मी सांगेन ते मुकाट्याने ऐक!"

"कबीर... तू माझ्यासोबत असं का केलंस? मी तुझ्यावर किती प्रेम केलं होतं!" अनघाने हुंदके देत विचारले.

"प्रेम? हाहाहा! तू खरंच मूर्ख आहेस अनघा. कबीर नावाचा कोणी फोटोग्राफर लंडनमध्ये अस्तित्वातच नाही. मी कोण आहे हे तुला कधीच कळणार नाही. उद्या दुपारपर्यंत मला एका क्रिप्टोकरन्सी वॉलेटमध्ये पाच लाख रुपये हवे आहेत. जर पैसे नाही मिळाले, तर तुझा हा व्हिडिओ इंटरनेटच्या प्रत्येक पॉर्न साईटवर आणि तुझ्या नातेवाईकांच्या इनबॉक्समध्ये असेल!"

● ब्लॅकमेलिंगची मानसशास्त्रीय जाळी:

सायबर खंडणीखोर (Sextortionists) पीडितेला इतके मानसिकदृष्ट्या एकाकी पाडतात की पीडित व्यक्तीला आत्महत्या किंवा पैसे देणे याशिवाय दुसरा कोणताही मार्ग दिसत नाही. अशा वेळी शांत राहणे आणि कोणताही आर्थिक व्यवहार न करणे हाच एकमेव मार्ग असतो.

अनघाचे जग उद्ध्वस्त झाले होते. एक मध्यमवर्गीय कॉलेज तरुणी पाच लाख रुपये कुठून आणणार? तिच्या डोक्यात आत्महत्येचे भयानक विचार चक्रावू लागले. खोलीचा पंखा आणि तिची ओढणी याशिवाय तिला तिच्या संकटातून सुटण्याचा कोणताही मार्ग दिसेनासा झाला.

तोडफोडीची रात्र आणि अश्रूंचा बांध

रात्रीचे दोन वाजले होते. अनघाच्या खोलीतील दिवा बंद होता. ती अंधारात बेडच्या कोपऱ्यात पाय पोटाशी धरून बसली होती. फोनवर दर दहा मिनिटांनी कबीरच्या धमक्यांचे काऊंटडाऊन मेसेजेस येत होते: 'फक्त १० तास शिल्लक... ९ तास शिल्लक...'

तिने पंख्याकडे पाहिले. तिच्या डोळ्यातून घळाघळा अश्रू वाहत होते. 'जर आई-बाबांनी हा व्हिडिओ पाहिला, तर ते समाजात तोंड कसे दाखवतील? कॉलेजमध्ये माझ्या चारित्र्यावर डाग लागेल. मी जिवंत राहून काय करू?' हे विचार तिच्या डोक्यात थैमान घालत होते.

तिने कागदावर आत्महत्येची चिठ्ठी लिहिण्यासाठी पेन उचलला. पण त्याच क्षणी तिच्या खोलीचा दरवाजा हळूच उघडला. तिची आई पाणी पिण्यासाठी उठली होती आणि अनघाच्या खोलीतून येणारा हुंदक्यांचा आवाज ऐकून आत आली.

"अनू! काय झालं बाळा? तू अंधारात का बसली आहेस? आणि तू रडतेस का?" आईने धावत येऊन अनघाला जवळ घेतले.

आईचा स्पर्श होताच अनघाचा सर्व संयम सुटला. तिने आईला घट्ट मिठी मारली आणि ढसाढसा रडू लागली. तिने काहीही न लपवता, फोनमधील चॅट्स, कबीरचे खोटे आश्वासन, तो डीपफेक व्हिडिओ आणि पाच लाखांची खंडणी... सर्व काही आई आणि वडिलांसमोर मांडले.

पालकांचा पाठींबा: जीव वाचवणारी संजीवनी!

अशा गंभीर सायबर संकटात जेव्हा मुले पालकांशी मोकळेपणाने बोलतात, तेव्हा ९०% गुन्हेगारांचे डाव अपयशी ठरतात. अनघाच्या वडिलांनी तिला ओरडण्याऐवजी छातीशी कवटाळले आणि म्हणाले, "तू कोणतीही चूक केलेली नाहीस अनू. तो गुन्हेगार आहे, तू नाहीस! आपण उद्या सकाळीच सायबर पोलिसांकडे जाऊ!"

वडिलांच्या त्या शब्दांनी अनघाच्या मनात जगण्याची आणि लढण्याची नवी उमेद निर्माण केली. काळोख्या रात्रीनंतर एक नवा सूर्य उगवणार होता.

[अध्याय ८]

सायबर सेलचा दरवाजा: इन्स्पेक्टर विक्रम

दुसऱ्या दिवशी सकाळी १० वाजता अनघा तिच्या आई-वडिलांसोबत वांद्रे-कुर्ला संकुल (BKC) येथील मुंबई सायबर क्राईम पोलीस ठाण्यात हजर झाली. तिच्या मनात प्रचंड भीती होती की पोलीस तिलाच दोष देतील किंवा उलटसुलट प्रश्न विचारतील.

परंतु सायबर सेलचे वरिष्ठ पोलीस निरीक्षक **विक्रम सूर्यवंशी** यांनी त्यांचे अतिशय सन्मानाने स्वागत केले. इन्स्पेक्टर विक्रम हे सायबर फॉरेन्सिक आणि एआय गुन्हांच्या तपासातील निष्णात अधिकारी मानले जात होते.

"बेटा अनघा, सर्वात आधी तू स्वतःला दोषी मानणे बंद कर. सोशल मीडियावर एका गुन्हेगाराने रचलेल्या कटकारस्थानाची तू बळी ठरली आहेस. अशा खंडणीखोरांना धडा शिकवणे हे आमचे कर्तव्य आहे," इन्स्पेक्टर विक्रम यांनी अत्यंत धीर दिला.

इन्स्पेक्टर विक्रम यांनी तात्काळ तीन महत्वाच्या कायदेशीर आणि तांत्रिक प्रक्रिया सुरू केल्या:

- **१. पुरावे गोळा करणे (Evidence Preservation):** गुन्हेगाराचे सर्व व्हॉट्सअॅप चॅट्स, स्क्रीनशॉट्स, ऑडिओ फाइल्स आणि ई-मेल हेडरचा डिजिटल पंचनामा करण्यात आला.
- **२. मेटा (Meta) आणि टेलिग्रामला नोटीस:** कलम ९१ अंतर्गत संबंधित सोशल मीडिया प्लॅटफॉर्मसना त्या बनावट अकाउंटचा आयपी लॉग (IP Log) आणि नोंदणी तपशील तातडीने गोठवण्याचे आदेश दिले गेले.
- **३. NCII/Take It Down पोर्टलवर नोंदणी:** डीपफेक व्हिडिओ इंटरनेटवर कुठेही अपलोड होऊ नये म्हणून त्याचा डिजिटल हॅश (Digital Hash) राष्ट्रीय सुरक्षा डेटाबेसमध्ये समाविष्ट करण्यात आला.

सायबर सेलचा सुवर्ण सल्ला:

गुन्हेगाराला कधीही पैसे देऊ नका! तसे असेल तर पैसे आपो छे असेल तेव्हा तेव्हा लावय वधती जाय छे. पोलीस आणि सायबर सेलकडे अशा गुन्हेगारांना पकडण्यासाठी प्रगत तंत्रज्ञान उपलब्ध असते.

अनघाच्या चेहऱ्यावर आता भीतीची जागा एका निर्धाराने घेतली होती. तिला आता स्क्रीनमागच्या त्या अदृश्य राक्षसाचा खरा चेहरा उघडा पाडायचा होता.

[अध्याय ९]

डिजिटल फॉरेंसिक आणि IP चा माग

सायबर सेलच्या प्रयोगशाळेत कॉम्प्युटरच्या स्क्रीनवर वेगाने कोड्स स्करोल होत होते. फॉरेंसिक तज्ज्ञ रोहनने अनघाच्या मोबाईलचे क्लोन तयार करून त्यातील स्पायवेअरचा अभ्यास सुरू केला.

"सर, गुन्हेगार खूप हुशार आहे. त्याने व्हर्चुअल प्रायव्हेट नेटवर्क (VPN) आणि डार्क वेब प्रॉक्सीचा वापर करून लंडनचा आयपी अड्रेस स्फूफ केला होता. पण त्याने एक मोठी चूक केली आहे," रोहनने इन्स्पेक्टर विक्रमना बोलावले.

"काय चूक केली त्याने रोहन?" विक्रम यांनी उत्सुकतेने विचारले.

"सर, त्याने अनघाला जी फिशिंग लिंक पाठवली होती, ती लिंक तयार करताना त्याने एका स्थानिक भारतीय सिमकार्डचा वापर करून क्लाउड सर्व्हरवर लॉगिन केले होते. त्या लॉगिन सेशनचा मॅक आयडी (MAC ID) आणि मूळ टॉवर लोकेशन आपल्या हाती लागले आहे!"

पोलिसांच्या तपासाची सुई लंडनवरून थेट महाराष्ट्रात वळली होती! तो गुन्हेगार कोणत्याही परदेशात नव्हता, तर तो मुंबईपासून अवघ्या दीडशे किलोमीटर अंतरावर असलेल्या पुण्याच्या एका उपनगरात बसून हा सर्व खेळ चालवत होता.

इन्स्पेक्टर विक्रम यांनी लगेचच सायबर सेलच्या स्पेशल टास्क फोर्सला पाचारण केले. गुन्हेगाराने दिलेले क्रिप्टोकरन्सी वॉलेटही ट्रॅक करण्यात आले. त्याने यापूर्वी अशाच प्रकारे आठ निष्पाप मुलींना डीपफेक व्हिडिओच्या माध्यमातून ब्लॅकमेल करून लाखो रुपये उकळल्याचे समोर आले.

डिजिटल फॉरेंसिक वास्तव:

डिजिटल जगात कोणताही गुन्हेगार परिपूर्ण नसतो. इंटरनेटवर टाकलेले प्रत्येक पाऊल (Digital Footprint) कायमस्वरूपी नोंदवले जाते. व्हीपीएन असो वा प्रॉक्सी, योग्य फॉरेंसिक तपासाने गुन्हेगाराची खरी ओळख उघड करता येतेच!

पोलिसांची दोन वाहने पुण्याच्या दिशेने सुसाट वेगाने रवाना झाली. शिकारी आता स्वतःच पोलिसांच्या जाळ्यात अडकणार होता!

स्क्रीनमागचा खरा चेहरा उघडा पडतो!

पुण्यातील बाणेर परिसरातील एका आलिशान फ्लॅटच्या बाहेर पोलिसांची गाडी शांतपणे थांबली. इन्स्पेक्टर विक्रम आणि त्यांच्या पथकाने बंद दरवाजावर ठोठावले.

दरवाजा उघडताच आत एका अंधाऱ्या खोलीत तीन-तीन मॉनिटर्स लावून एक पंचवीस वर्षांचा तरुण बसलेला दिसला. डोळ्यांवर चष्मा, अस्ताव्यस्त केस आणि अंगात सामान्य टी-शर्ट असलेला तो तरुण पोलिसांना पाहताच थरथर कापू लागला.

"रोहित सावंत? की आंतरराष्ट्रीय फॅशन फोटोग्राफर कबीर सिंग?" इन्स्पेक्टर विक्रम यांच्या भारदस्त आवाजाने त्या खोलीतील हवा गोठून गेली.

रोहितच्या हातातील लॅपटॉपवर अनघाचा फोटो आणि डीपफेक सॉफ्टवेअर उघडेच होते! पोलिसांनी क्षणाचाही विलंब न लावता त्याचे सर्व हार्ड ड्राईव्हज, तीन लॅपटॉप्स आणि बारा बनावट सिमकार्ड्स जप्त केले.

रोहित सावंत हा एका आयटी कंपनीतून कामावरून काढून टाकलेला इंजिनिअर होता. तो बेरोजगार झाल्यानंतर त्याने सोशल मीडियावरील मुलींना फसवून खंडणी उकळण्याचा हा काळा धंदा सुरू केला होता. मॉडेलचे फोटो इंटरनेटवरून चोरून त्याने कबीर सिंगचे बनावट प्रोफाइल तयार केले होते.

भारतीय माहिती तंत्रज्ञान कायदा (IT Act 2000):

आरोपीवर कलम 66C (ओळख चोरी), कलम 66D (तोतयागिरी करून फसवणूक), कलम 66E (गोपनीयतेचा भंग), कलम 67 / 67A (अश्लील साहित्य प्रसारित करणे) आणि भा.दं.सं. कलम ३८४ (खंडणी) अंतर्गत अजामीनपात्र गुन्हे दाखल करण्यात आले.

जेव्हा अनघाने पोलीस ठाण्यात त्या खऱ्याखऱ्या 'कबीर'ला—म्हणजेच भेकड रोहित सावंतला हातात बेड्या घातलेल्या अवस्थेत पाहिले, तेव्हा तिच्या डोळ्यांतील सर्व भीती संपली होती. स्क्रीनमागचा राक्षस प्रत्यक्षात किती क्षुद्र आणि दुबळा होता, हे तिला समजले होते.

[अध्याय ११]

अनफॉलो आणि नव्याने जगण्याची सुरुवात

रोहित सावंतला न्यायालयाने पाच वर्षांची सक्तमजुरी आणि दहा लाख रुपयांचा दंड ठोठावला. पोलिसांनी फॉरेन्सिक लॅबच्या मदतीने अनघाचे सर्व बनावट व्हिडिओ आणि फोटो कायमस्वरूपी नष्ट केले. अनघा आता पूर्णपणे सुरक्षित आणि मुक्त झाली होती.

घरी परतल्यानंतर अनघाने तिच्या खोलीतील आरशात पाहिले. आज तिला स्वतःचा चेहरा अधिक आत्मविश्वासू आणि तेजस्वी वाटत होता. तिने तिचा स्मार्टफोन हातात घेतला.

सर्वात प्रथम तिने तिच्या इन्स्टाग्रामवरील सर्व अनोळखी फॉलोअर्स आणि खोट्या प्रोफाईल्सना कायमचे 'अनफॉलो' (Unfollow) आणि 'ब्लॉक' (Block) केले. तिने तिचे प्रोफाईल 'प्रायव्हेट' केले आणि टू-फॅक्टर ऑथेंटिकेशन सुरू केले.

अनघाने तिच्या सोशल मीडियावर एक नवीन आणि खरीखुरी पोस्ट लिहिली:

"माझ्या मित्रांनो, आभासी जगातील लाईक्स आणि अनोळखी लोकांचे खोटे कौतुक म्हणजे तुमचे आयुष्य नाही. स्क्रीनच्या पलीकडे कोण बसले आहे हे आपल्याला ठाऊक नसते. सायबर धोक्यांपासून सावध राहा आणि स्वतःची डिजिटल सुरक्षा कधीही धोक्यात आणू नका!"

अनघा आता तिच्या कॉलेजमध्ये 'सायबर क्राईम अवेअरनेस सेल'ची प्रमुख बनली होती. तिच्या अनुभवातून तिने हजारो तरुण मुलींना सायबर गुन्हेगारांच्या जाळ्यात अडकण्यापासून वाचवले.

📖 कादंबरीचा अंतिम संदेश:

तंत्रज्ञान हे माणसाच्या प्रगतीसाठी आहे, विनाशासाठी नाही. एका चुकीच्या क्लिकमुळे आयुष्य उद्ध्वस्त होऊ शकते, पण योग्य वेळी दाखवलेले धाडस आणि सत्याची निवड तुम्हाला संकटातून बाहेर काढून एक विजेता बनवू शकते!

(समाप्त)

सायबर सुरक्षेचे १० सुवर्ण नियम (Digital Armor)

प्रत्येक स्मार्टफोन वापरकर्त्याने आणि सोशल मीडिया युझरने स्वतःचा डेटा सुरक्षित ठेवण्यासाठी खालील १० सुवर्ण नियमांचे तंतोतंत पालन केले पाहिजे:

१. टू-फॅक्टर ऑथेंटिकेशन (2FA) अनिवार्य करा:

तुमच्या सर्व खात्यांवर (Google, Instagram, WhatsApp, Banking) केवळ पासवर्डवर अवलंबून न राहता Authenticator App किंवा SMS आधारित 2FA सक्रिय ठेवा.

२. प्रोफाईल नेहमी 'Private' ठेवा:

तुमचे खाजगी फोटो, कुटुंबाचे फोटो आणि दैनंदिन फिरण्याचे ठिकाण (Location Tagging) सार्वजनिक (Public) करू नका. केवळ ओळखीच्या लोकांनाच ॲक्सेस द्या.

३. अनोळखी लिंक्स आणि एपीके फाइल्सपासून दूर राहा:

'फ्री रिकार्ज', 'लॉटरी लागली' किंवा 'तुमचा व्हिडिओ व्हायरल झाला आहे' अशा आशयाच्या कोणत्याही संशयास्पद लिंकवर कधीही क्लिक करू नका.

४. ओटीपी (OTP) आणि पिन कधीही शेअर करू नका:

बँकेचा अधिकारी असो, पोलीस असो वा जवळचा मित्र—कोणत्याही कारणासाठी ६-अंकी अथवा ४-अंकी ओटीपी कोणालाही सांगू नका.

५. वेबकॅम आणि कॅमेरा कव्हरचा वापर:

लॅपटॉप वापरत नसताना वेबकॅमवर स्टिकर किंवा शटर लावा. मालवेअरद्वारे तुमचा कॅमेरा नकळत ऑन केला जाऊ शकतो.

६. पब्लिक वाय-फाय (Public Wi-Fi) वर व्यवहार टाळा:

रेल्वे स्टेशन, कॅफे किंवा मॉलमध्ये मिळणाऱ्या मोफत वाय-फाय नेटवर्कवर कधीही नेट बँकिंग किंवा संवेदनशील पासवर्ड्स टाकू नका.

७. ॲप परमिशनचे नियमित ऑडिट:

कॅल्युलेटर किंवा फ्लॅशलाईट ॲपला कॉन्टॅक्ट्स आणि लोकेशनची परवानगी का हवी? गरजेपेक्षा जास्त परवानग्या त्वरित बंद करा.

कायदेशीर अधिकार व संरक्षण

भारतीय कायदे, महिलांचे अधिकार व हेल्पलाइन मार्गदर्शिका

सायबर गुन्ह्यांच्या विरोधात लढा देण्यासाठी भारतीय कायद्यात अत्यंत कठोर तरतुदी करण्यात आल्या आहेत. नागरिकांनी आपले कायदेशीर हक्क समजून घेणे अत्यंत आवश्यक आहे:

कलम (Act/Section)	गुन्ह्याचे स्वरूप	शिक्षेची तरतूद
IT Act 66C	ओळख चोरी (Identity Theft / बनावट खाते)	३ वर्षे कारावास व ₹१ लाख दंड
IT Act 66D	तोतयागिरी करून ऑनलाइन फसवणूक करणे	३ वर्षे कारावास व आर्थिक दंड
IT Act 66E	खाजगी अवयवांचे फोटो/व्हिडिओ काढणे व पाठवणे	३ वर्षे कारावास व ₹२ लाख दंड
IT Act 67/67A	अश्लील किंवा लैंगिक साहित्य इलेक्ट्रॉनिक स्वरूपात पसरवणे	५ वर्षे सक्तमजुरी व ₹१० लाख दंड
IPC 354D / BNS	सायबर स्टॉकिंग (सतत ऑनलाइन पाठलाग करणे)	३ ते ५ वर्षे तुरुंगवास
IPC 384 / BNS	डिजिटल ब्लॅकमेलिंग व खंडणी उकळणे	३ वर्षे कारावास व दंड

☎ महत्वाचे अधिकृत संपर्क क्रमांक (Emergency Contacts):

- राष्ट्रीय सायबर गुन्हे हेल्पलाइन: १९३० (टोल-फ्री २४x७)
- महिला राष्ट्रीय हेल्पलाइन: १०९१ / १८१
- राष्ट्रीय सायबर पोर्टल: <https://cybercrime.gov.in>
- NCII (नॉन-कन्सेन्सुअल इंटिमेट इमेजेस) पोर्टल: <https://stopncii.org>

झिरो एफआयआर (Zero FIR) चा अधिकार: सायबर गुन्ह्याची तक्रार देशातील कोणत्याही पोलीस ठाण्यात दाखल केली जाऊ शकते, गुन्हा कुठे घडला याने काहीही फरक पडत नाही.

वारंवार विचारले जाणारे प्रश्न (FAQs: प्रश्न १ ते १०)

१. जर कोणी माझा मॉर्फ केलेला किंवा डीपफेक फोटो व्हायरल करण्याची धमकी दिली तर काय करावे?

कधीही घाबरून पैसे देऊ नका. तात्काळ सर्व संभाषणांचे स्क्रीनशॉट घ्या, १९३० वर कॉल करा आणि stopncii.org वर जाऊन त्या फोटोचा डिजिटल हॅश सबमिट करा जेणेकरून तो इंटरनेटवरून ब्लॉक होईल.

२. सायबर गुन्हेगार प्रामुख्याने कोणाला टारगेट करतात?

ज्यांचे सोशल मीडिया प्रोफाईल पब्लिक असते, जे सतत स्वतःचे रिल-टाइम लोकेशन शेअर करतात आणि जे अनोळखी लोकांवर सहज विश्वास ठेवतात, अशा व्यक्तींना प्रामुख्याने टारगेट केले जाते.

३. इन्स्टाग्राम किंवा फेसबुकवर बनावट (Fake) प्रोफाईल कसे ओळखावे?

कमी पोस्ट्स, नवीनच तयार केलेले खाते, अत्यंत आकर्षक मॉडेलचा फोटो, फॉलोअर्सपेक्षा फॉलोईंग जास्त असणे आणि तातडीने खाजगी चॅटवर बोलण्याचा आग्रह धरणे ही बनावट खात्यांची लक्षणे आहेत.

४. हॅकर माझा फोन रिमोटली हॅक करू शकतो का?

होय, जर तुम्ही कोणत्याही संशयास्पद लिंकवरून अज्ञात APK फाईल डाऊनलोड केली किंवा अनधिकृत ॲपला सर्व परमिशन्स दिल्या, तर फोनचा संपूर्ण ताबा हॅकरकडे जाऊ शकतो.

५. सायबर क्राईम पोर्टलवर तक्रार करताना कोणती कागदपत्रे लागतात?

गुन्हेगाराचा फोन नंबर किंवा सोशल मीडिया हँडल, चॅटचे स्क्रीनशॉट्स, संशयित बँक व्यवहार तपशील (असल्यास) आणि ओळखपत्राची प्रत आवश्यक असते.

६. पोलीस ठाण्यात न जाता घरबसल्या तक्रार नोंदवता येते का?

होय, भारत सरकारच्या cybercrime.gov.in या पोर्टलवर नागरिक घरबसल्या पूर्णपणे गोपनीय पद्धतीने ऑनलाइन तक्रार नोंदवू शकतात.

७. डिजिटल अरेस्ट (Digital Arrest) ही खरी गोष्ट आहे का?

नाही! कायद्यात 'डिजिटल अरेस्ट' नावाची कोणतीही संकल्पना नाही. सीबीआय, कस्टम्स किंवा पोलीस कधीही स्काईप किंवा व्हॉट्सॲप व्हिडिओ कॉलवर कोणाला अटक करत नाहीत किंवा पैशांची मागणी करत नाहीत. हा १००% सायबर फ्रॉड आहे.

८. टू-फॅक्टर ऑथेंटिकेशन (2FA) साठी एसएमएस सुरक्षित आहे की ॲप?

एसएमएसपेक्षा गुगल ऑथेंटिकेटर (Google Authenticator) किंवा मायक्रोसॉफ्ट ऑथेंटिकेटर सारखे ॲप्स अधिक सुरक्षित मानले जातात, कारण सिम स्वॅपिंगद्वारे एसएमएस चोरीला जाऊ शकतात.

९. पब्लिक वाय-फाय वापरताना व्हीपीएन (VPN) वापरणे गरजेचे आहे का?

होय, सार्वजनिक वाय-फाय नेटवर्कवर तुमचा डेटा एन्क्रिप्टेड ठेवण्यासाठी एका विश्वासू पेड व्हीपीएनचा वापर करणे सुरक्षिततेच्या दृष्टीने फायदेशीर ठरते.

१०. सायबर क्राईम हेल्पलाइन १९३० वर तक्रार केल्यास त्वरित काय कारवाई होते?

१९३० वर तत्काळ तक्रार केल्यास फसवणूक झालेली रक्कम गुन्हेगाराच्या बँक खात्यात गोठवली (Freeze) जाते, ज्यामुळे तुमचे पैसे परत मिळण्याची शक्यता सर्वाधिक असते.

वारंवार विचारले जाणारे प्रश्न (FAQs: प्रश्न ११ ते २०)

११. जर माझ्या सोशल मीडिया खात्याचा पासवर्ड चोरीला गेला तर काय करावे?

तातडीने 'Forgot Password' द्वारे पासवर्ड रिसेट करा, 'Log out of all devices' पर्याय निवडा आणि ॲप सपोर्टकडे खात्याच्या अनधिकृत ॲक्सेसची तक्रार नोंदवा.

१२. व्हॉट्सॲपवर येणाऱ्या व्हिडिओ कॉल फ्रॉडपासून कसे वाचावे?

अनोळखी क्रमांकावरून येणारे व्हिडिओ कॉल्स कधीही उचलू नका. व्हॉट्सॲपच्या प्रायव्हसी सेटिंग्जमध्ये जाऊन 'Silence Unknown Callers' पर्याय चालू ठेवा.

१३. फिशिंग ई-मेल कसा ओळखावा?

प्रेषकाचा खरा ई-मेल पत्ता तपासा (उदा. support@bank.com ऐवजी support@bnk-security12.com), भाषेतील व्याकरणाच्या चुका आणि तातडीने खात्यावर कारवाई करण्याची दिलेली धमकी ही फिशिंगची चिन्हे आहेत.

१४. लहान मुलांच्या मोबाईल वापरावर पालकांनी कशी देखरेख ठेवावी?

गुगल फॅमिली लिंक (Google Family Link) सारख्या पॅरेंटल कंट्रोल ॲप्सचा वापर करा आणि मुलांशी सायबर धोक्यांबद्दल भीती न दाखवता मैत्रीपूर्ण संवाद ठेवा.

१५. डार्क वेब (Dark Web) वर सामान्य युझरचा डेटा कसा पोहोचतो?

जेव्हा एखादी मोठी ई-कॉमर्स किंवा सोशल मीडिया कंपनी डेटा ब्रीचचा बळी ठरते, तेव्हा वापरकर्त्यांचे पासवर्ड्स आणि ई-मेल्स डार्क वेबवर विकले जातात. HaveIBeenPwned.com वर तपासा.

१६. सिम स्वॅप (SIM Swap) फ्रॉड म्हणजे काय आणि तो कसा रोखावा?

गुन्हेगार तुमच्या नावाचे बनावट आयडी देऊन तुमच्या क्रमांकाचे नवीन सिम कार्ड मिळवतात. जर तुमच्या फोनचे नेटवर्क अचानक पूर्णपणे गेले तर त्वरित टेलिकॉम कंपनीशी संपर्क साधा.

१७. सायबर बुलिंग (Cyber Bullying) विरोधात कायदेशीर कारवाई होते का?

होय, सोशल मीडियावर कोणालाही अश्लील मेसेज पाठवणे, ट्रोल करणे किंवा धमकी देणे हा माहिती तंत्रज्ञान कायदांतर्गत आणि भारतीय न्याय संहितेअंतर्गत दखलपात्र गुन्हा आहे.

१८. सुरक्षित पासवर्ड कसा तयार करावा?

किमान १२ अक्षरांचा पासवर्ड ठेवा, ज्यामध्ये कॅपिटल आणि स्मॉल अक्षरे, आकडे आणि विशेष चिन्हे (!@#\$%^) असावीत. कधीही स्वतःचे नाव किंवा जन्मतारीख पासवर्ड म्हणून ठेवू नका.

१९. आर्थिक सायबर फसवणूक झाल्यावर 'गोल्डन अवर' (Golden Hour) म्हणजे काय?

फसवणूक झाल्यानंतरचे पहिले २ तास हे अत्यंत महत्वाचे असतात. या काळात १९३० वर तक्रार केल्यास गुन्हेगाराच्या खात्यातील व्यवहार रोखले जाण्याची शक्यता ९५% पेक्षा जास्त असते.

२०. सामान्य नागरिकांसाठी सर्वोत्तम सायबर सुरक्षा सवय कोणती?

"शून्य विश्वास" (Zero Trust) दृष्टिकोन! स्क्रीनच्या पलीकडे कोणतीही व्यक्ती कितीही गोड बोलत असली तरीही, जोपर्यंत प्रत्यक्ष ओळख पटत नाही तोपर्यंत कोणतीही खाजगी माहिती किंवा डेटा शेअर करू नका.

अंतिम संकल्प व कृती संदेश

लेखकाचा अंतिम संदेश, डिजिटल प्रतिज्ञा व अधिकृत दुवे

प्रिय वाचक मित्र-मैत्रिणींनो, 'अनफॉलो: स्क्रीनमागचा अदृश्य चेहरा' ही केवळ अनघाची कहाणी नसून आपल्या आजूबाजूला घडणारे एक कटू वास्तव आहे. तंत्रज्ञानाने आपल्याला जग जवळ आणण्याची ताकद दिली, पण त्याच वेळी आपण आपल्या सुरक्षिततेच्या भिंती कमकुवत करून बसलो.

🇮🇳 आपली सामूहिक डिजिटल प्रतिज्ञा:

"मी प्रतिज्ञा करतो/करते की मी सोशल मीडियाचा वापर अत्यंत जबाबदारीने आणि सजगतेने करेन. आभासी मोहापायी माझी वैयक्तिक गोपनीयता कधीही धोक्यात आणणार नाही. कोणत्याही संशयास्पद सायबर गुन्हेगाराला भीक न घालता कायदेशीर मार्गाने लढा देईन आणि माझ्या कुटुंबातील प्रत्येकाला सायबर-सुरक्षित बनवेन!"

📢 हे पुस्तक सर्वापर्यंत पोहोचवा!

राष्ट्रहित आणि सायबर सुरक्षा जनजागृतीसाठी ही संपूर्ण ई-बुक विनामूल्य उपलब्ध करून देण्यात आली आहे. आपल्या घरातील तरुण मुले, मुली, मित्रपरिवार आणि शाळे-कॉलेजच्या ग्रुप्समध्ये ही मोफत ई-बुक आवर्जून शेअर करा!

अधिकृत ई-बुक डाऊनलोड लिंक:

<https://dhavalhirapara.com/ebook>

👉 लेखकाशी थेट संवाद साधा:

- अधिकृत संकेतस्थळ: <https://dhavalhirapara.com/>
- सोशल कम्युनिटी: **Instagram / Facebook @dhavalhirapara1995**
- आपल्या प्रतिक्रिया आणि सायबर जनजागृती मोहीमेत सहभागी होण्यासाठी आमच्या सोशल मंचावर नक्की जुळा.

© २०२६ संकलन व अधिकार: धवल हिरपरा (Dhaval Hirapara)

सर्व हक्क राखीव. सायबर जनजागृतीसाठी निःशुल्क ई-बुक संस्करण.