



डिजिटल इंडिया में साइबर धोखाधड़ी पर अंकुश लगाना

06 अक्टूबर, 2025

"मैं एक ऐसे डिजिटल इंडिया का सपना देखता हूँ जहाँ साइबर सुरक्षा हमारी राष्ट्रीय सुरक्षा का अभिन्न अंग बन जाए"

- प्रधानमंत्री नरेन्द्र मोदी

प्रमुख तथ्य

- 86 प्रतिशत से अधिक घर अब इंटरनेट से जुड़े हुए हैं।
- भारत में साइबर सुरक्षा की घटनाएं वर्ष 2022 में 10.29 लाख से बढ़कर वर्ष 2024 में 22.68 लाख हो गईं।
- केंद्रीय बजट 2025-2026 में साइबर सुरक्षा परियोजनाओं के लिए 782 करोड़ रुपये आवंटित किए गए हैं।
- साइबर धोखाधड़ी से जुड़े 9.42 लाख से अधिक सिम कार्ड और 2,63,348 आईएमईआई को ब्लॉक कर दिया गया है।
- एक समर्पित हेल्पलाइन 1930 तत्काल साइबर सुरक्षा सहायता प्रदान करती है।

परिचय

भारत का साइबर स्पेस पहले से कहीं अधिक व्यस्त है, हर दिन करोड़ों लेन-देन और पारस्परिक कार्यकलाप किए जा रहे हैं। 86 प्रतिशत से अधिक परिवार अब इंटरनेट से जुड़े हुए हैं², जो डिजिटल इंडिया पहल के अंतर्गत उल्लेखनीय प्रगति को दर्शाता है। बढ़ते डिजिटल परिदृश्य ने नागरिकों को अपनी उंगलियों पर डिजिटल सेवाओं तक पहुंचने में सक्षम बनाया है। साथ ही, इसने साइबर धोखाधड़ी के लिए हमले की संभावनाओं को और भी प्रबल बना दिया है, जिससे साइबर सुरक्षा राष्ट्रीय प्राथमिकता बन गई है।

साइबर धोखाधड़ी डिजिटल प्लेटफॉर्म के माध्यम से की जाने वाली भ्रामक गतिविधियों को संदर्भित करती है जैसे कि अनाधिकृत पहुंच, डेटा चोरी या ऑनलाइन घोटाले, जिनका उद्देश्य अक्सर पीड़ितों को वित्तीय नुकसान पहुंचाना होता है।³

साइबर सुरक्षा घटनाओं में वर्ष 2022 में 10.29 लाख से वर्ष 2024 में 22.68 लाख तक की⁴ यह वृद्धि भारत में डिजिटल खतरों के बढ़ते पैमाने और जटिलता को दर्शाती है। साथ ही, वित्तीय टोल अधिक स्पष्ट होता जा रहा है, 28 फरवरी 2025 तक राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल (एनसीआरपी) पर साइबर धोखाधड़ी की सूचना

¹ <https://www.pib.gov.in/newsite/PrintRelease.aspx?relid=122920> (प्रेस विज्ञप्ति के अंत में)

² <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2132330>

³ <https://i4c.mha.gov.in/cyber-crime-categories.aspx> (ऑनलाइन वित्तीय धोखाधड़ी के तहत)

⁴ <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2153524>

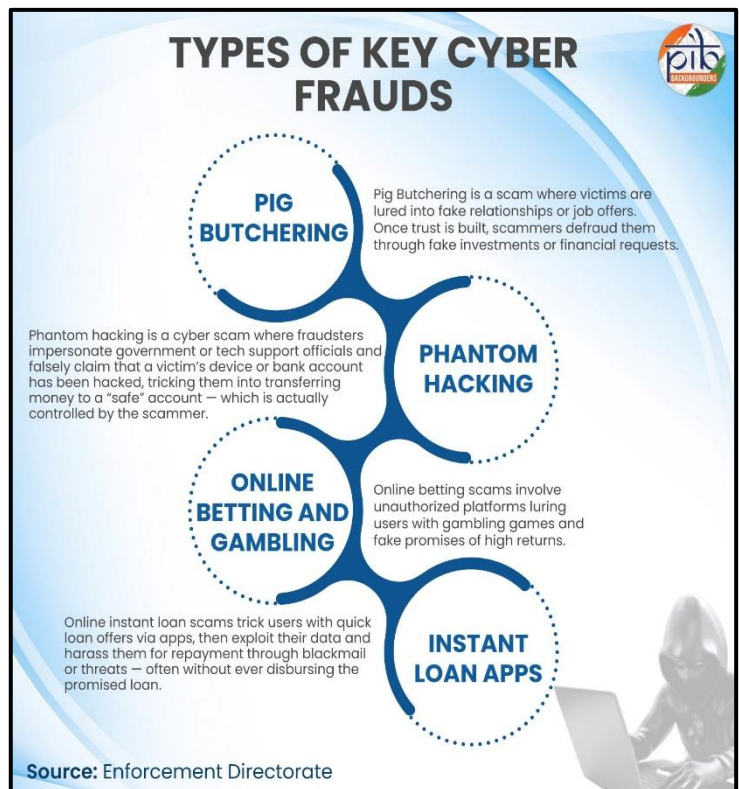
36.45 लाख रूपए है।⁵ जबकि यह संख्याएं बढ़ती चुनौतियों की ओर इशारा करती हैं, यह देश में जानकारी जुटाने और रिपोर्टिंग तंत्र में उल्लेखनीय प्रगति को भी उजागर करती हैं।

साइबर धोखाधड़ी पैटर्न का पता लगाना

साइबर धोखाधड़ी के उभरते परिदृश्य से पता चलता है कि धोखाधड़ी किसी एक ही तरीके तक सीमित नहीं है, बल्कि विविध रूप लेती है, जो अक्सर नई तकनीकों और उपयोगकर्ता व्यवहार को अपनाती है। निवारक उपायों को सक्षम करने के लिए इन पैटर्नों का मानचित्रण करना महत्वपूर्ण है। दुनिया भर में हैरान करने वाला यह वित्तीय प्रभाव धोखेबाजों की वैश्विक पहुंच और संगठित अपराध की भागीदारी को दर्शा रहा है, जो अक्सर दक्षिण पूर्व एशिया में धोखाधड़ी के नेटवर्क से जुड़ा होता है।⁶

उभरते साइबर खतरे

- स्फूफिंग जैसी तकनीकें, जहां अपराधी विश्वसनीय स्रोतों की तरह काम करते हैं, कई धोखाधड़ी रिपोर्टों में नज़र आते हैं। इसी तरह, एआई (आर्टिफिशियल इंटेलिजेंस) और फ़िशिंग का लाभ उठाने वाले डीपफेक के मामले, जहां व्यक्तियों को भ्रामक ईमेल या संदेशों के माध्यम से संवेदनशील जानकारी देने का लालच दिया जाता है, भी बढ़ रहे हैं⁷- और यह घोटालों के समग्र प्रभाव को बढ़ा रहे हैं।⁸
- 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। इस समस्या का समाधान करने के लिए, दूरसंचार विभाग (डीओटी) ने वित्तीय धोखाधड़ी जोखिम संकेतक (एफआरआई) की शुरुआत की, जो संदिग्ध संख्याओं को मध्यम, उच्च या बहुत उच्च जोखिम के रूप में वर्गीकृत करता है।⁹
- ऑनलाइन सट्टेबाजी ऐप के रूप में अवैध डिजिटल गतिविधियां भी सामने आई हैं, जो उपयोगकर्ताओं को बड़े रिटर्न के नकली वादे के साथ ऐसे गेम खेलने के लिए अपने ऑनलाइन वॉलेट में धन जमा करने का लालच देते हैं, जिससे आपराधिक आय में 400 करोड़ रूपए से अधिक की कमाई होती है।⁹



साइबर धोखाधड़ी के खिलाफ भारत की लड़ाई को मजबूत बनाते हुए, ऑनलाइन गेमिंग संवर्धन और विनियमन विधेयक, 2025 21 अगस्त 2025 को पारित किया गया। यह कानून ई-स्पोर्ट्स और सोशल ऑनलाइन गेम को

⁵ <https://www.data.gov.in/resource/stateut-wise-details-statistics-national-cyber-crime-reporting-portal-ncrp-related-cyber>

⁶ https://enforcementdirectorate.gov.in/sites/default/files/2025-05/Annual_Report_24-25.pdf (पृष्ठ 43 अंतिम पंक्ति)

⁷ https://enforcementdirectorate.gov.in/sites/default/files/2025-05/Annual_Report_24-25.pdf (पृष्ठ 48)

⁸ <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2130249>

⁹ https://enforcementdirectorate.gov.in/sites/default/files/2025-05/Annual_Report_24-25.pdf (पृष्ठ 46)

प्रोत्साहित करने के लिए डिज़ाइन किया गया है, जबकि यह ऑनलाइन मनी गेमिंग पर पूर्ण प्रतिबंध लगाता है, जिसमें उनके प्रचार, विज्ञापन और वित्तीय लेनदेन शामिल हैं।¹⁰

भारत का साइबर सुरक्षा ढांचा

भारत सरकार ने अपने विशाल ऑनलाइन समुदाय की सुरक्षा के उद्देश्य से मजबूत रक्षा तंत्र लागू किया है। भारतीय तेजी से अपने दैनिक जीवन में इंटरनेट को एकीकृत कर रहे हैं, व्यावसायिक लेन-देन, शिक्षा, वित्तीय गतिविधियों और सरकारी सेवाओं तक डिजिटल रूप से पहुंच जैसी आवश्यक जरूरतों के लिए इस पर भरोसा कर रहे हैं। 1,05,796 से अधिक पुलिस अधिकारी अब साइबर पोर्टल पर पंजीकृत हैं, जिसमें 82,704 से अधिक प्रमाण पत्र जारी किए गए हैं, जो फ्रंटलाइन कर्मियों को आवश्यक साइबर अपराध जांच कौशल से लैस करते हैं।¹¹

साइबर स्पेस को सुरक्षित करने वाले साइबर कानून

एक सुरक्षित डिजिटल वातावरण के महत्व को स्वीकार करते हुए, भारत का साइबर सुरक्षा ढांचा प्रमुख कानूनों पर आधारित है, विशेष रूप से:

- सूचना प्रौद्योगिकी अधिनियम, 2000 भारत के साइबर कानून ढांचे के आधार के रूप में कार्य करता है। यह पहचान की चोरी, प्रतिरूपण, कंप्यूटर संसाधनों के माध्यम से प्रतिरूपण द्वारा धोखाधड़ी और अश्लील या हानिकारक सामग्री के प्रसार को रोकता है। ये प्रावधान उन धोखेबाजों पर मुकदमा चलाने में महत्वपूर्ण हैं जो वित्तीय लाभ के लिए डिजिटल प्लेटफॉर्म का उपयोग करते हैं, साथ ही अधिकारियों को दुर्भावनापूर्ण वेबसाइटों और धोखाधड़ी वाले एप्लिकेशन को ब्लॉक करने के लिए भी सशक्त बनाते हैं।
- सूचना प्रौद्योगिकी (मध्यवर्ती दिशा-निर्देश और डिजिटल मीडिया आचार संहिता) नियम, 2021 सोशल मीडिया मध्यस्थों, डिजिटल प्लेटफॉर्म और ऑनलाइन मार्केटप्लेस की जवाबदेही सुनिश्चित करते हैं। यह एआई सहित प्रौद्योगिकियों के उभरते दुरुपयोग को संबोधित करता है और प्लेटफॉर्मों से गैर-कानूनी सामग्री को हटाने का आदेश देता है।
- डिजिटल व्यक्तिगत डेटा संरक्षण अधिनियम, 2023: इसके लिए आवश्यक है कि सभी व्यक्तिगत डेटा को कानूनी रूप से और उपयोगकर्ता की सहमति से सुरक्षित किया जाए, जिससे भारत का डिजिटल परिदृश्य सभी के लिए सुरक्षित और अधिक जवाबदेह हो सके। अधिनियम सुरक्षा उपायों को सुनिश्चित करने के लिए डेटा न्यासियों पर सख्त दायित्व रखता है, जिससे अनाधिकृत पहुंच या दुरुपयोग के जोखिम को कम किया जा सके।¹² अब तक धोखाधड़ी गतिविधियों से जुड़े 9.42 लाख से अधिक सिम कार्ड और 2,63,348 आईएमईआई (इंटरनेशनल मोबाइल इक्विपमेंट आइडेंटिटी) को ब्लॉक किया जा चुका है।¹³



¹⁰ <https://www.pib.gov.in/PressNoteDetails.aspx?PRID=2158408>

¹¹ <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2154268>

¹² <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2154268>

¹³ <https://www.pib.gov.in/PressReleaseDetail.aspx?PRID=2146786>

साइबर घटनाओं की जबाबदेही

इंडियन कंप्यूटर इमरजेंसी रिस्पांस टीम (सीईआरटी-इन) साइबर सुरक्षा घटनाओं से निपटने के लिए राष्ट्रीय एजेंसी है। यह साइबर खतरों की निगरानी करता है, कमजोरियों का पता लगाता है और आवश्यक सलाह जारी करता है। डेटा उल्लंघन, फ़िशिंग अभियान या मैलवेयर घुसपैठ जैसी घटनाओं की पहचान करने पर, सीईआरटी-इन अलर्ट प्रसारित करता है और प्रभावित संगठनों के लिए उपचारात्मक उपाय निर्धारित करता है। यह सक्रिय तंत्र जोखिमों की समय पर रोकथाम सुनिश्चित करता है और सरकार, उद्योग और महत्वपूर्ण सेवा प्रदाताओं में सरलता को बढ़ाता है। मार्च 2025 तक, सीईआरटी-इन ने साइबर तत्परता का आकलन करने और अनुकूल बनाने के लिए विभिन्न राज्यों और क्षेत्रों के 1,438 संगठनों को शामिल करते हुए 109 साइबर सुरक्षा मॉक ड्रिल की सुविधा प्रदान की।¹⁶

महत्वपूर्ण बुनियादी ढांचे की रक्षा करना

सूचना प्रौद्योगिकी अधिनियम, 2000 की धारा 70ए के तहत नामित राष्ट्रीय महत्वपूर्ण सूचना अवसंरचना संरक्षण केंद्र (एनसीआईआईपीसी), भारत में महत्वपूर्ण सूचना बुनियादी ढांचे के संरक्षण के लिए राष्ट्रीय नोडल एजेंसी है। यह बैंकिंग, दूरसंचार, बिजली और परिवहन जैसे क्षेत्रों में हितधारकों के साथ घनिष्ठ समन्वय में कार्य करता है, जो राष्ट्रीय सुरक्षा और सार्वजनिक सुरक्षा के लिए महत्वपूर्ण हैं। निरंतर निगरानी, जोखिम मूल्यांकन और क्षेत्र-विशिष्ट दिशानिर्देश जारी करने के माध्यम से, एनसीआईआईपीसी रक्षात्मक क्षमताओं को मजबूत करता है और उन खतरों को कम करता है जो अन्यथा आवश्यक सेवाओं से समझौता कर सकते हैं।

कानून प्रवर्तन क्षमता को मजबूत बनाना

गृह मंत्रालय के तहत स्थापित भारतीय साइबर अपराध समन्वय केंद्र (I4सी), कानून प्रवर्तन एजेंसियों (एलईएएस) को संगठित और समन्वित तरीके से साइबर अपराधों से निपटने में सक्षम बनाने के लिए एक व्यापक स्वरूप प्रदान करता है। यह विशेष प्रशिक्षण कार्यक्रमों, अनुसंधान और तकनीकी उपकरणों के विकास के माध्यम से क्षमता निर्माण का समर्थन करता है। यह वास्तविक समय में सूचना साझा करने और समन्वित जांच की सुविधा भी प्रदान करता है, जिससे वित्तीय धोखाधड़ी और अन्य संगठित साइबर अपराधों में शामिल साइबर आपराधिक नेटवर्क के खिलाफ प्रभावी कार्रवाई करने में सक्षम होता है। अब तक, आई4सी ने साइबर धोखाधड़ी से जुड़े 3,962 स्काइप आईडी और 83,668 व्हाट्सएप खातों को सक्रिय रूप से ब्लॉक कर दिया है।¹⁵

साइबर सुरक्षा पहल: शासन की कार्रवाई

भारत की साइबर सुरक्षा को मजबूत करने के प्रयास में, केंद्रीय बजट 2025 में साइबर सुरक्षा परियोजनाओं के लिए 782 करोड़ रुपये आवंटित किए गए हैं। यह महत्वपूर्ण कदम राष्ट्रीय सुरक्षा के लिए खतरा पैदा करने वाले साइबर खतरों पर सरकार के बढ़ते फोकस को उजागर करता है।¹⁶ सिटीजन फाइनैशियल साइबर फ्रॉड रिपोर्टिंग एंड मैनेजमेंट सिस्टम (सीएफसीएफआरएमएस) के माध्यम से, वित्तीय संस्थान 17.82 लाख से अधिक शिकायतों में 5,489 करोड़ रुपये से अधिक की बचत करने में सक्षम रहे हैं।¹⁷

राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल

¹⁴ <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2115416>

¹⁵ <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2112244>

¹⁶ <https://www.indiabudget.gov.in/doc/eb/vol1.pdf>

¹⁷ <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2158408>

साइबर अपराध के खिलाफ लड़ाई में नागरिकों की भागीदारी को मजबूत करने के लिए, सरकार ने राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल (www.cybercrime.gov.in) का संचालन किया है। यह पोर्टल नागरिकों को साइबर अपराध की विभिन्न श्रेणियों से संबंधित शिकायतों की रिपोर्ट करने में सक्षम बनाता है, जिसमें महिलाओं और बच्चों को लक्षित करने वाले अपराधों पर विशेष ध्यान दिया जाता है। एक समर्पित साइबर अपराध हेल्पलाइन नंबर **1930** ऑनलाइन वित्तीय धोखाधड़ी के पीड़ितों को त्वरित रिपोर्टिंग की सुविधा प्रदान करता है और जहां संभव हो, धोखाधड़ी वाले लेन-देन को फ्रीज करता है। साथ में, ये पहल नागरिकों के लिए एक सुलभ और उत्तरदायी शिकायत निवारण तंत्र के रूप में काम करती हैं।¹⁸

अंतःविषय साइबर-भौतिक प्रणालियों पर राष्ट्रीय मिशन (एनएम-आईसीपीएस)

एनएम-आईसीपीएस साइबर सुरक्षा, कृत्रिम बुद्धिमत्ता आदि में उन्नत अनुसंधान और नवाचार को बढ़ावा देकर साइबर धोखाधड़ी से निपटने में महत्वपूर्ण भूमिका निभाता है। खतरे का पता लगाने के लिए उपकरणों, प्लेटफॉर्मों और पद्धतियों के विकास का समर्थन करके, मिशन व्यक्तियों, व्यवसायों और महत्वपूर्ण बुनियादी ढांचे को लक्षित करने वाली साइबर धोखाधड़ी की पहचान करने और उन्हें रोकने की भारत की क्षमता को मजबूत करता है। एनएम-आईसीपीएस के तहत शैक्षणिक संस्थानों, उद्योग और सरकार के बीच सहयोग वित्तीय धोखाधड़ी, फिशिंग और पहचान-आधारित अपराधों सहित उभरते और परिष्कृत साइबर खतरों के समाधान में भी तेजी लाता है।¹⁹

महिलाओं और बच्चों के खिलाफ साइबर अपराध रोकथाम (सीसीपीडब्ल्यूसी) योजना

सीसीपीडब्ल्यूसी योजना कमजोर वर्गों, विशेष रूप से महिलाओं और बच्चों को लक्षित करने वाली साइबर धोखाधड़ी का समाधान प्रदान करती है। 132.93 करोड़ रुपये की वित्तीय सहायता के साथ, इस योजना ने 33 राज्यों और केंद्र शासित प्रदेशों में साइबर फॉरेंसिक-सह-प्रशिक्षण प्रयोगशालाओं की स्थापना की है। इन प्रयोगशालाओं ने साइबर अपराध जांच, डिजिटल फॉरेंसिक और निवारक उपायों में **24,600** से अधिक कर्मियों को प्रशिक्षित किया है। बढ़ी हुई जागरूकता, प्रारंभिक पहचान और त्वरित प्रतिक्रिया क्षमताओं के माध्यम से, सीसीपीडब्ल्यूसी ऑनलाइन धोखाधड़ी, घोटालों और महिलाओं और बच्चों के शोषण को रोकने के लिए कानून प्रवर्तन की क्षमता को मजबूत करता है, जिससे एक सुरक्षित डिजिटल वातावरण सुनिश्चित होता है।²⁰

साइबर संकट प्रबंधन योजना (सीसीएमपी)

साइबर हमलों और साइबर-आतंकवाद के खिलाफ तैयारियों को मजबूत करने के लिए, सरकार ने सभी सरकारी निकायों के लिए सीसीएमपी शुरू किया है। यह योजना किसी भी साइबर संकट से समन्वित रिकवरी सुनिश्चित करने के लिए एक रणनीतिक ढांचे के रूप में कार्य करती है। इस ढांचे के तहत क्षमता निर्माण और जागरूकता के लिए अब तक देश भर में 205 कार्यशालाएं आयोजित की जा चुकी हैं।²¹

समन्वय मंच

समन्वय प्लेटफॉर्म अपराधियों और अपराधों के विश्लेषण-आधारित अंतरराज्यीय संबंध प्रदान करके साइबर धोखाधड़ी धोखाधड़ी की जांच को मजबूत करता है। इसका 'प्रतिबिंब' मॉड्यूल अपराधियों और अपराध के बुनियादी ढांचे के स्थानों का मानचित्रण करता है, जिससे अधिकारियों को कार्रवाई योग्य जानकारी मिलती है। अब तक, इसने **12,987** आरोपियों की गिरफ्तारी, **1,51,984** आपराधिक संबंध और **70,584** साइबर जांच सहायता अनुरोधों को अंजाम दिया गया है, जिससे संगठित साइबर धोखाधड़ी नेटवर्क को कुशलतापूर्वक नष्ट करने में सहायता मिली है।²²

सहयोग पोर्टल

¹⁸ <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2085609>

¹⁹ <https://nmcps.gov.in/#mission>

²⁰ <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2152495>

²¹ <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2148943>

²² <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2152495>

सहयोग पोर्टल गैरकानूनी ऑनलाइन सामग्री का समाधान निकालने की दिशा में एक केंद्रीकृत मंच प्रदान करता है। यह बिचौलियों को हटाने के नोटिस को स्वचालित रूप से जारी करने में सक्षम बनाता है, जिससे साइबरस्पेस में प्रसारित होने वाली हानिकारक सामग्री के खिलाफ त्वरित कार्रवाई सुनिश्चित होती है। यह देश भर में सभी अधिकृत एजेंसियों को एक इंटरफेस पर एक साथ लाता है, जिससे समय पर गैर-कानूनी सामग्री का प्रभावी ढंग से जवाब देने की सरकार की क्षमता मजबूत होती है।²³

साइबर सुरक्षा अभ्यास

भारत राष्ट्रीय साइबर सुरक्षा अभ्यास 2025 21 जुलाई से 01 अगस्त तक आयोजित किया गया था, जो अपनी साइबर अनुकूलता को मजबूत बनाने के लिए भारत की प्रतिबद्धता की पुष्टि करता है। इस अभ्यास में साइबर सुरक्षा पेशेवरों, नियामकों और नीति निर्माताओं सहित 600 से अधिक प्रतिभागियों ने भाग लिया। इस अभ्यास का मुख्य आकर्षण एसटीआरएटीईएक्स था, यह एक राष्ट्रीय साइबर उल्लंघन के रूप में वास्तविक समय अंतर-एजेंसी समन्वय और निर्णय लेने का परीक्षण करने के लिए डिज़ाइन किया गया था।²⁴



इंडिया मोबाइल कांग्रेस 2025 में साइबर सुरक्षा पर विशेष रूप से ध्यान

9वें इंडिया मोबाइल कांग्रेस में, साइबर सुरक्षा प्रमुख ध्यान देने वाले क्षेत्रों में से एक है और यह डिजिटल नेटवर्क और उभरती प्रौद्योगिकियों को साइबर खतरों से बचाने के भारत के प्रयासों का उल्लेख करती है। प्रधानमंत्री श्री नरेन्द्र मोदी द्वारा 8 से 11 अक्टूबर तक यशोभूमि, नई दिल्ली में "इनोवेट टू ट्रांसफॉर्म" विषय पर आईएमसी 2025 का उद्घाटन किया जाएगा।

आईएमसी 2025 में साइबर सुरक्षा शिखर सम्मेलन और भारत 6जी संगोष्ठी सहित छह वैश्विक शिखर सम्मेलनों का आयोजन किया जाएगा। यह सम्मेलन अगली पीढ़ी की डिजिटल प्रौद्योगिकियों में भारत के बढ़ते नेतृत्व की जानकारी प्रदान करते हैं। प्रमुख ध्यान दिए जाने वाले क्षेत्रों में 6जी, साइबर सुरक्षा, उपग्रह संचार, एआई, आईओटी और दूरसंचार विनिर्माण शामिल हैं।

इस कार्यक्रम में 1.5 लाख से अधिक आगंतुकों, 7,000 से अधिक अंतर्राष्ट्रीय प्रतिनिधियों, 400 से अधिक प्रदर्शकों और 1,600 से अधिक अत्याधुनिक उपयोग के मामलों को प्रदर्शित किए जाने की आशा है। 100 से अधिक सत्रों और 800 से अधिक वक्ताओं के साथ, आईएमसी 2025 वैश्विक सहयोग और नवाचार के लिए एक प्रमुख मंच के रूप में कार्य करेगा।

जैसा कि भारत अपने 1.2 बिलियन मोबाइल ग्राहकों और 970 मिलियन इंटरनेट उपयोगकर्ताओं के साथ त्वरित 5जी रोलआउट का उत्सव मना रहा है और यह सुरक्षित, समावेशी और स्केलेबल डिजिटल इकोसिस्टम पर ध्यान केंद्रित करते हुए विश्वसनीय तथा परिवर्तनकारी डिजिटल बुनियादी ढांचे के लिए वैश्विक केंद्र के रूप में देश की स्थिति को मजबूत करता है।

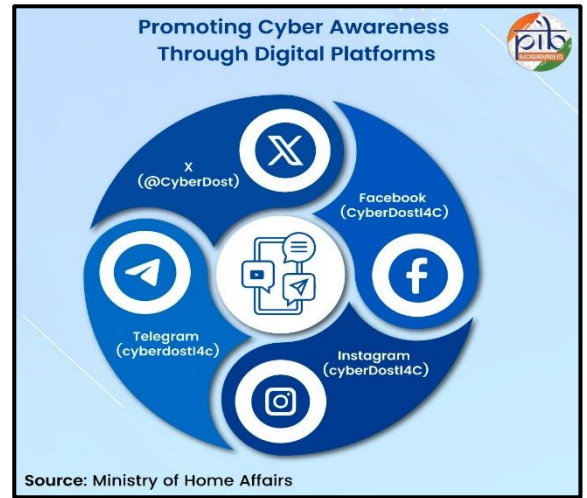
भविष्य का मार्ग: साइबर जागरूकता

²³ <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2154268>

²⁴ <https://www.pib.gov.in/PressReleaseDetail.aspx?PRID=2151613>

साइबर अपराधों के बारे में जन जागरूकता को सुदृढ़ करने के लिए सरकार ने एक बहु-मंच पहुंच रणनीति अपनाई है।

- सरकार ने साइबर धोखाधड़ी के बारे में लोगों को आगाह करने के लिए रेडियो, अखबारों और मेट्रो घोषणाओं के माध्यम से नागरिक-केंद्रित पहुंच अभियान शुरू किया है।
- वर्तमान और संभावित साइबर सुरक्षा खतरों के बारे में आवश्यक स्थितिजन्य जागरूकता पैदा करने के लिए सीईआरटी-इन द्वारा राष्ट्रीय साइबर समन्वय केंद्र (एनसीसीसी) (एनसीसीसी) की स्थापना की गई है।
- माईगांव प्लेटफॉर्म के माध्यम से साइबर सुरक्षा और सुरक्षा जागरूकता सप्ताह आयोजित करके जनता को शामिल करना।
- किशोरों और छात्रों के लिए एक पुस्तिका साइबर सुरक्षा और सुरक्षा पर युवाओं का मार्गदर्शन करने के लिए प्रकाशित की गई है।
- साइबर अपराध को रोकने के लिए साइबर जागरूकता और सुरक्षित प्रथाओं को फैलाने के लिए सोशल मीडिया का उपयोग।²⁵



निष्कर्ष

भारत डिजिटल परिवर्तन और साइबर खतरों के चौराहे पर है, जहां यह प्रगति का लौह स्तंभ बन चुका है तो वहीं यह साइबर धोखेबाजों को भी मौका दे रहा है। डिजिटल इंडिया के विजन को साकार करते हुए, सरकार की बहुस्तरीय साइबर प्रतिक्रिया टीम धोखाधड़ी की रोकथाम की सुविधा प्रदान कर रही है और हजारों घोटाले से जुड़े अवैध कृत्यों को रोक रही है। उन्नत फॉरेंसिक, बिग डेटा एनालिटिक्स और स्वदेशी उपकरणों ने राष्ट्रीय साइबर सुरक्षा को मजबूत किया है। फिर भी, भारत के साइबरस्पेस को सुरक्षित करना एक साझा जिम्मेदारी है जहां सरकार और नागरिकों को साइबर धोखाधड़ी के खिलाफ इस लड़ाई में एक साथ मिलकर कार्य करना चाहिए।

संदर्भ

सांख्यिकी एवं कार्यक्रम कार्यान्वयन मंत्रालय

- <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2132330>

इलेक्ट्रानिक्स एवं आईटी मंत्रालय

- <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2154268>
- <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2115416>
- <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2051934>

गृह मंत्रालय

- <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2112244>
- <https://www.pib.gov.in/PressReleaseDetail.aspx?PRID=2146786>
- <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2152495>
- <https://www.pib.gov.in/PressReleaseFramePage.aspx?PRID=2110359>

²⁵ <https://www.pib.gov.in/PressReleaseDetail.aspx?PRID=2146786>

- <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2101613>
- <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2158408>

संचार एवं सूचना प्रौद्योगिकी मंत्रालय

- <https://www.pib.gov.in/PressReleaseDetailm.aspx?PRID=2153524>
- <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2130249>

Ministry of Women and Child Development

- <https://www.pib.gov.in/PressReleasePage.aspx?PRID=2085609>

PIB Backgrounders

- <https://www.pib.gov.in/PressNoteDetails.aspx?NoteId=155075&ModuleId=3>

विश्व आर्थिक मंच

- <https://www.weforum.org/stories/2024/04/cybercrime-target-sectors-cybersecurity-news/>

राष्ट्रीय सुरक्षा परिषद सचिवालय

- <https://www.pib.gov.in/PressReleaseDetailm.aspx?PRID=2151613>

प्रवर्तन निदेशालय (ईडी) की वार्षिक रिपोर्ट **2024-2025**

- https://enforcementdirectorate.gov.in/sites/default/files/2025-05/Annual_Report_24-25.pdf

भारत का बजट

- <https://www.indiabudget.gov.in/doc/eb/vol1.pdf>

अंतःविषय साइबर-भौतिक प्रणालियों पर राष्ट्रीय मिशन (एनएम-आईसीपीएस)

- <https://nmicps.gov.in/#mission>

भारतीय साइबर अपराध समन्वय केंद्र (I4C)

- <https://i4c.mha.gov.in/cyber-crime-categories.aspx>

ओपन गवर्नमेंट डेटा प्लेटफॉर्म (OGD) इंडिया

- <https://www.data.gov.in/resource/stateut-wise-details-statistics-national-cyber-crime-reporting-portal-ncrp-related-cyber>

पीके/केसी/एसएस/एसएस