BACKGROUNDERS
Press Information Bureau
Government of India

IMEI से छेड़छाड़

डिजिटल संप्रभुता के लिए खतरा

23 सितंबर 2026

भारत का बढ़ता डिजिटल इकोसिस्टम और सुरक्षित डिवाइसों की आवश्यकता

भारत में तेजी से हो रहे डिजिटल बदलाव ने दूरसंचार को रोजमर्रा की जिंदगी, व्यापार और शासन (गवर्नेंस) का अहम हिस्सा बना दिया है। जुलाई 2026 में देश में सक्रिय वायरलेस मोबाइल सब्सक्राइबरों की संख्या 1,204.01 मिलियन तक पहुंच गई। सब्सक्राइबरों की यह बड़ी संख्या भारत के जुड़े हुए डिजिटल इकोसिस्टम के बड़े दायरे को दिखाती है। मोबाइल नेटवर्क और डिवाइस तेजी से डिजिटल पेमेंट, ऑनलाइन सेवाओं और नागरिकों पर केंद्रित शासन (गवर्नेंस) को समर्थन दे रहे हैं। जैसे-जैसे इन तकनीक पर निर्भरता बढ़ रही है, दूरसंचार नेटवर्क और डिवाइस की सुरक्षा और अखंडता (इंटीग्रिटी) सुनिश्चित करना और भी आवश्यक हो गया है।

यह बढ़ता हुआ डिजिटल इकोसिस्टम सुरक्षा से जुड़ी नई चुनौतियां भी लाता है। ऐसी ही एक चिंता इंटरनेशनल मोबाइल इक्विपमेंट आइडेंटिटी (IMEI) नंबर का गलत इस्तेमाल है। IMEI नंबर के साथ छेड़छाड़ या उनके गलत इस्तेमाल से बदली हुई पहचान वाले डिवाइस का इस्तेमाल आसान हो सकता है और दूरसंचार नेटवर्क पर डिवाइस की पहचान करना मुश्किल हो सकता है। ऐसी हरकतें कानून लागू करने वाली एजेंसियों, उपभोक्ता सुरक्षा और नेटवर्क सुरक्षा के लिए चुनौतियां पैदा कर सकती हैं। इसलिए, एक सुरक्षित, भरोसेमंद और मजबूत दूरसंचार इकोसिस्टम बनाए रखने के लिए डिवाइस आइडेंटिफायर (पहचानकर्ता) की अखंडता को मजबूत करना जरूरी है।

IMEI के साथ गैर-कानूनी छेड़छाड़ क्या है?

अगर कोई व्यक्ति ऐसा करता है तो यह गैर-कानूनी होगा:

- जानबूझकर मोबाइल डिवाइस इक्विपमेंट आइडेंटिफिकेशन नंबर (IMEI) को हटाता है, मिटाता है या बदलता है; या
- जानबूझकर ऐसा हार्डवेयर या सॉफ्टवेयर इस्तेमाल करता है, बनाता है, उसकी तस्करी करता है, उस पर नियंत्रण या कब्जा रखता है, जिसके बारे में उसे पता है कि उसे ऊपर बताए गए तरीके से आकार दिया गया (कॉन्फ़िगर किया गया) है।

IMEI को समझना

- **IMEI क्या है?** IMEI एक खास 15 अंकों का नंबर है जो दूरसंचार नेटवर्क पर मोबाइल डिवाइस की पहचान करता है।
- **TAC का क्या मतलब है?** IMEI के शुरुआती आठ अंक 'टाइप एलोकेशन कोड' (टीएसी) बनाते हैं, जो डिवाइस के मॉडल या प्रकार की पहचान करते हैं।
- **IMEI नंबर कौन देता है?** 'ग्लोबल सिस्टम फॉर मोबाइल कम्युनिकेशंस एसोसिएशन' (जीएसएमए) टीएसी के वैश्विक आवंटन (एलोकेशन) की देखरेख करता है।
- **IMEI कैसे दिए जाते हैं?** जीएसएमए मैन्युफैक्चरर्स और ब्रांड मालिकों को टीएसी देता है। इसके बाद विनिर्माताओं अलग-अलग डिवाइस को खास आईएमईआई नंबर देते हैं।
- **डुअल-सिम फोन में कितने IMEI होते हैं?** डुअल-सिम फोन में आम तौर पर दो IMEI नंबर -हर सिम स्लॉट के लिए एक- होते हैं।
- **यूजर्स अपना IMEI कैसे पता कर सकते हैं?** यूजर्स अपने मोबाइल डिवाइस पर *#06# डायल करके उसका IMEI नंबर देख सकते हैं।

- **यूजर्स IMEI को कैसे वेरिफाई कर सकते हैं?** डिवाइस की जानकारी वेरिफाई करने के लिए यूजर्स 'संचार साथी' पोर्टल या मोबाइल ऐप पर जा सकते हैं, या 14422 पर SMS के जरिए 'KYM <15-अंकों का IMEI नंबर>' भेज सकते हैं।

सुरक्षा के प्रति सबकी जवाबदेही

एक सुरक्षित दूरसंचार इकोसिस्टम के लिए डिवाइस के पूरे लाइफसाइकिल-यानी विनिर्माण से लेकर रोजमर्रा के इस्तेमाल तक-जिम्मेदारी की आवश्यकता होती है। आईएमईआई के गलत इस्तेमाल को रोकने में विनिर्माताओं, आयातकों, विक्रेताओं और नागरिकों, सभी की भूमिका होती है।

- **विनिर्माताओं को** भारत में बनने वाले सभी संबंधित दूरसंचार डिवाइस के IMEI नंबरों को पहली बार बेचने, टेस्टिंग, रिसर्च या किसी और इस्तेमाल से पहले सरकार के पास पंजीकरण करना होगा। यह पंजीकरण 'डिवाइस सेतु-इंडियन काउंटरफीटेड डिवाइस रिस्ट्रिक्शन (आईसीडीआर)' पोर्टल के जरिए किया जाता है। विनिर्ताओं को यह भी पक्का करना होगा कि डिवाइस को सही, विशेष और बिना छेड़छाड़ वाले IMEI नंबर दिए जाएं।

- **आयातकों** को भारत में संबंधित दूरसंचार उपकरण आयात इंपोर्ट करने से पहले केंद्र सरकार के पास IMEI नंबर पंजीकृत करने होंगे। बिक्री, टेस्टिंग, आरएंडडी या दूसरे कामों के लिए लाए जाने वाले डिवाइस का पंजीकरण 'डिवाइस सेतु-ICDR' पोर्टल के जरिए पूरा किया जाना चाहिए। आयातकों को यह पक्का करना होगा कि आयात की गईं डिवाइस पर सही और अधिकृत IMEI नंबर हों।
- **रीसेलर्स और रिटेलर्स** को यह पक्का करना होगा कि बिक्री के लिए रखी गईं दूरसंचार डिवाइस पर सही और बिना छेड़छाड़ वाले आईएमईआई नंबर हों। जो लोग इस्तेमाल किए गए डिवाइस का व्यापार करते हैं, उन्हें ट्रांजैक्शन पूरा करने से पहले, हर आईएमईआई वेरिफिकेशन के लिए तय फीस देकर, सरकार के सेंट्रल डेटाबेस (जिसमें छेड़छाड़ किए गए और ब्लैकलिस्टेड डिवाइस की जानकारी होती है) से IMEI की जांच करनी चाहिए। छेड़छाड़ किए गए या कॉन्फ़िगर किए जा सकने वाले IMEI वाले डिवाइस बेचने या उनका व्यापार करने पर सख्त कानूनी कार्रवाई हो सकती है।

- ब्रांड मालिकों को यह पक्का करना होगा कि उनके ब्रांड के तहत बेचे जाने वाले डिवाइस, IMEI पंजीकरण और साइबर सुरक्षा से जुड़ी जरूरी शर्तों को पूरा करते हों। उनके ब्रांड 'डिवाइस सेतु-आईसीडीआर' पोर्टल पर सही तरीके से पंजीकृत होने चाहिए और संबंधित जीएसएमए टाइप

एलोकेशन कोड (टीएसी) से जुड़े होने चाहिए। उन्हें यह पक्का करना चाहिए कि बाज़ार में लाए गए डिवाइस पर असली और अधिकृत आईएमईआई हों।

नागरिकों को किन चीजों से बचना चाहिए

दूरसंचार विभाग (डीओटी) नागरिकों को सलाह देता है कि वे ऐसी गतिविधियों से बचें जिनमें टेलीकम्युनिकेशन आइडेंटिफायर और संसाधनों के साथ छेड़छाड़ या उनका गलत इस्तेमाल शामिल हो:

- कॉन्फिगर किए जा सकने वाले या छेड़छाड़ किए गए आईएमईआई वाले डिवाइस, जैसे कि मॉडेम, मॉड्यूल, सिम बॉक्स या अन्य उपकरण का इस्तेमाल करना, उन्हें हासिल करना या असेंबल करना।
- नकली दस्तावेजों, धोखाधड़ी, जालसाजी या किसी और का रूप धरकर सिम कार्ड हासिल करना।
- अपने नाम पर लिए गए सिम कार्ड को दूसरों को हस्तांतरित करना, बेचना या सौंपना, जो उनका गलत इस्तेमाल कर सकते हैं।
- कॉलिंग लाइन आइडेंटिटी (सीएलआई) या अन्य टेलीकम्युनिकेशन आइडेंटिफायर में बदलाव करने के लिए मोबाइल एप्लिकेशन, वेबसाइट या किसी अन्य तरीके का इस्तेमाल करना।

संचार साथी प्लेटफॉर्म

नागरिक अपने मोबाइल हैंडसेट को वेरिफाई और सुरक्षित करने के लिए संचार साथी प्लेटफॉर्म का इस्तेमाल कर सकते हैं। यह प्लेटफॉर्म यूजर्स को डिवाइस की IMEI जानकारी (जैसे ब्रांड, मॉडल और निर्माता) को वेरिफाई करने की सुविधा देता है, जिससे डिवाइस की असलियत और सुरक्षा को मजबूत करने में मदद मिलती है। संचार साथी ऐप के बारे में और जानें।

नागरिकों को क्या करना चाहिए

उपभोक्ताओं को अपने डिवाइस की सुरक्षा के लिए सावधानी बरतनी चाहिए और यह पक्का करना चाहिए कि उनके IMEI नंबर असली और सुरक्षित रहें।

- मोबाइल डिवाइस सिर्फ अधिकृत विक्रेताओं से ही खरीदें और IMEI की जानकारी की जांच करें।
- हैंडसेट को सुरक्षित रखने के लिए मजबूत पासवर्ड, पिन या बायोमेट्रिक ऑथेंटिकेशन का इस्तेमाल करें।

- IMEI के साथ छेड़छाड़ या किसी अन्य गलत गतिविधि के जोखिम को कम करने के लिए डिवाइस को सिर्फ अधिकृत सर्विस सेंटर पर ही ठीक करवाएं।
- डिवाइस खो जाने या चोरी हो जाने की स्थिति में, ब्लॉक करने की आधिकारिक प्रक्रिया का पालन करें:
  i) स्थानीय पुलिस के पास तुरंत रिपोर्ट दर्ज कराएं और शिकायत की एक कॉपी ले लें।
  ii) अपने दूरसंचार ऑपरेटर से खोए हुए मोबाइल नंबर के लिए डुप्लीकेट सिम कार्ड लें। (ट्राई के नियमों के तहत, दोबारा जारी किए गए सिम के एक्टिवेशन के पहले 24 घंटों के लिए एसएमएस सेवाएं सीमित रहती हैं। चूंकि संचार साथी के लिए मोबाइल ओटीपी वेरिफिकेशन की जरूरत होती है, इसलिए अपना अनुरोध जमा करने के लिए आपको एक्टिवेशन के बाद 24 घंटे इंतजार करना होगा)।
  iii) संचार साथी (सीईआईआर) पोर्टल या मोबाइल ऐप पर ब्लॉक करने का अनुरोध दर्ज करें; इसके लिए पुलिस रिपोर्ट और वैध आईडी प्रूफ अपलोड करें ताकि एक विशेष अनुरोध आईडी मिल सके।
  iv) अगर बाद में आपकी डिवाइस मिल जाती है, तो पहले स्थानीय पुलिस को इसकी सूचना दें और फिर हैंडसेट को सुरक्षित रूप से अनब्लॉक करने के लिए पोर्टल पर अपनी अनुरोध आईडी का इस्तेमाल करें।

डिवाइस की सुरक्षा बनाए रखना पूरे दूरसंचार इकोसिस्टम की सामूहिक जिम्मेदारी है। जागरूकता, नियमों का पालन और जिम्मेदार इस्तेमाल से धोखाधड़ी को रोकने, नागरिकों की सुरक्षा करने और भारत के डिजिटल इंफ्रास्ट्रक्चर की सुरक्षा को मज़बूत करने में मदद मिल सकती है।

IMEI के साथ छेड़छाड़ के खिलाफ कानूनी सुरक्षा उपाय[1&2]

भारत ने दूरसंचार इकोसिस्टम की सुरक्षा और अखंडता बनाए रखने के लिए एक मजबूत कानूनी ढांचा तैयार किया है।

- **टेलीकम्युनिकेशन एक्ट, 2023** में टेलीकम्युनिकेशन आइडेंटिफायर्स (जैसे मोबाइल हैंडसेट और अन्य टेलीकम्युनिकेशन डिवाइस के IMEI नंबर) के साथ छेड़छाड़ करने पर सख्त कार्रवाई का प्रावधान है।

[1] https://www.pib.gov.in/PressReleaseDetail.aspx?PRID=2305203&reg=3&lang=1
[2] https://www.pib.gov.in/PressReleasePage.aspx?PRID=2190763&reg=48&lang=2

- धारा 42(3)(c) टेलीकम्युनिकेशन आइडेंटिफायर्स के साथ छेड़छाड़ करने पर रोक लगाती है। धारा 42(3)(e) धोखाधड़ी, जालसाजी या किसी और का रूप धरकर सब्सक्राइबर आइडेंटिटी मॉड्यूल (SIM) या टेलीकम्युनिकेशन आइडेंटिफायर्स हासिल करने पर रोक लगाती है।
- नियमों का उल्लंघन करने पर तीन साल तक की जेल, ₹50 लाख तक का जुर्माना या दोनों हो सकते हैं। एक्ट की धारा 42(7) के तहत ऐसे अपराध संज्ञेय और गैर-जमानती हैं।
- धारा 42(6) के तहत, जो लोग ऐसे अपराध करने में मदद या बढ़ावा देते हैं, उन्हें भी वैसी ही सजा हो सकती है।

ये प्रावधान IMEI के साथ छेड़छाड़ और दूरसंचार संसाधनों के गलत इस्तेमाल को रोकने के लिए एक मजबूत रोकथाम का उपाय बनाते हैं।

भारत के डिजिटल भविष्य की सुरक्षा

भारत की दूरसंचार यात्रा शानदार प्रगति और साझा जिम्मेदारी, दोनों को दर्शाती है। मजबूत कानून, वेरिफिकेशन टूल और नागरिकों की जागरूकता मिलकर इस नेटवर्क को सुरक्षित और भरोसेमंद बनाते हैं। सरकार, उद्योग और आम यूजर्स समेत हर हितधारक की इस भरोसे को बनाए रखने में भूमिका है। जागरूक और जानकारी रखने वाले नागरिक ही इसके गलत इस्तेमाल के खिलाफ सबसे मजबूत सुरक्षा कवच हैं। लगातार सहयोग से ही आने वाली पीढ़ियों के लिए भारत की डिजिटल कनेक्टिविटी सुरक्षित रहेगी।

संदर्भ:

Ministry of Communications

- https://www.pib.gov.in/PressReleaseDetail.aspx?PRID=2305203&reg=3&lang=1
- https://www.ceir.gov.in/Home/index.jsp
- https://www.pib.gov.in/PressReleasePage.aspx?PRID=2190763&reg=48&lang=2
- https://www.pib.gov.in/PressReleasePage.aspx?PRID=2190763&reg=48&lang=2
- https://www.pib.gov.in/PressReleasePage.aspx?PRID=2190763&reg=48&lang=2
- https://www.eservices.dot.gov.in/sites/default/files/circular-notifications/cybersecurity-rules-2024.pdf
- https://www.eservices.dot.gov.in/sites/default/files/circular-notifications/telecom-cyber-security-amendment-rules-2025.pdf
- https://www.pib.gov.in/PressReleasePage.aspx?PRID=2193461&lang=2&reg=3&utm_source
- https://www.pib.gov.in/PressReleasePage.aspx?PRID=1598008&lang=2&reg=3&utm_source

Telecom Regulatory Authority of India

- www.trai.gov.in/sites/default/files/2026-08/PR_No116of2026_0.pdf

PIB Research

पीके/केसी/एमपी