समाचार वाणी
ख़बर जो करें असर !

नाशिक | Thursday, 24 September 2026

पहचान नहीं छिपा सकेगें स्पैमर्स और स्कैमर्स: मोबाइल करेगा असली कॉलर का खुलासा, CNAP सेवा का ट्रायल शुरू

Publisher

Published on 08 Nov 2025

अब स्पैमर्स और स्कैमर्स के दिन लदने वाले हैं। जल्द ही कोई भी फर्जी पहचान या नकली नाम से कॉल करने वाला व्यक्ति अपनी पहचान छिपा नहीं सकेगा, क्योंकि आपका मोबाइल खुद उस कॉलर की असली जानकारी उजागर करेगा। भारत में अब कॉलिंग नेम प्रेजेंटेशन (CNAP) नाम की एक नई तकनीक का ट्रायल शुरू हो गया है, जिससे मोबाइल यूजर ट्रू कॉलर जैसे थर्ड पार्टी ऐप के बिना ही कॉल करने वाले का वास्तविक नाम देख सकेंगे।

यह पहल भारत सरकार के दूरसंचार विभाग (DoT) के निर्देशन में शुरू की गई है। इस सेवा के तहत यदि कोई कॉल किसी ऐसे नंबर से आए जो आपके फोन में सेव नहीं है, तो स्क्रीन पर उस व्यक्ति या संस्था का वास्तविक नाम दिखाई देगा, जो उस मोबाइल नंबर के साथ रजिस्टर्ड है। इससे फर्जी कॉल, ठगी, और साइबर फ्रॉड जैसे अपराधों पर प्रभावी रोक लगाने की उम्मीद की जा रही है।

इकोनॉमिक टाइम्स की रिपोर्ट के अनुसार, CNAP सेवा का ट्रायल फिलहाल हरियाणा और हिमाचल प्रदेश सर्किल में शुरू किया गया है। रिलायंस जियो (Reliance Jio), वोडाफोन आइडिया (Vi) और बीएसएनएल (BSNL) जैसी प्रमुख टेलीकॉम कंपनियां हरियाणा में इस सेवा का परीक्षण कर रही हैं, जबकि भारती एयरटेल (Bharti Airtel) ने हिमाचल प्रदेश सर्किल में इसकी टेस्टिंग शुरू की है। सफल ट्रायल के बाद इसे अगले साल पूरे देश में लागू करने की योजना है।

इस तकनीक का मकसद देशभर में तेजी से बढ़ रहे स्पैम और स्कैम कॉल्स की समस्या को खत्म करना है। आए दिन ऐसी शिकायतें सामने आती हैं कि फर्जी नाम या नकली आईडी का इस्तेमाल करके कॉल करने वाले लोगों ने आम नागरिकों को ठगा या परेशान किया। ट्रू कॉलर जैसे ऐप्स ने इस समस्या को कुछ हद तक कम किया, लेकिन ये ऐप्स हमेशा सटीक जानकारी नहीं दिखाते और यूजर की प्राइवेसी को लेकर भी कई सवाल उठे। CNAP के लागू होने से यह जानकारी सीधे मोबाइल नेटवर्क से आएगी, जिससे डेटा का दुरुपयोग नहीं होगा और कॉलर की पहचान की पूरी पारदर्शिता बनी रहेगी।

टेलीकॉम विशेषज्ञों के अनुसार, CNAP तकनीक न केवल यूजर्स की सुरक्षा बढ़ाएगी बल्कि सरकार के 'डिजिटल सेफ्टी मिशन' को भी गति देगी। एक बार जब यह सुविधा पूरे देश में लागू हो जाएगी, तो मोबाइल यूजर्स को कॉल उठाने से पहले ही यह पता चल जाएगा कि कॉल किस नाम से रजिस्टर्ड व्यक्ति या संस्था की ओर से आ रही है। इससे साइबर अपराध, बैंकिंग फ्रॉड और फर्जी निवेश योजनाओं से जुड़ी कॉल्स की संख्या में उल्लेखनीय कमी आने की उम्मीद है।

रिपोर्ट्स के मुताबिक, CNAP ट्रायल के दौरान यूजर्स को मोबाइल स्क्रीन पर कॉल आने पर नंबर के साथ-साथ उस कॉलर का नाम भी दिखाई देगा। उदाहरण के तौर पर, अगर किसी बैंक के कस्टमर केयर से कॉल आती है, तो कॉलर आईडी पर "State Bank of India" जैसे नाम दिखाई देंगे। इसी तरह, किसी निजी व्यक्ति का कॉल आएगा तो उसके रजिस्टर्ड नाम से कॉल की पहचान होगी।

हालांकि, विशेषज्ञों का कहना है कि इस सेवा को लागू करने से पहले टेलीकॉम कंपनियों को कुछ तकनीकी और गोपनीयता से जुड़ी चुनौतियों का समाधान करना होगा। कॉल डेटा को सुरक्षित रखना और यूजर्स की जानकारी की प्राइवेसी बनाए रखना इसके सफल संचालन की प्राथमिक शर्त होगी।

डिपार्टमेंट ऑफ टेलीकम्युनिकेशन (DoT) ने सभी प्रमुख टेलीकॉम ऑपरेटरों को इस प्रोजेक्ट का हिस्सा बनने के लिए कहा है। मंत्रालय ने यह भी सुनिश्चित करने के निर्देश दिए हैं कि CNAP सेवा लागू होने पर यूजर डेटा को किसी भी थर्ड पार्टी के साथ साझा नहीं किया जाएगा।

उद्योग जगत में CNAP को भारत के डिजिटल सुरक्षा ढांचे में एक बड़ा कदम माना जा रहा है। मोबाइल उपयोगकर्ताओं के लिए यह एक बड़ी राहत साबित हो सकती है क्योंकि यह सुविधा आने के बाद उन्हें बार-बार स्पैम कॉल्स, धोखाधड़ी और फर्जी प्रचार कॉल्स से निजात मिलेगी।

यदि ट्रायल सफल रहता है, तो अगले साल यानी 2026 की शुरुआत तक CNAP सेवा पूरे भारत में उपलब्ध हो सकती है। यह सेवा मोबाइल संचार के क्षेत्र में एक ऐतिहासिक बदलाव लेकर आएगी और भारत को उन देशों की सूची में शामिल कर देगी जहां कॉलिंग ट्रांसपेरेंसी को कानूनी रूप से लागू किया गया है।

साइबर सिक्योरिटी विशेषज्ञों का कहना है कि CNAP से न केवल डिजिटल विश्वास बढ़ेगा, बल्कि यह कदम भारत को सुरक्षित डिजिटल इकोसिस्टम की दिशा में एक और मजबूत कदम साबित होगा। आने वाले समय में CNAP सेवा मोबाइल उपयोगकर्ताओं के लिए "डिजिटल सुरक्षा कवच" की तरह काम कर सकती है।

DISCLAIMER: the views/contents expressed/presented herein, within this advertorial and promotional feature are the sole and exclusive responsibility of individual clients/expert/their authorised representative/Publisher, to which effect, publication house/its representative/affiliates are not responsible/liable whatsover.