भारत सरकार
संचार मंत्रालय
दूरसंचार विभाग

राज्य सभा
तारांकित प्रश्न संख्या *141
उत्तर देने की तारीख 12 फरवरी, 2026

साइबर/दूरसंचार धोखाधड़ी में कमी

***141. श्री नीरज डांगी**

क्या **संचार** मंत्री यह बताने की कृपा करेंगे किः

(क) डिजिटल इंटेलिजेंस प्लेटफॉर्म के माध्यम से अब तक कितने फर्जी/संदिग्ध कनेक्शनों या खातों की पहचान कर कार्रवाई की गई है;
(ख) क्या इस प्लेटफॉर्म के कारण साइबर/दूरसंचार धोखाधड़ी में कमी आई है और यदि हां, तो तत्संबंधी ब्यौरा क्या है;
(ग) किन-किन मंत्रालयों/विभागों और एजेंसियों को प्लेटफॉर्म से एकीकृत किया गया है; और
(घ) उक्त प्लेटफॉर्म के माध्यम से किस प्रकार का डेटा संग्रहित किया जा रहा है और डेटा सुरक्षा तथा गोपनीयता सुनिश्चित करने के लिए क्या सुरक्षा उपाय किए गए हैं?

उत्तर
संचार और पूर्वोत्तर क्षेत्र विकास मंत्री
(श्री ज्योतिरादित्य मा. सिंधिया)

(क) से (घ) विवरण सभा पटल पर रख दिया गया है।

"साइबर/दूरसंचार धोखाधड़ी में कमी" के संबंध में राज्य सभा के दिनांक 12.02.2026 के तारांकित प्रश्न सं. 141 के उत्तर के भाग (क) से (घ) के बारे में विवरण ।

(क) से (ग) दूरसंचार विभाग (डीओटी) ने साइबर अपराध और वित्तीय धोखाधड़ी में दूरसंचार संसाधनों के दुरूपयोग को रोकने के लिए हितधारकों के साथ द्विपक्षीय जानकारी साझा करने के लिए एक सुरक्षित ऑनलाइन डिजिटल इंटेलिजेंस प्लेटफॉर्म (डीआईपी) विकसित किया है। डीआईपी पर 1,200 से ज़्यादा संगठन जुड़े हैं, जिनमें केंद्रीय सुरक्षा एजेंसियां, 36 राज्य/संघ राज्य क्षेत्रों के पुलिस विभाग, भारतीय साइबर अपराध समन्वय केंद्र (आई4सी), बैंक, यूनिफाइड पेमेंट्स इंटरफेस (यूपीआई) सर्विस प्रोवाइडर, पेमेंट सिस्टम ऑपरेटर और दूरसंचार सेवा प्रदाता (टीएसपी) शामिल हैं।

डीआईपी जुड़े हुए हितधारकों को साइबर अपराध और वित्तीय धोखाधड़ी में दुरूपयोग होने की संभावना वाले मोबाइल नंबरों को डीओटी के साथ साझा करने में सक्षम बनाता है। हितधारकों द्वारा साझा किए गए डेटा का डीओटी द्वारा विश्लेषण किया जाता है। इसके मुख्य नतीजे इस तरह हैं -

(i) *अस्त्र* - यह एक आर्टिफिशियल इंटेलिजेंस और बिग डेटा एनालिटिक्स टूल है जो संदिग्ध मोबाइल कनेक्शन की पहचान करता है। ऐसे नंबर डीआईपी के ज़रिए टीएसपी के साथ साझा किए जाते हैं। ऐसे 88 लाख से ज़्यादा मोबाइल कनेक्शन पुन: सत्यापन में फेल होने के बाद काट दिए गए हैं।

(ii) *इंटरनेशनल इनकमिंग स्पूफ्ड कॉल्स प्रिवेंशन सिस्टम (सीआईओआर)* - यह एक ऐसा सिस्टम है जो उन इंटरनेशनल स्पूफ्ड कॉल्स की पहचान और ब्लॉक करता है जिनमें भारतीय मोबाइल नंबर दिखते हैं और जो भारत से ही आरंभ हुई लगती हैं। 17.10.2024 को शुरू हुए सीआईओआर ने 24 घंटों में 1.35 करोड़ कॉल ब्लॉक करके अच्छे नतीजे दिखाए हैं और इससे भारतीय कॉलिंग लाइन आईडेंटिफीकेशन वाली स्पूफ्ड कॉल्स में लगभग 99% की कमी आई है। जो कॉल्स अभी भी इंटरनेशनल गेटवे पर आती हैं, उन्हें वहीं ब्लॉक कर दिया जाता है।

(iii) *फाइनेंशियल फ्रॉड रिस्क इंडिकेटर (एफआरआई)* - यह एक ऐसा जोखिम-आधारित मिट्रिक है जो संदिग्ध मोबाइल नंबर को इसके वित्तीय धोखाधड़ी से जुड़े होने की संभावना के आधार पर मध्यम, उच्च अथवा अत्यधिक उच्च जोखिम श्रेणी में वर्गीकृत करता है। एफआरआई हितधारकों-विशेष रूप से बैंकों, गैर-बैंकिंग वित्तीय कंपनियों (एनबीएफसी) तथा यूपीआई सेवा

प्रदाताओं को प्राथमिकता देने तथा अतिरिक्त ग्राहक सुरक्षा उपाय अपनाने का अधिकार देता है, जैसे– अधिक सावधानी बरतना और निर्दिष्ट मोबाइल नंबरों के लिए आवश्यक रियल-टाइम प्रतिक्रिया प्रोटोकॉल (अलर्ट, लेन-देन में विलंब, चेतावनी, लेन-देन अस्वीकृति आदि) अपनाना। मई, 2025 में इसके आरंभ होने के बाद से, वित्तीय संस्थानों की रिपोर्ट के अनुसार एफआरआई के उपयोग से लेन-देन अस्वीकार करके तथा नागरिकों को जारी अलर्ट या सूचनाओं के आधार पर ₹1400 करोड़ से अधिक की संभावित धोखाधड़ी रोकी गई है।

(iv) संचार साथी पर नागरिकों द्वारा साझा किए गए संदिग्ध धोखाधड़ी संचार की 7.93 लाख रिपोर्ट के आधार पर, 39.53 लाख मोबाइल कनेक्शन काट दिए गए हैं।

(घ) डेटा पर आधारित विश्लेषण को डीओटी, डीआईपी पर हितधारकों के साथ काटे गए मोबाइल नंबरों को काटने के कारण तथा काटने की तारीख सहित मोबाइल नंबर रिवोकेशन सूची और एफआरआई के रूप में साझा करता है। बदले में, हितधारक की गई कार्रवाई संबंधी रिपोर्ट और साइबर अपराध और वित्तीय धोखाधड़ी में दुरूपयोग होने की संभावना वाले मोबाइल नंबरों को भी साझा करते हैं। डीआईपी एक ऑनलाइन सुरक्षित प्लेटफॉर्म है जो डेटा सुरक्षा और प्राइवेसी को सुनिश्चित करता है, जिस पर सख्त, रियल-टाइम ऑथेंटिकेशन और ऑथराइजेशन के आधार पर एक्सेस दिया जाता है। इसके अलावा, इंडस्ट्री की बेस्ट प्रैक्टिस के आधार पर ज़रूरी सुरक्षा उपाय - फायरवॉल, मल्टी-फैक्टर ऑथेंटिकेशन (एमएफए), पहचान एवं एक्सेस मैनेजमेंट और नियमित सुरक्षा आकलन और ऑडिट के ज़रिए लागू किए गए हैं।

*****