भारत सरकार

संचार मंत्रालय

दूरसंचार विभाग

लोक सभा

अतारांकित प्रश्न सं. 5405

उत्तर देने की तारीख 25 मार्च, 2026

संचार साथी 2.0 पोर्टल/प्लेटफार्म

5405. श्रीमती अनिता नागरसिंह चौहानः

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

(क) क्या सरकार ने साइबर धोखाधड़ी, मोबाइल चोरी और नकली सिम कार्ड जैसी समस्याओं से नागरिकों को सुरक्षा प्रदान करने के उद्देश्य से 'संचार साथी 2.0' पोर्टल/प्लेटफार्म आरंभ किया है और यदि हां, तो इसके प्रमुख उद्देश्य और विशेषताएं क्या हैं;

(ख) क्या इस प्लेटफार्म के माध्यम से मोबाइल फोनों को ब्लॉक करने/ट्रेस करने, संदिग्ध सिम कार्डों की पहचान करने और उपभोक्ताओं द्वारा शिकायत दर्ज कराने की सुविधाएं प्रदान की जा रही हैं;

(ग) क्या सरकार ने उक्त पोर्टल के प्रभावी उपयोग के लिए दूरसंचार सेवा प्रदाताओं (टीएसपी), राज्य सरकारों और कानून प्रवर्तन एजेंसियों (एलईए) के साथ समन्वय स्थापित किया है; और

(घ) यदि हां, तो नागरिकों की सुरक्षा को और अधिक सुदृढ़ करने और डिजिटल धोखाधड़ी पर प्रभावी नियंत्रण सुनिश्चित करने के लिए उठाए गए प्रमुख कदमों और सरकार की भावी कार्य योजना का ब्यौरा क्या है?

उत्तर

संचार एवं ग्रामीण विकास राज्य मंत्री

(डॉ. पेम्मासानी चंद्र शेखर)

(क) और (ख) दूरसंचार विभाग (डीओटी) ने डिजिटल धोखाधड़ी में दूरसंचार संसाधनों के दुरुपयोग को रोकने के उद्देश्य से एक नागरिक केंद्रित पहल, संचार साथी विकसित की है। यह वेब पोर्टल (www.sancharsaathi.gov.in) और मोबाइल ऐप के रूप में उपलब्ध है। संचार साथी की प्रमुख विशेषताओं में नागरिकों को संदिग्ध धोखाधड़ी संचार की रिपोर्ट करने, उनके नाम पर मोबाइल कनेक्शन जानने और उन कनेक्शनों की रिपोर्ट करने जो आवश्यक नहीं हैं या

उनके द्वारा नहीं लिए गए हैं, खोए हुए / चोरी हुए मोबाइल हैंडसेट की रिपोर्ट करने, मोबाइल हैंडसेट की प्रामाणिकता की जांच करने की सुविधा शामिल है।

(ग) दूरसंचार विभाग ने डिजिटल इंटेलिजेंस प्लेटफॉर्म (डीआईपी) विकसित किया है, जो साइबर अपराधों और वित्तीय धोखाधड़ी में दूरसंचार संसाधनों के दुरुपयोग की रोकथाम के लिए हितधारकों के साथ दो-तरफा सूचना साझा करने के लिए एक सुरक्षित ऑनलाइन प्लेटफॉर्म है। डीआईपी पर 1,400 से अधिक संगठन शामिल हैं, जिनमें केंद्रीय सुरक्षा एजेंसियां, 36 राज्यों और संघ राज्य क्षेत्र के पुलिस विभाग, भारतीय साइबर अपराध समन्वय केंद्र (आई4सी), बैंक, एकीकृत भुगतान इंटरफेस (यूपीआई) सेवा प्रदाता, भुगतान प्रणाली ऑपरेटर और दूरसंचार सेवा प्रदाता (टीएसपी) शामिल हैं।

(घ) संचार साथी और डीआईपी के साथ-साथ नागरिक सुरक्षा को मजबूत करने और डिजिटल धोखाधड़ी पर प्रभावी नियंत्रण सुनिश्चित करने के लिए कुछ अन्य प्रमुख उपाय निम्नलिखित हैं:

i. *अंतर्राष्ट्रीय इनकमिंग स्पूफ कॉल प्रिवेंशन सिस्टम (सीआईओआर):* यह भारतीय मोबाइल नंबर प्रदर्शित करने वाली आने वाली अंतर्राष्ट्रीय स्पूफ कॉल, जो भारत के भीतर से उत्पन्न होती प्रतीत होती है, की पहचान करने और उन्हें ब्लॉक करने के लिए एक प्रणाली है। अन्य बातों के साथ साथ इस तरह के कॉल्स का दुरुपयोग डिजिटल-गिरफ्तारी जैसे साइबर-धोखाधड़ी में सरकारी अधिकारियों के रूप में प्रतिरूपण करने के लिए किया जा रहा है।

ii. *अस्त्र (एएसटीआर):* यह एक कृत्रिम बुद्धिमत्ता और बिग डेटा एनालिटिक्स टूल है जो संदिग्ध मोबाइल कनेक्शनों की पहचान करता है। ऐसे नंबर डीआईपी के माध्यम से टीएसपी के साथ साझा किए जाते है।

iii. *वित्तीय धोखाधड़ी जोखिम संकेतक (एफआरआई):* यह एक जोखिम-आधारित मीट्रिक है जो वित्तीय धोखाधड़ी के मध्यम, उच्च या बहुत उच्च जोखिम से जुड़े होने की संभावना के अनुसार एक संदिग्ध मोबाइल नंबर को वर्गीकृत करता है। एफआरआई, हितधारकों - विशेष रूप से बैंकों, गैर-बैंकिंग वित्तीय कंपनियों (एनबीएफसी) और यूपीआई सेवा प्रदाताओं को चिह्नित मोबाइल नंबरों के लिए प्रवर्तन को प्राथमिकता देने और अतिरिक्त ग्राहक सुरक्षा उपायों जैसे उन्नत उचित डिलिजेंस और आवश्यक रीयल टाइम रिसपॉन्स प्रोटोकॉल (अलर्ट, लेनदेन में देरी, चेतावनी, लेनदेन में गिरावट आदि) को अपनाने के लिए सशक्त बनाता है।

*****