भारत सरकार
संचार मंत्रालय
दूरसंचार विभाग

लोक सभा
अतारांकित प्रश्न सं. 780
उत्तर देने की तारीख दिनांक 04 फरवरी, 2026

साइबर हमलों को रोकने के लिए दूरसंचार नेटवर्क की सुरक्षा

780. श्रीमती अनिता नागरसिंह चौहानः

क्या संचार मंत्री यह बताने की कृपा करेंगे किः

(क) सरकार द्वारा देश में दूरसंचार नेटवर्क की सुरक्षा को मजबूत करने और साइबर हमलों और दूरसंचार अवसंरचना के दुरूपयोग को रोकने के लिए क्या नीतिगत और तकनीकी उपाय किए गए हैं;
(ख) साइबर धोखाधड़ी, फर्जी कॉल/संदेश, सिम-स्वैप धोखाधड़ी और डिजिटल वित्तीय अपराधों को रोकने में अब तक क्या प्रगति हुई है और इसके क्या परिणाम रहे;

(ग) क्या सार्वजनिक सुरक्षा, डेटा गोपनीयता और सेवा की उपलब्धता सुनिश्चित करने के लिए कोई नागरिक-केंद्रित डिजिटल पहल की गई है; और

(घ) यदि हां, तो इन पहलों के तहत जन जागरूकता कार्यक्रम, शिकायत निवारण तंत्र और विभिन्न विभागों के बीच समन्वय का ब्यौरा क्या है?

उत्तर
संचार एवं ग्रामीण विकास राज्य मंत्री
(डॉ. पेम्मासानी चंद्र शेखर)

क) दूरसंचार विभाग ने देश में दूरसंचार नेटवर्क की सुरक्षा को सुदृढ़ करने और साइबर–अटैक को रोकने और दूरसंचार अवसंरचना के दुरुपयोग को रोकने के लिए विभिन्न नीतिगत और तकनीकी उपाय किए हैं। इनमें उल्लेखनीय उपाय निम्नलिखित हैं:

1) डीओटी और दूरसंचार सेवा प्रदाताओं (टीएसपी) ने भारतीय मोबाइल नंबर प्रदर्शित करने वाली इनकंमिंग अंतर्राष्ट्रीय स्पूफ कॉल की पहचान करने और ब्लॉक करने के लिए एक प्रणाली तैयार की है। इस प्रणाली के परिणामस्वरूप ऐसी कॉलों में लगभग 99% की कमी आई है।

2) डीओटी ने विभिन्न हितधारकों की केंद्रीय सुरक्षा एजेंसियों, राज्य/संघ राज्य क्षेत्रों की पुलिस, बैंकों, यूपीआई सेवा प्रदाताओं, दूरसंचार सेवा प्रदाताओं (टीएसपी) आदि के साथ दूरसंचार संसाधनों के दुरुपयोग से संबंधित जानकारी साझा करने के लिए एक ऑनलाइन सुरक्षित डिजिटल इंटेलिजेंस प्लेटफॉर्म (डीआईपी) विकसित किया है।

3) डीओटी के निर्देश के अनुसार, दूरसंचार सेवा प्रदाताओं को सुरक्षा के दृष्टिकोण से वर्ष में एक बार या जब भी नेटवर्क के कॉन्फ़िगरेशन में बड़ा बदलाव हो, तो अपने नेटवर्क का ऑडिट करवाना होगा या नेटवर्क प्रमाणन एजेंसी से ऑडिट करवाना होगा, जो ISO/IEC 27001 जैसे इंटरनेशनल स्टैंडर्ड के तहत नेटवर्क ऑडिट करने के लिए प्रत्यायित हो, जिसमें वल्नरेबिलिटी असेसमेंट और पेनिट्रेशन टेस्टिंग (वीएपीटी) भी शामिल है। टीएसपी के नेटवर्क का बाह्य ऑडिट तीन वर्षों की अवधि में एक बार अनिवार्य है।

4) डीओटी ने दूरसंचार सेवा प्रदाताओं को डेटा ऐट रेस्ट और ट्रांजिट में डेटा की सुरक्षा के लिए सब्सक्राइबर डिटेल रिकॉर्ड (एसडीआर), कॉल डिटेल रिकॉर्ड (सीडीआर) और आईपी डिटेल रिकॉर्ड (आईपीडीआर) जैसे संवेदनशील दूरसंचार डेटासेट की सुरक्षा को सुदृढ़ करने के लिए परामर्शिका जारी की है।

5) डीओटी ने सभी लाइसेंसधारियों द्वारा अनुपालन के लिए "डीओटी लाइसेंसधारियों की सुरक्षा नीति के लिए न्यूनतम अपेक्षिता" पर निर्देश जारी किए हैं। सुरक्षा नीति सुरक्षा और सुरक्षा प्रबंधन की स्थापना, कार्यान्वयन, रखरखाव और निरंतर सुधार के लिए दिशा प्रदान करेगी।

6) राष्ट्रीय सुरक्षा के दृष्टिकोण से नेटवर्क उपकरण, सॉफ्टवेयर, आपूर्ति श्रृंखला और डेटा प्रबंधन की सुरक्षा सुनिश्चित करने के लिए टीएसपीएस/आईएसपी का क्रॉस चेक नेटवर्क सिक्योरिटी ऑडिट वार्षिक रूप से किया जा रहा है।

7) विभाग ने दूरसंचार साइबर सुरक्षा मामलों पर स्थितिजन्य जागरूकता, निगरानी और समन्वय बढ़ाने के लिए दूरसंचार सुरक्षा संचालन केंद्र (टीएसओसी) की स्थापना की है।

ख) डीओटी ने वित्तीय धोखाधड़ी जोखिम संकेतक (एफआरआई) विकसित किया है, जो जोखिम-आधारित मीट्रिक है जो वित्तीय धोखाधड़ी के मध्यम, उच्च या बहुत उच्च जोखिम से जुड़े मोबाइल नंबर को वर्गीकृत करता है। एफआरआई हितधारकों-विशेष रूप से बैंकों, गैर-बैंकिंग वित्तीय कंपनियों

(एनबीएफसी) और यूनिफाइड पेमेंट्स इंटरफेस (यूपीआई) सेवा प्रदाताओं को प्रवर्तन को प्राथमिकता देने और यदि मोबाइल नंबर उच्च जोखिम वाला है तो अतिरिक्त ग्राहक सुरक्षा उपाय करने के लिए सशक्त बनाता है। हितधारकों द्वारा की गई रिपोर्ट के अनुसार, ट्रांजेक्शन डिक्लाइन और नागरिकों को दी गई चेतावनी / सूचना के आधार पर रोकी गई कुल धोखाधड़ी की राशि 1,000 करोड़ रुपये से अधिक है।

ग) डीओटी ने संचार साथी, नागरिक केंद्रित पहल विकसित की है, जो नागरिकों को संदिग्ध धोखाधड़ी संचार की रिपोर्ट करने, उनके नाम पर के मोबाइल कनेक्शन जानने, खोए हुए/ चोरी हुए मोबाइल हैंडसेट की रिपोर्ट करने, मोबाइल हैंडसेट की प्रामाणिकता की जांच करने आदि की सुविधा प्रदान करती है। संचार साथी के परिणाम निम्नानुसार हैं:

क. 27.96 लाख खोए/चोरी हुए मोबाइल हैंडसेट का पता लगाया गया है और 8.22 लाख खोए/चोरी हुए मोबाइल हैंडसेट बरामद किए गए हैं और राज्य/संघ राज्य क्षेत्र पुलिस द्वारा वास्तविक मालिकों को लौटा दिए गए हैं।

ख. नागरिकों द्वारा 'नॉट माई नंबर' या 'नॉट रिक्वायर्ड' के रूप में रिपोर्टिंग के आधार पर 2.22 करोड़ मोबाइल कनेक्शन काटे गए हैं।

ग. सतर्क नागरिकों द्वारा संदिग्ध धोखाधड़ी कम्युनिकेशन से संबंधित प्रदान किए गए 7.72 लाख इनपुट के आधार पर 39.42 लाख मोबाइल कनेक्शन काटे गए हैं।

घ) डीओटी संचार साथी और एफआरआई पहलों के तहत व्यापक जागरूकता अभियानों के माध्यम से डिजिटल सुरक्षा को सक्रिय रूप से बढ़ावा दे रहा है और दूरसंचार से संबंधित धोखाधड़ी को रोक रहा है। जागरूकता फैलाने के लिए इन पहलों के बारे में व्याख्यात्मक वीडियो और इन्फोग्राफिक्स नियमित रूप से तैयार किए जाते हैं और डीओटी के सोशल मीडिया प्लेटफॉर्म पर अपलोड किए जाते हैं। डीओटी ने संचार मित्र योजना भी शुरू की है, जिसके माध्यम से छात्र स्वयंसेवकों को डिजिटल सुरक्षा, धोखाधड़ी की रोकथाम और संचार साथी पोर्टल और ऐप के उपयोग के बारे में नागरिकों को शिक्षित करने के लिए लगाया गया है। उपर्युक्त के अलावा, नागरिक आउटरीच में बहुभाषी समाचार लेख और विज्ञापन, सार्वजनिक स्थानों पर डिजिटल स्क्रीन और होर्डिंग, टीवी और रेडियो संदेश, डीओटी फील्ड इकाइयों द्वारा स्थानीय स्तर की गतिविधियां, दूरसंचार सेवा प्रदाताओं के साथ एसएमएस अभियान और व्यापक सोशल मीडिया सामग्री शामिल हैं।

*****