**GOVERNMENT OF INDIA**
**MINISTRY OF COMMUNICATIONS**
**DEPARTMENT OF TELECOMMUNICATIONS**

**LOK SABHA**
**UNSTARRED QUESTION NO. 780**
**TO BE ANSWERED ON 4TH FEBRUARY, 2026**

## SECURITY OF TELECOM NETWORK TO PREVENT CYBER ATTACKS

**†780. SMT. ANITA NAGARSINGH CHOUHAN:**

Will the Minister of COMMUNICATIONS be pleased to state:

(a) the policy and technical measures taken by the Government to strengthen the security of the telecom network and to prevent cyber attacks and misuse of telecommunications infrastructure in the country;

(b) the progress made so far in preventing cyber fraud, fake calls/messages, SIM-swap fraud and digital financial crimes along with the outcomes thereof;

(c) whether any citizen-centric digital initiatives have been taken to ensure public safety, data privacy and availability of service; and

(d) if so, the details of the public awareness programme, grievance redressal mechanisms and coordination among various departments under these initiatives?

## ANSWER

**MINISTER OF STATE FOR COMMUNICATIONS AND RURAL DEVELOPMENT**
**(DR. PEMMASANI CHANDRA SEKHAR)**

(a) Department of Telecommunications have taken various policy and technical measures to strengthen the security of the telecom network and to prevent cyber-attacks and misuse of telecommunications infrastructure in the country. The notable ones are as under:

1) DoT and Telecom Service Providers (TSPs) have devised a system to identify and block incoming international spoofed calls displaying Indian mobile numbers. The system has resulted in almost 99% reduction in such calls.
2) DoT has developed an online secure Digital Intelligence Platform (DIP) for sharing of information related to misuse of telecom resources with different stakeholders’ central security agencies, State/UT Police, Banks, UPI service providers, Telecom Service Providers (TSPs) etc.
3) DoT directive requires Telecom Service Providers to audit their network or get the network audited from security point of view once a year or as and when configuration of network is changed significantly, from a network certification agency which is accredited to carry out the network audit under international standards such as ISO/IEC 270011 including Vulnerability Assessment and Penetration Testing (VAPT). An external audit of the TSPs network is mandatory once in a period of three years.

4) DoT has issued advisory to telecom service providers to strengthen protection of sensitive telecom datasets such as Subscriber Detail Record (SDR), Call Detail Record (CDR) and IP Detail Record (IPDR) for the security of data at rest and transit.

5) DoT has issued instructions on “Minimum Requirement for Security Policy of DoT Licensees” to be complied with by all licensees. Security Policy will provide direction for establishment, implementation, maintenance and continual improvement in Security and Security Management.

6) Cross Check Network Security Audit of TSPs/ISPs is being done annually to ensure security of network equipment, software, supply chains and data management from perspective of national security.

7) The Department has established a Telecom Security Operations Centre (TSOC) to enhance situational awareness, monitoring, and coordination on telecom cyber security matters.

(b) DoT has developed Financial Fraud Risk Indicator (FRI), which is a risk-based metric that classifies a mobile number to have been associated with Medium, High, or Very High risk of financial fraud. FRI empowers stakeholders-especially banks, Non-Banking Financial Companies ( NBFCs), and Unified Payments Interface (UPI) service providers to prioritize enforcement and take additional customer protection measures in case a mobile number has high risk. As reported by stakeholders, total fraud amount prevented based on transaction decline and alert/notifications given to citizens is more than ₹1,000 crores.

(c) DoT has developed Sanchar Saathi, a citizen centric initiative, which facilitates citizens to report suspected fraud Communications, to know mobile connections in their name, to report lost/ stolen mobile handsets, to check genuineness of mobile handset etc. Outcomes of Sanchar Saathi are as under:

a. 27.96 lakh lost/ stolen mobile handsets have been traced and 8.22 lakh lost/ stolen mobile handsets have been recovered and returned to rightful owners by State/ UT Police.
b. 2.22 crore mobile connections have been disconnected based on reporting by citizens as ‘Not My Number’ or ‘Not Required’.
c. 39.42 lakh mobile connections have been disconnected based on 7.72 lakh inputs provided by vigilant citizens related to suspected fraud communications.

(d) DoT has been actively promoting digital safety and preventing telecom-related fraud through widespread awareness campaigns under Sanchar Saathi and FRI initiatives. Explainer videos and infographics about these initiatives are regularly prepared and uploaded on DoT's social media platforms for spreading awareness. DoT has also launched Sanchar Mitra scheme, through which student volunteers have been engaged to educate citizens about digital safety, fraud prevention, and the use of the Sanchar Saathi portal and app. Apart from above, citizen outreach includes multilingual news articles and ads, digital screens and hoardings in public spaces, TV and radio messages, local-level activities by DoT field units, SMS campaigns with Telecom Service Providers, and extensive social media content.

*****