DoT combats Cyber-frauds: Central system to stop spoofed calls to be commissioned shortly

Citizens are advised to use ‘Chakshu’ to report Spam Calls

45 lakh spoof international calls with Indian phone numbers being blocked by TSPs daily

Posted On: 04 OCT 2024 4:31PM by PIB Delhi

In recent times, citizens are receiving many fraudulent calls, often disguised as originating from Indian mobile numbers. These calls are in fact manipulated by cyber-criminals operating from abroad. These criminals exploit the Calling Line Identity (CLI) to mask the actual origin of the calls, which has led to a spate of incidents involving threats of mobile number disconnection, fake digital arrests, and even impersonation of government officials or law enforcement agencies. Recent cases have included false accusations involving drugs, narcotics, and sex rackets, further intensifying public concern.

In response to this growing threat, the Department of Telecommunications (DoT), in collaboration with Telecom Service Providers (TSPs), has introduced an advanced system designed to identify and block incoming international spoofed calls before they can reach Indian telecom subscribers. This system is being deployed in two phases: first, at the TSP level, to prevent calls spoofed with phone numbers of their own subscribers; and second, at a central level, to stop calls spoofed with the numbers of subscribers from other TSPs.

As of now, all four TSPs have successfully implemented the system. About one third of total spoofed calls at 4.5 million spoofed calls are being stopped from entering the Indian telecom network. The next phase, involving a centralized system that will eliminate the remaining spoofed calls across all TSPs, is expected to be commissioned shortly.

Fraudsters, however, continue to adapt and devise new methods to deceive the public. DoT is taking timely measures to protect telecom users as these new ways are reported. In the age of rapidly evolving technology, the DoT has taken multiple measures to make the telecom eco-systems safer and secure. However, even with these robust safeguards, there may still be instances where fraudsters succeed through other means.

In such cases, DoT encourages citizens to proactively report suspected fraud communications to help DoT in identification and prevention of misuse of telecom resources for cyber-crime, financial frauds. It will also help in safeguarding citizens from impersonation, exploitation, and enabling proactive action against potential threats.

Citizen can report such calls at *Chakshu* facility available on the *Sanchar Saathi* platform (https://sancharsaathi.gov.in/) by providing details about suspected fraud calls, SMS, and WhatsApp messages including screenshot, medium of receipt, category of intended fraud, date and time of receiving such communication. An OTP based verification will be carried out.

The Chakshu facility is a significant step towards safeguarding citizens from cyber fraud. By providing a streamlined process for reporting suspicious activities, it helps in the early detection and prevention of potential frauds, thereby protecting users from financial and personal losses

In addition, the Government has taken various measures for preventing misuse of telecom resources including:

i. Department of Telecommunications (DoT) has rolled out Digital Intelligence Unit (DIU) project with objective to devise systems to curb misuse of telecom resources for cybercrime and financial frauds.

ii. **Sanchar Saathi portal**: DoT has developed a citizen centric Sanchar Saathi portal (www.sancharsaathi.gov.in) providing various facilities for reporting of cases related to misuse of telecom resources which are as under:

a. to report suspected fraud communications and Unsolicited Commercial Communication (UCC);

b. to know the mobile connections issued in their name and report the mobile connections for disconnection which are either not required or not taken by them;

c. to report the stolen / lost mobile handset for blocking and tracing;

d. to check the genuineness of mobile handset while buying a new/old device;

e. to report the incoming international calls received with Indian telephone number as calling line identification.

iii. **Digital Intelligence Platform**: DoT has launched an online secure Digital Intelligence Platform (DIP) for sharing of information related to misuse of telecom resources among the stakeholders for prevention of cyber-crime and financial frauds. At present DoT field units, all Telecom Service Providers (TSPs), MHA, 460 banks and financial institutions, 33 States/UTs police, central agencies and other stakeholders have on-boarded this platform. This platform, inter-alia, hosts the list of disconnected mobile connections on near real time basis along with the reasons for disconnections enabling the stakeholders to take appropriate action including to disengage the associated services linked with these mobile numbers.

iv. **DoT using AI based tools** has identified the mobile connections taken on fake / forged documents or taken exceeding the prescribed limits for an individual. Such mobile connections along with telecom resources and mobile handsets used in fraudulent activities are being weeded out from the telecom ecosystem.

Following are the outcomes, as on date in brief, of the actions taken by DoT:

a. Disconnected 1.77 crore mobile connections taken on fake/forged documents.

b. Targeted action of disconnection of 33.48 lakh mobile connections and blocking of 49,930 mobile handsets used by cyber criminals in cyber-crime hotspots/districts of the country.

c. 77.61 lakh mobile connections exceeding the prescribed limits for an individual have been disconnected.

d. Pan India blocking of 2.29 lakh mobile phones involved in cyber-crime or fraudulent activities.

e. About 12.02 lakh out of 21.03 lakh reported stolen/lost mobile phones have been traced.

f. Disconnected about 20,000 entities, 32,000 SMS headers and 2 lakh SMS templates involved in sending malicious SMSs.

g. About 11 lakhs accounts have been frozen by the banks and payments wallets which were linked to disconnected mobile connections taken on fake / forged documents.

h. About 11 lakhs WhatsApp profiles/accounts have been disengaged by WhatsApp which were linked to disconnected mobile connections taken on fake / forged documents

i. 71,000 Point of Sale (SIM Agents) have been blacklisted. 365 FIRs have been registered in multiple States/UTs.

[Follow DoT Handles for more :-
X - https://x.com/DoT_India
Insta - https://www.instagram.com/department_of_telecom?igsh=MXUxbHFjd3llZTU0YQ==
Fb - https://www.facebook.com/DoTIndia
YT- https://www.youtube.com/@departmentoftelecom]

****

SB/DP

(Release ID: 2062022)