Ministry of Communications

DOT's directions for SIM binding for prevention of misuse of telecommunication identifiers for ensuring telecom cyber security

App Based Communication Services that are utilizing Indian Mobile Number for identification of its customers/users or for provisioning or delivery of services to comply within 90 days

Apps offering web access must enforce periodic logout and re-linking, preventing remote misuse of accounts authenticated once and operated from abroad

Mandatory SIM binding, already standard in banking/UPI systems, now extended to communication apps to counter phishing, digital arrest, impersonation and investment scams

प्रविष्टि तिथि: 01 DEC 2025 6:48PM by PIB Delhi

The Department of Telecommunications (DoT) has observed that some of the App Based Communication Services that are utilizing Indian Mobile Number for identification of its customers/users or for provisioning or delivery of services, allows users to consume their services without availability of the underlying Subscriber Identity Module (SIM) within the device in which App Based Communication Services is running. This feature is being misused to commit cyber-frauds especially from operating outside the country.

The issue of SIM binding in messaging apps and its misuse has been raised by multiple government bodies/agencies and an inter-ministerial group. On this issue, DOT had multiple discussions with major App Based Communication Services provider on the feasibility and importance. Thereafter, given the seriousness of the issue, DoT issued Directions to major App Based Communication Services on 28.11.2025 under the Telecom Cyber Security (TCS) Rules, 2024 (as amended) to prevent the misuse of telecommunication identifiers and to safeguard the integrity and security of the telecom ecosystem. These include WhatsApp, Telegram, Snapchat, Arattai, Sharechat, Josh, Jiochat and Signal.

Directions mandate such App Based Communication Services to –

i. Ensure that the App Based Communication Services is continuously linked to the SIM card (associated with Mobile Number used for identification of customers/users or for provisioning or delivery of services) installed in the device, making it impossible to use the app without that specific, active SIM.
ii. Ensure that the web service instance of the Mobile App, if provided, shall be logged out periodically (not later than 6 hours) and allowing the facility to the user to re-link the device using QR code.

Directions mandates to complete the implementation in 90 days and submit the report in 120 days.

DoT's SIM-binding directions are essential to plug a concrete security gap that cybercriminals are exploiting to run large-scale, often cross-border, digital frauds. Accounts on instant messaging and calling apps continue to work even after the associated SIM is removed, deactivated or moved abroad, enabling anonymous scams, remote "digital arrest" frauds and government-impersonation calls using Indian numbers.

Long-lived web/desktop sessions let fraudsters control victims' accounts from distant locations without needing the original device or SIM, which complicates tracing and takedown. A session can currently be authenticated once on a device in India and then continue to operate from abroad, letting criminals run scams using Indian numbers without any fresh verification. Auto-logout every 6 hours (its only for web version and not for App version) shuts down such long web-sessions and forces periodic re-authentication with control of the device/SIM, sharply reducing scope for account takeover, remote-access misuse and mule-account operations. Frequent re-authentication forces criminals to repeatedly prove control of the device/SIM, raising friction and detectability.

Mandatory continuous SIM–device binding and periodic logout ensure that every active account and web session is anchored to a live, KYC-verified SIM, restoring traceability of numbers used in phishing, investment, digital arrest and loan scams. The direction does not affect the cases where the SIM is present in the handset and the user is on roaming. With cyber-fraud losses exceeding ₹22,800 crore in 2024 alone, these uniform, enforceable directions under the Telecom Cyber Security Rules are a proportionate measure to prevent misuse of telecom identifiers, ensure traceability, and protect citizens' trust in India's digital ecosystem.

Device binding and automatic session logout are widely used in banking and payment apps to prevent account takeover, session hijacking and misuse from untrusted devices and accordingly extended to app-based communication platforms that are now central to cyber frauds.

DoT is committed to make India a cyber secure nation.

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

Youtube: https://www.youtube.com/@departmentoftelecom

***

MI/ARJ

(रिलीज़ आईडी: 2197146) आगंतुक पटल : 1110
इस विज्ञप्ति को इन भाषाओं में पढ़ें: Urdu , हिन्दी