GOVERNMENT OF INDIA
MINISTRY OF RAILWAYS

LOK SABHA
STARRED QUESTION NO. 43
TO BE ANSWERED ON 22.07.2026

UNAUTHORISED BOOKING OF TATKAL TICKETS

***43. SHRI SHYAMKUMAR DAULAT BARVE:**

Will the Minister of RAILWAYS be pleased to state:

(a) whether the Government is aware that the Tatkal ticket booking system remains highly ineffective for ordinary passengers as tickets get exhausted within minutes due to the use of software and nexus of brokers;

(b) if so, the number of unauthorized agents apprehended across railway zones during the last five years and current year along with the details of punitive actions taken against them; and

(c) the details of the concrete and detailed structural, technical and cybersecurity measures being implemented by the Government to permanently block automated booking bots and ensure a fair, transparent ticketing process for common citizens?

ANSWER

MINISTER OF RAILWAYS, INFORMATION & BROADCASTING AND ELECTRONICS & INFORMATION TECHNOLOGY

(SHRI ASHWINI VAISHNAW)

(a) to (c): A Statement is laid on the Table of the House.

*****

§

STATEMENT REFERRED TO IN REPLY TO PARTS (a) TO (c) OF STARRED QUESTION NO.43 TO BE ANSWERED ON 22.07.2026 IN LOK SABHA

(a) to (c): The reservation ticket booking system of Indian Railways is a robust and highly secure system equipped with industry-standard, state-of-the-art cyber security controls. Indian Railways has taken the following measures to safeguard the system from cyber attacks and to prevent auto filling of forms by hacking tools for curbing frauds in tatkal ticketing booking through internet:

1. Aadhaar authentication to book tatkal tickets – A provision has been made to allow only Aadhaar authenticated passengers to book Tatkal tickets online. It helps in preventing the creation and operation of fake or unauthorized agent-controlled multiple user account by imposing a uniqueness constraint. This measure acts as an effective safeguard against account multiplication and automated misuse, thereby ensuring fair allocation of tatkal tickets. It has enhanced transparency in the online tatkal booking system. To curb misuse and improve fairness in tatkal bookings, Aadhaar based One-Time Password (OTP) verification for online tatkal ticket booking has also been introduced on selected trains.

2. Application layer Security Control -- Several application level security controls have been implemented at multiple levels to avoid scripting, Brute-Force Attack and DDoS (Distributed Denial of Service) attacks. A number of security measures have also been applied for handling the OWASP (Open Web Application Security Project) for application security vulnerability.

To optimize system performance, Indian Railways has implemented a Content Delivery Network (CDN) to offload static content and reduce direct traffic on internet ticket booking website system. Further, Anti-bot solutions have been deployed to filter non-genuine users which help in

mitigating suspicious attempts on the internet ticket booking website system to ensure smooth booking for genuine passengers.

In addition, multiple protective layers such as network firewalls, intrusion prevention systems, application delivery controllers and web application firewalls have been deployed to safeguard the system against cyber threats.

3. Network and Infrastructure Layer Security Controls – The entire ICT (Information and Communication Technology) infrastructure has been deployed on high availability mode to minimize failures.

The system is protected by industry-standard state-of-the-art and data centre grade network along with security equipment consisting of network firewalls, network intrusion prevention system, application delivery controllers and web application firewalls.

The system is also protected from volume-based DDoS (Distributed Denial of Service) attacks with ISP (Internet Service Provider) layer, DDoS Detection and Mitigation Services through multiple ISPs with aggregated DDoS mitigation capacity of nearly 30 Gbps.

The enterprise level Content Delivery Network (CDN), anti-bot, secure DNS and Web Application Firewall (WAF) services for enhanced security, better customer experience, regulating web traffic load, resource optimisation and threat mitigation have been deployed.

For comprehensive cyber threat intelligence services, specialized agencies have been engaged to undertake Deep-Dark Web Monitoring, Digital Risk Protection and improve incident response.

4. Physical Security Controls – The system is hosted in a captive data centre facility Chanakyapuri, New Delhi secured with CCTV footage and

restricted physical access. The facility is ISO 27001 (Information Security Management System) certified.

5. Security Audit and Monitoring -- The system is integrated with CERT-In TSAP (Threat & Situational Awareness Projects) for round the clock monitoring of security incidents and events.

Security log monitoring of the system is being done by on-premises security team for detection and mitigation of security incidents.

6. Administrative measures – Several anti-fraud measures have been adopted to prevent unauthorized access and to ensure seamless booking for genuine users.

- **Rigorous revalidation and verification of user accounts have been done. About 3.04 crore suspicious user IDs have been deactivated and 6.22 crore have been placed under revalidation in the year 2025-26 & 2026-27 (till 30.06.2026).**
- **Regular security audits of the reservation system are carried out by CERT-In empanelled information Security Audit Agencies. Moreover, internet traffic related to the ticketing system is continuously monitored by CERT-In and the National Critical Information Infrastructure Protection Centre (NCIIPC) to detect and prevent cyber attacks.**
- **530 complaints have been lodged on the National Cyber Crime Portal pertaining to suspicious bookings in the year 2025-26 & 2026-27 (till 30.06.2026).**
- **13,343 suspicious email domains have been blocked in the year 2025-26 & 2026-27 (till 30.06.2026).**

During the last five years i.e. 2021 to 2025 and 2026 up to June, 22,676 touts have been arrested by RPF (Railway Protection Force) and legal action has been taken under the relevant provisions of the Railways Act, 1989.

The details of spurious attempts denied to access the e-ticketing system during the last six months is as under:

June 2026	**Out of 19.12 billion requests, 12.61 billion were bots. (65.95%)**
May 2026	**Out of 20.07 billion requests, 12.08 billion were bots. (60.18%)**
April 2026	**Out of 17.33 billion requests, 10.64 billion were bots. (61.39%)**
March 2026	**Out of 12.44 billion requests, 05.71 billion were bots. (45.90%)**
February 2026	**Out of 11.01 billion requests, 05.01 billion were bots. (45.50%)**
January 2026	**Out of 12.35 billion requests, 07.26 billion were bots. (58.78%)**

Average for last six months: Out of 15.38 billion requests, 8.88 billion were bots(57.74%).

*****