GOVERNMENT OF INDIA
MINISTRY OF COMMUNICATIONS
DEPARTMENT OF TELECOMMUNICATIONS

LOK SABHA
UNSTARRED QUESTION NO. 4187
TO BE ANSWERED ON 18TH MARCH, 2026

HACKING ATTEMPTS OF ANDROID PHONES

4187. SHRI NAVEEN JINDAL:

Will the Minister of COMMUNICATIONS be pleased to state:

(a) the details of the number of reported hacking attempts on Android phones in the country during the last five years, State and year-wise;

(b) the details of the initiatives undertaken by the Government to educate citizens about mobile security best practices and prevent hacking of Android devices;

(c) the details of the measures taken by the Government to prevent hacking of Android phones and protect users from cyber threats;

(d) the steps taken/being taken by the Government to ensure that mobile manufacturers and software developers comply with security standards to prevent Android phone hacking; and

(e) whether the Government is regulating app stores and mobile service providers effectively to ensure that malicious applications are not distributed and if so, the details thereof?

ANSWER

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

(a) There is no specific category for 'hacking of mobile phones' on the National Cybercrime Reporting Portal (NCRP), which was launched in 2019 by Indian Cyber Crime Coordination Centre (I4C), MHA to enable citizens to register complaints regarding cybercrimes from across India.

However, complaints related to such incidents may be reported under the following categories available on portal:

i. **"Hacking / Damage to Computer, Computer System etc."**, which covers incidents involving unauthorized access or damage to computer systems; and
ii. **Sub-category for reporting of "Profile Hacking / Identity Theft"** under the category **"Online and Social Media Related Crime."**

(b) & (c) The Government has undertaken several initiatives to enhance awareness among citizens regarding mobile security best practices and to protect users from cyber threats, including those targeting Android devices. Under the **Information Security Education and Awareness (ISEA)** programme of the Ministry of Electronics and Information Technology (MeitY), nationwide

awareness campaigns, training programmes, workshops, and dissemination of educational materials are conducted to promote cyber hygiene and safe usage of digital devices and applications. Further, the Government has established the **Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre),** which provides tools and resources for detection and removal of malware, including those affecting mobile devices, and disseminates advisories and alerts on emerging cyber threats. CERT-In is regularly carrying out various activities for awareness and citizen sensitization with respect to cyber-attacks and cyber frauds. CERT-In is observing the Cyber Security Awareness Month (NCSAM) during October of every year, Safer Internet Day on 2nd Tuesday of February, Swachhta Pakhwada from 1 to 15 February and Cyber Jagrookta Diwas (CJD) on 1st Wednesday of every month by organizing various events and activities for citizens as well as the technical cyber community in India. CERT-In is regularly sharing safety and security tips, awareness posters, info-graphics, booklets and videos through its official websites and social media handles such as Facebook, X(Twitter), Instagram, YouTube and LinkedIn for sensitizing internet users on cyber security attacks and frauds and prevention measures.

(d) The Government promotes secure software development and adoption of security best practices through **cyber security guidelines, vulnerability reporting mechanisms, certification frameworks, and regular advisories issued to stakeholders.** Mobile manufacturers and software developers **track these advisories and release security patches or updates** to address the vulnerabilities. Further, MeitY has been designated as the Appropriate Authority by Rule 4(2) of Telecommunications (Framework to notify Standards, Conformity Assessment and Certification) Rules, 2025 under Telecommunication Act 2023 for notifying standards and conformity assessment measures for certain ICT products including Mobile phones.

(e) The Information Technology Act, 2000 ("IT Act") and the rules made thereunder provide for penal action against a wide range of cyber offences, including impersonation, identity theft, violation of privacy, circulation of obscene or sexually explicit content, and child sexual abuse material. These statutory provisions are further reinforced through intermediary due diligence obligations under the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021 ("IT Rules, 2021"), which mandate proactive prevention of unlawful content, time-bound grievance redressal, and cooperation with law enforcement agencies to prevent misuse of digital platforms and to safeguard the dignity, safety, and rights of users in cyberspace.

*****