No. 22012/07/2025-CC(Pt.1)
Government of India
Ministry of Home Affairs
Cyber and Information Security Division
(Cyber Crime Section)

*****

35022, Kartavya Bhavan-3, New Delhi
Dated the 25th September, 2026

OFFICE MEMORANDUM

Sub: Advisory regarding Undertaking and Promotion of Sustained Awareness Programmes relating to Cybercrimes, Grievance Redressal, Money Restoration Mechanisms, Safe Digital Practices and Allied Concerns.

The Hon'ble Supreme Court in *Suo Motu Writ Petition (Criminal) No. 03/2025 – In Re: Victims of Digital Arrest Related to Forged Documents* has taken cognizance of the increasing threat posed by cyber-enabled crimes, including digital arrest scams and other forms of online financial fraud and vide order dated 04.08.2026 has directed the Inter-Departmental Committee to issue necessary directives, advisories and instructions to all States, UTs, Ministries and Government Departments to undertake and promote awareness program about cybercrimes, grievance redressal and money restoration modules and allied concerns.

2. In view of the above directions and the evolving nature of cyber enabled frauds, all Ministries and Departments are advised to conduct regular cybercrime awareness sessions, workshops, campaigns and outreach programmes for officials, employees, students and citizens. Awareness should cover major categories of cyber frauds, including Digital Arrest, Investment/Trading Scams, UPI/Banking Frauds, Phishing, OTP/KYC Frauds, Impersonation, Job/Loan Scams, Social Media Frauds, misuse of bank/mule accounts etc.

3. The message "STOP-THINK-TAKE ACTION" may be prominently promoted to encourage citizens to pause, verify suspicious communications and act promptly in case of fraud. Specialised campaigns may be undertaken for senior citizens, women, children and other vulnerable groups, leveraging existing outreach networks and public facing services of Ministries/Departments. Ministries such as Panchayati Raj, Consumer Affairs, Civil Aviation, Railways and Department of Posts, which already collaborate with I4C, may utilise their extensive institutional reach for wider dissemination. Educational institutions, including NSS and NCC networks, may also be engaged, and CBSE/UGC advisories may be used to facilitate dissemination of awareness material *(Annexure 1 & 2)*.

4. All Ministries and Departments shall widely disseminate information regarding the Cyber Crime Helpline 1930 and the National Cyber Crime Reporting Portal (NCRP) – *www.cybercrime.gov.in* and emphasise that prompt reporting of financial cyber frauds through these channels is critical for timely action and possible prevention of further movement of defrauded funds. Awareness may also be created regarding the recently launched Grievance Redressal Mechanism (GRM) and Money Restoration Mechanism (MRM) of MHA for complaints relating to blocking/freezing of defrauded money. The purpose, utility and appropriate use of GRM and MRM should be explained in simple, citizen friendly language. Relevant I4C videos and approved

awareness material may be utilised for dissemination. Citizens should be cautioned against mule accounts and advised not to share bank accounts, payment instruments or financial credentials to suspicious persons for receiving/transferring funds. Victims may be encouraged to preserve transaction IDs, bank/payment details, screenshots, messages, phone numbers, URLs and other evidence to facilitate investigation and grievance redressal.

5. It is advised to utilise official I4C/CyberDost creatives, infographics, videos and advisories for cybercrime awareness programmes which may be disseminated through official websites, social media handles, public places, offices, outreach networks and educational institutions. Ministries and Departments may periodically share cyber safety content through their digital communication channels. Multilingual awareness material is accessible at *https://i4c.mha.gov.in/awareness.aspx* and I4C may be contacted for any assistance.

6. All Ministries and Departments are further advised to designate nodal officers/points of contact for coordinating cybercrime awareness activities with I4C. Cyber safety awareness may be integrated into existing training, capacity building programmes, school/college/university activities, NSS/NCC engagements and public outreach initiatives. Ministries/Departments with existing collaborations with I4C may utilise these institutional arrangements for sustained and periodic awareness activities aligned with their mandates.

7. Basic details of awareness programmes undertaken such as number and type of programmes, target audience, geographical coverage, communication platforms and key initiatives may be maintained for monitoring and assessment. Significant initiatives may be documented and shared with I4C/MHA for identification and dissemination of best practices. Ministries and Departments may periodically review the effectiveness and reach of their awareness activities and take suitable measures to strengthen outreach, particularly among vulnerable and high-risk groups.

8. It is also apprised that **Sh. Nishant Kumar, Director, NCEMU, I4C, MHA (email: dir-i4c2@gov.in)**, has been designated as the nodal officer from I4C, MHA for coordination and facilitation of awareness initiatives undertaken pursuant to this advisory.

9. This issues with the approval of the Competent Authority.

Enclosed: Annexure 1 & 2

(Ashish Gaur)
Dy. Commandant (Cyber Crime)
Tele: No. 011-24010226
Email: dc-cybercrime@mha.gov.in

To,

Secretaries of all Ministries and Departments of Government of India (as per the standard list)