Ministry of Home Affairs
Government of India
सत्यमेव जयते

Indian Cyber Crime Coordination Centre

Intelligence Bureau
खुफिया विभाग
India भारत

Indian Cyber Crime Coordination Centre (I4C) and Ministry of Home Affairs, Government of India
Address: 5th Floor, NDCC-II Building, Jai Singh Road, New Delhi – 110001, India
Official Website: https://cybercrime.gov.in

TO WHOM IT MAY CONCERN

By the mandate of Mr.Shri Rajesh Kumar, Chief Executive Officer of the Indian Cybercrime Coordination Centre (I4C), in partnership with the Central Bureau of Investigation (CBI) the National Nodal Agency for INTERPOL in India I hereby notify you of a computerized seizure relating to cyber infiltration detected and captured on your Internet Protocol (IP) address, pursuant to the following analysis.

1. CHILD PORNOGRAPHY
2. PEDOPHILIA
3. TAX VIOLATION
4. UNAUTHORZED FOREIGN CURRENCY TRANSACTIONS TO INDIA

Your IP address has been detected by the Indian Cyber Crime Coordination Centre (I4C), in partnership with the Central Bureau of Investigation (CBI), the National Nodal Agency in India, and has been identified in connection with an illegal foreign currency transaction under Case Number (FMT-1571). Failure to respond within 24 hours from the time of this notice will compel the Prosecutor to issue an arrest warrant against you through the nearest police station.

The Criminal Code of India, under Section 14 of the Protection of Children from Sexual Offences (POCSO) Act, 2012, together with Sections 292, 67A, and 67B of the Information Technology Act, 2000, criminalizes the publication or transmission of sexually explicit acts or content involving juvenile pornography in electronic form, and such offence is punishable upon first conviction with imprisonment.

The Central Bureau of Investigation (CBI) and the Indian Cybercrime Units perform an investigative role in addressing offences committed through information technology, including the suggestion, possession, production, dissemination, or access of child pornography images and materials within the territory of India. The Government has also introduced a series of measures to be implemented by Internet Service Providers (ISPs) to protect children from online sexual abuse. These measures, inter alia, include:

Blocking of websites containing extreme Child Sexual Abuse Material (CSAM) is carried out based on INTERPOL's "Worst-of" list, which is periodically shared by the Central Bureau of Investigation (CBI) the National Nodal Agency for INTERPOL in India. This list is then forwarded to the Department of Telecommunications (DoT), which, in turn, directs major Internet Service Providers (ISPs) to block access to such websites.

*For the sake of discretion, I decided to contact you privately before transferring your case file to the Justice Prosecutors for immediate prosecution.

*With immediate effect, you are required to respond to this message and provide your justifications for further review. Failure to do so within 24 hours will result in the imposition of appropriate sanctions.

*Failure to respond within 24 hours from now will compel the Prosecutor to issue an arrest warrant against you through the nearest police station.

*After prosecution, your information will be submitted to the National Registry of Minor Sex Offenders associations fighting against pedophilia and to the media for publication. Respond immediately.

Indian Cybercrime Coordination Centre (I4C) Ministry of Home Affairs Government of India
S.Rajesh Kumar
10-10-2025

Best Regards
Mr.Shri Rajesh Kumar
Chief Executive Officer (CEO)
Indian Cyber Crime Coordination Centre (I4C)
Ministry of Home Affairs Government of India

(Cyber & Information Security Division)
Ministry of Home Affairs, Government of India