INTEGRAL UNIVERSITY
LUCKNOW - INDIA
A+ ACCREDITED BY NAAC | NABH ACCREDITED 820 BEDDED HOSPITAL | NABL ACCREDITED LABS | NBA & ICAR ACCREDITED PROGRAMS | QS I-GAUGE DIAMOND | CELEBRATING 28 YEARS OF EXCELLENCE

# CYBER BULLETIN

CYBER AWARENESS CLUB
DEPARTMENT OF COMPUTER APPLICATION
INTEGRAL UNIVERSITY, LUCKNOW

JULY 2026

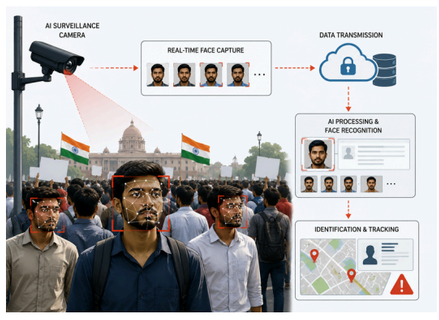
DOI No. 10.5281/zenodo.21791041

## DIGITAL FREEDOM & NATIONAL SECURITY


### Secure Messaging Risks

The allegations against Telegram CEO Pavel Durov intensified the global debate over encrypted messaging platforms. While end-to-end encryption protects users privacy and confidential communications the same technology can also be exploited by cybercriminals to coordinate illegal activities without detection.

Cause: Strong end-to-end encryption, limited platform oversight, challenges in detecting illegal activities.




### AI Surveillance Controversy

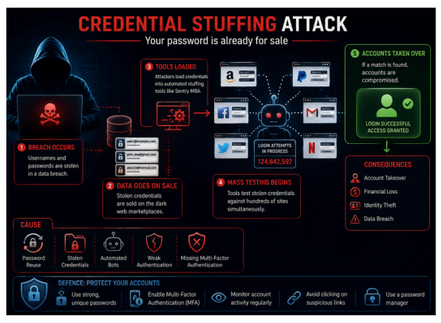
India's use of AI-powered facial recognition and surveillance systems during nationwide youth protests sparked legal and privacy concerns. Activists challenged the deployment, arguing that biometric monitoring lacked adequate legal safeguards and threatened citizen's privacy. The case raised significant cybersecurity and digital rights issues regarding responsible use of AI surveillance technologies.

Cause: AI facial recognition, biometric surveillance and weak legal safeguards.


### Encryption Security at Risk

Apple and Google warned that Canada's proposed Bill C-22 could weaken end-to-end encryption by requiring technology companies to provide lawful access to encrypted data. Security experts cautioned that creating such access could introduce vulnerabilities exploitable by cybercriminals and attacks the users relying on secure digital communications.

Cause: Proposed encryption backdoors, increased surveillance capabilities and creation of security vulnerabilities.




### Credential Stuffing Attack

Credential stuffing is a cyberattack where attackers use usernames and passwords stolen from previous data breaches to gain unauthorized access to online accounts through automated login attempts. Because many users reuse passwords across multiple websites, attackers can compromise shopping, banking and email accounts, leading to fraud, identity theft and financial losses.

Cause: Password reuse, stolen credentials, automated bots and missing MFA.


### Digital Trust Under Attack

Cybercriminals targeted company executives using fake WhatsApp messages, malicious ZIP files and CEO impersonation. After malware hijacked WhatsApp Web sessions, attackers instructed finance teams to transfer funds to mule bank accounts. In one reported case, an employee transferred ₹1.5 crore, believing the request came from the company's CEO.

Cause: CEO impersonation, malicious ZIP files, WhatsApp hijacking, urgency and inadequate payment verification.


### Transnational Scam Networks

The UN warned that organized cybercrime groups across the Asia-Pacific region are expanding large-scale online scam operations generating more than ₹8.39 lakh crore annually. Criminal networks use phishing, investment fraud, romance scams, and fake job offers to steal money and personal information, posing a growing threat to regional cybersecurity and economic stability.

Cause: Organized cybercrime, phishing, investment scams, weak enforcement and cross-border criminal networks.

## BEST PRACTICE

- **Enable multi-factor authentication for all critical accounts.**
- **Use strong, unique passwords with password managers.**
- **Verify identities before approving financial transactions.**
- **Avoid opening suspicious links, files or messages.**
- **Keep operating systems and security software updated.**
- **Monitor account activity and report suspicious incidents promptly.**

## NEWS OF THE MONTH

**Capillary Technologies disclosed that its overseas subsidiary lost over ₹32 crore in a sophisticated deepfake-enabled banking fraud. Attackers used AI voice cloning, forged signatures, and social engineering to impersonate senior executives and authorize fraudulent fund transfers. The incident highlights the growing threat of AI-powered financial fraud targeting corporate approval and payment systems.**

INTEGRAL UNIVERSITY
LUCKNOW - INDIA

A+ ACCREDITED BY NAAC | NABH ACCREDITED 820 BEDDED HOSPITAL | NABL ACCREDITED LABS | NBA & ICAR ACCREDITED PROGRAMS | QS I-GAUGE DIAMOND | CELEBRATING 28 YEARS OF EXCELLENCE

# CYBER BULLETIN

## CYBER AWARENESS CLUB

### DEPARTMENT OF COMPUTER APPLICATION

### INTEGRAL UNIVERSITY, LUCKNOW

JULY 2026

DOI No. 10.5281/zenodo.21791041

इलेक्ट्रॉनिकी एवं सूचना प्रौद्योगिकी मंत्रालय
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
सत्यमेव जयते

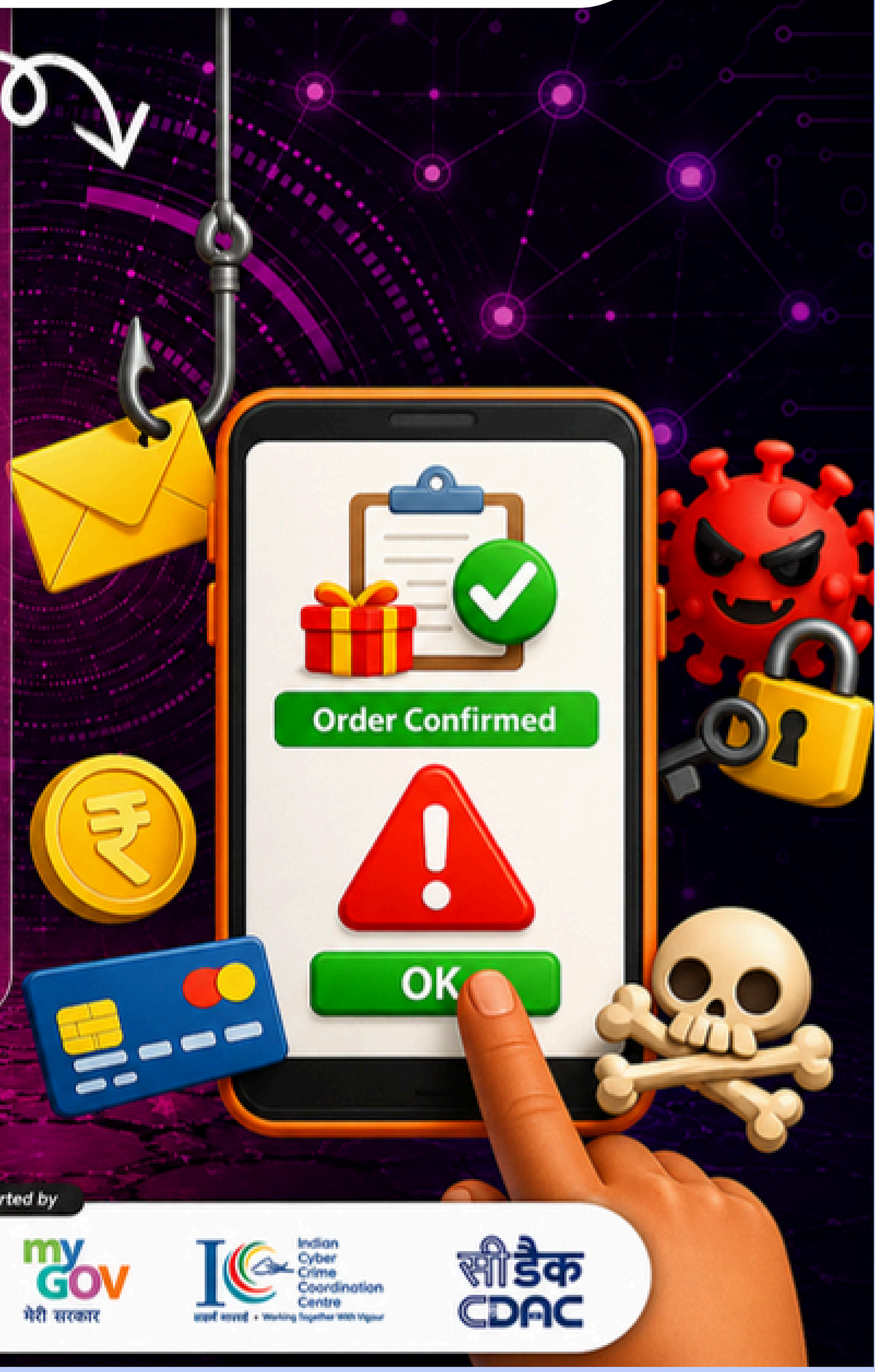
Digital India
Power To Empower

STAY SAFE ONLINE
ऑनलाइन सुरक्षा कवच

ISEA
www.isea.gov.in

CYBER DOST
Follow CyberDost
for official cyber safety tips, fraud alerts, and online security advisories.
Follow CyberDost (@CyberDost) or visit
linktr.ee/cyberdost
Cyber Safety Tips | Fraud Alerts | Security Advisories

**Never click on unexpected order confirmation emails without verifying the sender.**




#PhishingAlert
#OnlineShopping

Supported by

certin — Enhancing Cyber Security in India
साइबर स्वच्छता केन्द्र
CYBER SWACHHTA KENDRA
Botnet Cleaning and Malware Analysis Centre
MyGov मेरी सरकार
I4C Indian Cyber Crime Coordination Centre
सी डैक CDAC

**Stay Alert, Stay Safe, Report Cybercrime 1930 | cybercrime.gov.in**

## CYBER SAKCHHARTA ABHIYAN UNDER THE AEGIS OF CYBER AWARENESS CLUB

FACULTY COORDINATORS
MR. SHUBHAM KUMAR | MR. FAIZAN MAHMOOD | MR. MOHD TALHA

STUDENT COORDINATORS
ANAMTA ANSARI | AREEBA KHAN | ANWAR AHMAD | HASHMAT ZAHRA | HERA FATIMA

Prof.(Dr.) MOHAMMAD FAISAL
HEAD, DEPARTMENT OF COMPUTER APPLICATION

4 QUALITY EDUCATION | 8 DECENT WORK AND ECONOMIC GROWTH | 9 INDUSTRY, INNOVATION AND INFRASTRUCTURE | 16 PEACE, JUSTICE AND STRONG INSTITUTIONS | 17 PARTNERSHIPS FOR THE GOALS

This initiative contributes to the UN Sustainable Development Goals by promoting cybersecurity awareness, digital safety, and resilient technological infrastructure.