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

# CYBER BULLETIN

CYBER AWARENESS CLUB
DEPARTMENT OF COMPUTER APPLICATION
INTEGRAL UNIVERSITY, LUCKNOW

MARCH 2026

DOI No. 10.5281/zenodo.19504892

## END OF FINANCIAL YEAR CYBER ALERT


### ₹7 Crore Cyber Heist

Around ₹7 crore was siphoned from four branches of a cooperative bank after cybercriminals performed unauthorized system access by exploiting a mobile application vulnerability leading to a backend compromise of the core banking software. The fraud was executed on a holiday using multiple devices causing operational disruption though customer deposits remained unsafe.

Cause: Mobile app vulnerability and weak system security controls.

readme

### ITR Phishing Scam

Cyber criminals targeted taxpayers during the filing season by sending fake messages, emails, and calls related to ITR filing and tax refunds. Victims were lured into clicking malicious links and sharing sensitive details like bank credentials and OTPs leading to unauthorized transactions and financial loss.

Cause: Phishing attacks using fake tax-related messages and links.

readme

### Digital Arrest Scam

AAn 81-year-old businessman from Belagavi lost ₹15.45 crore after fraudsters impersonated officials from the Central Bureau of Investigation and Reserve Bank of India. They falsely accused him of involvement in money laundering and used fake documents to create fear. Over six weeks the victim was psychologically pressured to liquidate assets and transfer funds.

Cause: Fear-based social engineering and impersonation scam.

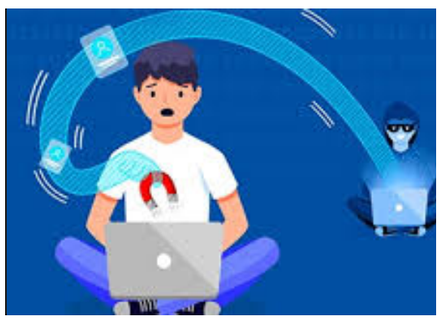
readme


### Recruitment Scam

An inter-state cyber fraud racket defrauded job seekers of ₹7.80 crore by advertising fake government job opportunities. Fraudsters used posters and mobile numbers to trap victims, then demanded money for registration, training and joining. Fake documents were provided to gain trust and funds were routed through mule accounts to avoid detection.

Cause: Fake recruitment offers and social engineering using mule bank accounts.

readme



### Data Exfiltration Attack

A major BPO service provider suffered a cyberattack where attackers gained unauthorized access to internal systems and allegedly stole massive volumes of sensitive data. The attack involved credential harvesting through vishing and phishing, allowing attackers to misuse legitimate access and remain undetected for a long period.

Cause: Vishing-based credential compromise and misuse of legitimate access privileges.

readme


### Multi-Vector Cyber Attack

Hyderabad Cyber Crime Police reported multiple fraud cases where attackers used phishing links, fake apps and impersonation to trick victims into sharing banking details and OTPs. Once access was gained fraudsters performed unauthorized transactions through online banking systems resulting in losses exceeding ₹4.4 crore across various scams including digital arrest fake investment and gaming fraud.

Cause: Victims were tricked into sharing OTPs and banking credentials.

readme

## BEST PRACTICE

- **Enforce MFA zero-trust access and behavior monitoring to prevent unauthorized system access.**
- **Use phishing protection domain authentication and user awareness for safe communication.**
- **Apply strict verification for jobs government claims and financial instructions via official channels.**
- **Strengthen banking security with OTP restrictions device binding biometrics and real-time fraud detection.**

## NEWS OF THE MONTH

**₹67 Crore Investment Scam Operation**

The cyber fraud was caused by a gang operating through fake investment schemes via “Crown Pay” on Telegram. They used social engineering APK malware and identity theft to access banking data and created 700 mule accounts to laundered ₹67 crore through crypto platforms exploiting victim’s trust and financial greed across states.

readme

INTEGRAL UNIVERSITY
LUCKNOW - INDIA

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

# CYBER BULLETIN

## CYBER AWARENESS CLUB

### DEPARTMENT OF COMPUTER APPLICATION

### INTEGRAL UNIVERSITY, LUCKNOW

MARCH 2026

DOI No. 10.5281/zenodo.19504892

इलेक्ट्रॉनिकी एवं सूचना प्रौद्योगिकी मंत्रालय
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY

ISEA www.isea.gov.in

STAY SAFE ONLINE
ऑनलाइन सुरक्षा बन्धन

Always check for RBI or SEBI alerts on risky or fake investment schemes


#RBIAlert
#SEBIUpdate

Supported by

साइबर स्वच्छता केन्द्र
CYBER SWACHHTA KENDRA
Botnet Cleaning and Malware Analysis Centre

Digital India Power To Empower

MyGov मेरी सरकार

Indian Cyber Crime Coordination Centre

सीडैक CDAC

## STAY ALERT, STAY SAFE, REPORT CYBERCRIME 1930

## 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.