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

MAY 2026

DOI No. 10.5281/zenodo.20757321

SAFE TRAVEL & SAFE DIGITAL LIFE

Hotel Reservation Breach

A large-scale reservation hijacking campaign affected 350+ hotels, motels, vacation rentals, & guesthouses across 50 countries. Cybercriminals gained access to hotel booking systems and guest details like names and stay dates. They used this information to send phishing messages via email, SMS, WhatsApp & booking platforms leading victims to fake payment pages and stealing personal and financial data.

Cause: Compromised accounts, weak security, and missing multi-factor authentication.

readme

Travel Cyber Threats

Travel organizations, including hotels, airlines, airports, and car rental companies, faced increasing cyber threats due to the vast amount of customer and travel data they manage. Attackers used phishing, ransomware, third-party vendor breaches, and AI-driven social engineering, exposing millions of records and stealing sensitive traveler and business information.

Cause: Phishing, ransomware, vendor breaches, and weak cybersecurity practices.

readme

Digital Payment Fraud

A major cyber money-laundering network involving ₹631.86 crore was uncovered in Gujarat under Operation Mule Hunt 2.0. Criminals used fake companies and mule bank accounts across multiple cities to transfer proceeds from cyber scams. Funds were layered through transactions and cash withdrawals to hide origins and support fraud.

Cause: Mule accounts, shell companies, weak KYC, inadequate monitoring.

readme

Digital Arrest Scam

Cyber police in Gurugram arrested two accused in a ₹78 lakh "digital arrest" fraud case. Victims were intimidated by scammers posing as police officials and forced to transfer money into multiple accounts under false investigation claims. The funds were routed through mule accounts linked to broader cybercrime networks.

Cause: Police impersonation, intimidation scams, and mule accounts misuse.

readme

Hotel Account Phishing

Attackers targeted Booking.com hosts and guests by exploiting messaging and review systems to send phishing emails and malware links. Using compromised or fake hotel accounts, they impersonated legitimate properties and tricked victims into revealing login credentials and payment information, leading to account takeovers, credential theft, and financial fraud.

Cause: Compromised accounts, phishing abuse and weak message verification.

readme

FIFA 2026 Digital Scams

Cybercriminals are exploiting the excitement around FIFA World Cup 2026 through fake ticketing websites, counterfeit travel booking platforms, malicious mobile apps, and phishing pages. These scams steal login credentials, payment information and personal data. Attackers also target travel, hospitality and sports organizations with ransomware and social engineering tactics.

Cause: Fake websites, event hype, fake domains, phishing and ransomware attacks.

readme

BEST PRACTICE

- **Enable multi-factor authentication on all important accounts**
- **Use only official websites, apps, and verified platforms**
- **Never share OTPs, passwords, or banking credentials with anyone**
- **Verify emails, messages, and calls before taking any action**
- **Avoid clicking unknown links, fake ads, or suspicious attachments**
- **Report suspicious transactions and fraud attempts immediately to authorities**

NEWS OF THE MONTH

Attackers used Claude and GPT-4.1 to automate vulnerability discovery, reconnaissance, exploit development, and data analysis. The AI-assisted attack enabled the compromise of multiple Mexican government systems and the theft of hundreds of millions of sensitive citizen records, demonstrating how AI can significantly enhance cybercriminal capabilities and attack efficiency.

readme

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

MAY 2026

DOI No. 10.5281/zenodo.20757321

MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY | Digital India | ISEA www.isea.gov.in | STAY SAFE ONLINE

STAY ALERT. STAY SECURE

Supported by

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

myGov मेरी सरकार | Indian Cyber Crime Coordination Centre | सी-डैक 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.