INTEGRAL UNIVERSITY
LUCKNOW - INDIA
A+ ACCREDITED BY NAAC
DOI No. 10.5281/zenodo.16215217
JUNE 2025

CYBER BULLETIN

Cyber Surge: June's Attack Watch

1. FileFix Rat Threat

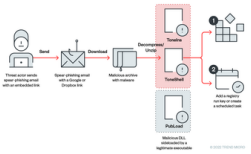
CLIPBOARD HIJACKING

TARGET: Healthcare, tech firms, public sector; users with poor security awareness.

IMPACT: Data theft, double extortion, follow-up ransomware payloads.

MITIGATION: Train users to avoid suspicious links and pop-ups, use antivirus and block risky tools like PowerShell.

2. Mustang Panda Espionage



PHISHING SIDELOAD

TARGET: Tibetan communities, cultural and religious organizations.

IMPACT: Espionage activity, data theft, unauthorized access, surveillance breach, phishing emails, USB infections, targeted spying.

MITITGATION: Avoid unknown emails, block USBs, set alerts, train staff, monitor traffic, detect sideloading.

3. Newsroom Data Heist

CREDENTIAL THEFT

TARGET: Newspaper giant Lee Enterprises, Employee Records, Sensitive Documents, Editorial Content Systems

IMPACT: The attack leaked 40,000 SSNs, cost the company ₹16 crore and disrupted newspaper publishing services.

MITIGATION: Keep offline backups and act quickly on infections. train employees to spot phishing and alert authorities.

4. Echo Chamber Exploit

SEMANTIC PROMPT INJECTION

TARGET: LLMs like OpenAI's , ChatGPT and Google's Gemini, primarily used by the general public, developers, and enterprises.

IMPACT: Atackers bypassed AI safety to generate hate speech, misinformation, and self-harm content.
Success rates 90% for toxic output and 80% for misleading prompts.

MITIGATION: Ensure AI safety tools analyze full conversations. Use JBShield to detect hidden jailbreaks and conduct ongoing adversarial testing.

5. Korea Ticket Hack

SERVICE DISRUPTION

TARGET: Yes24's online ticketing system, user accounts, employee data, and event booking infrastructure.

IMPACT: Booking and concert services were disrupted, user data was potentially exposed, and public trust in the platform was weakened.

MITIGATION: Legal steps were taken, identity verification was strengthened, advanced technologies like AI, blockchain, biometrics were used to secure user data.

6. Oxford Data Breach

PHISHING EMAILS

TARGET: Oxford City Council's internal IT systems, including administrative data, citizen records, and service portals.

IMPACT: Sensitive data from past 20 years was exposed, disrupting essential public services and potentially risking citizen privacy and identity security.

MITIGATION: Authorities isolated compromised systems, used expert forensics to trace the breach, and strengthened data protection with advanced monitoring tools.

INTEGRAL UNIVERSITY
LUCKNOW - INDIA
A+ ACCREDITED BY NAAC
DOI No. 10.5281/zenodo.16215217
JUNE 2025

इलेक्ट्रॉनिकी एवं सूचना प्रौद्योगिकी मंत्रालय
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
ISEA www.isea.gov.in
STAY SAFE ONLINE ऑनलाइन सुरक्षा बचाव

CYBER SECURITY
POSTER OF THE DAY

Phishing scams can trick you into giving your multi-factor codes

Never share these codes with anyone

#Vishing calls

Supported by
साइबर स्वच्छता केन्द्र
CYBER SWACHHTA KENDRA
Botnet Cleaning and Malware Analysis Centre
Digital India
myGov मेरी सरकार
Indian Cyber Crime Coordination Centre
सी डैक CDAC

CYBER SAKCHHARTA ABHIYAN
UNDER THE AEGIS OF
CYBER AWARENESS CLUB
DEPARTMENT OF COMPUTER APPLICATION

FACULTY COORDINATORS
MR. SHUBHAM KUMAR | MR. FAIZAN MAHMOOD | MR. MOHD TALHA
STUDENTS COORDINATORS
ANAMTA ANSARI | AREEBA KHAN

Prof.(Dr.) MOHAMMAD FAISAL
Head, Department of Computer Application