

CYBER BULLETIN



CYBER AWARENESS CLUB
DEPARTMENT OF COMPUTER APPLICATION
INTEGRAL UNIVERSITY, LUCKNOW

JUNE 2026

DOI No. 10.5281/zenodo.21404307

SMART ONLINE SHOPPING SAFETY



AI-Assisted Shopping Fraud

Cybercriminals created fake e-commerce websites that closely resembled trusted brands and appeared in AI-assisted shopping recommendations. Victims were lured by attractive discounts, entered payment details, and purchased products that were never delivered. The incident demonstrated how AI-generated recommendations can unintentionally expose users to fraudulent websites.

Cause: Cloned shopping websites and failure to verify website authenticity before purchasing.



Fake Shopping Websites

Google's June 2026 Fraud & Scams Advisory warned that cybercriminals are increasingly using AI to create realistic fake shopping websites, phishing pages, and fraudulent advertisements that imitate trusted brands. These scams steal payment details, login credentials, and personal information, causing financial losses and identity theft. Google identified this as a growing global cyber threat affecting online shoppers.

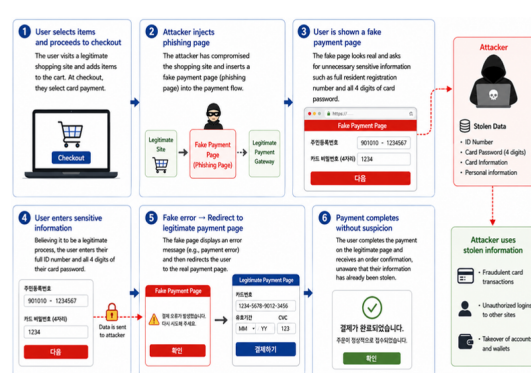
Cause: AI-generated fake shopping websites, phishing pages and fraudulent advertisements



Jamtara E-Commerce Fraud

A cybercrime groups are using device farming to conduct large-scale e-commerce fraud. The study analyzed 70 million users and identified 256 fraud clusters around 45,000 fake accounts operating from 9,000 devices. Fraudsters exploited cashback and referral to steal money and compromise customer accounts causing financial losses for businesses and consumers.

Cause: Device farming, exploitation of return policies and exploitation of saved payment details.



AI Checkout Phishing

South Korean authorities uncovered a large-scale phishing campaign targeting online shopping sites. Attackers used fake checkout pages into legitimate payment processes tricking users into entering their cards details and passwords before redirecting them to the real payment page. Authorities identified 5,707 cases involving stolen credit card details and personal information.

Cause: Fake AI-generated checkout pages and entering sensitive details without verifying payment page authenticity.



AI Fake Store Scam

The growing use of AI-assisted online shopping scams involving fake Instagram stores, fraudulent delivery confirmations, parcel substitution and OTP misuse. In one case a shopper lost ₹49,235 after paying a fake delivery verification fee while another purchased sunglasses for ₹399 that never arrived. Fraudsters exploit trust in digital shopping and delivery systems to steal money and personal information.

Cause: AI-generated fake shopping stores, OTP misuse and inadequate verification of sellers.



Prime Day Delivery Scam

During Amazon Prime Day cybercriminals exploited the surge in online shopping by using AI enabled phishing techniques to send fake delivery messages, QR codes, emails and payment requests. Victims were tricked into revealing OTPs, card details or making fake delivery payments. The attacks leveraged shoppers expectation of parcel updates, increasing the success of financial fraud and identity theft.

Cause: Counterfeit Amazon login pages, spoofed customer support calls and clicking unverified links



BEST PRACTICE

- Enable multi-factor authentication on all important online accounts.
- Purchase products only from official websites.
- Never share OTPs, passwords, PINs or banking credentials with anyone.
- Verify website URLs, payment pages and seller before purchasing.
- Avoid clicking suspicious links, advertisements, emails.
- Report fraudulent websites, suspicious transactions to authorities immediately.

NEWS OF THE MONTH

Google filed a lawsuit against the operators of the "Outsider" phishing network accusing them of using AI-powered phishing kits to create fake banking, shopping and government websites. The campaign generated over 1.5 million phishing URLs enabling large-scale theft of login credentials, financial information and personal data highlighting the growing threat of AI-enabled cybercrime.





INTEGRAL UNIVERSITY
LUCKNOW - INDIA

A+ ACCREDITED BY NAAC

NABH ACCREDITED
820 BEDDED HOSPITAL

NABL ACCREDITED
LABS

NBA & ICAR ACCREDITED
PROGRAMS

QS I-GAUGE
DIAMOND

28
YEARS
OF EXCELLENCE

CYBER BULLETIN



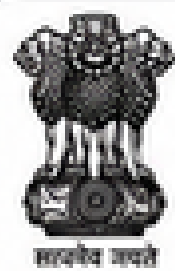
CYBER AWARENESS CLUB

DEPARTMENT OF COMPUTER APPLICATION

INTEGRAL UNIVERSITY, LUCKNOW

JUNE 2026

DOI No. 10.5281/zenodo.21404307



इलेक्ट्रॉनिक्स एवं सूचना प्रौद्योगिकी मंत्रालय
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY



Digital India
Power To Empower



www.isea.gov.in



STAY SAFE ONLINE
ऑनलाइन सुरक्षा कायम

Read customer reviews carefully
fake reviews are often overly positive and repetitive.

#ReviewCheck
CyberSafety

Supported by

certin
Enhancing Cyber Security in India

साइबर स्वच्छता केंद्र
CYBER SWACHHTA KENDRA
Botnet Clearing and Malware Analysis Centre

my GOV
मेरी सरकार

IC Indian Cyber Crime Coordination Centre
क़ानून से सजगें • Working Together With Vigour

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

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

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



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