



**CHHATRAPATI SHAHU JI MAHARAJ UNIVERSITY, KANPUR**

**ATAL BIHARI VAJPAYEE SCHOOL OF LEGAL STUDIES**

## **EVENT REPORT**

**GUEST LECTURE ON :**  
**ARTIFICIAL INTELLIGENCE (AI) AND CYBER CRIME**  
**NEW CHALLENGES BEFORE LAW**

**Date:** 31 January 2026

**Venue:** Lecture hall 1

Chhatrapati Shahu Ji Maharaj University, Kanpur.

### EVENT DETAILS

<b>Particulars</b>	<b>Details</b>
Name of the Event	Guest lecture on Artificial Intelligence (A.I.) and cyber crime new challenges before law
Date	31 January 2026
Venue	Lecture Hall 1, CSJMU, Kanpur
Organized By	Atal Bihari Vajpayee School of Legal Studies
Nature of Event	Guest lecture
Faculty Coordinators	Mr. Prerit Narayan Mishra

# Atal Bihari Vajpayee School of Legal Studies

(January 31, 2026)

## FLOW OF EVENT

Time	Event
12:00PM	Arrival of the Dignitaries
12:05 PM	Lighting of the Lamp
12:10PM	Felicitation of the Dignitaries with Pot, Shawl & Mementos
12:20 PM	Welcome Address by Dr. Shashikant Tripathi, Chief Proctor, CSJMU.
12:25PM	Address by Shri Rajiv Kumar , S.I. U.P. Police
12:30PM	Address by Shri Subham Yadav, S.I. U.P. Police
12:35PM	Address by Shri Arun Yadav, S.I. U.P. Police
12:40 PM	Address by Ms. Riya , S.I. U.P. Police
01:15 PM	Special Address by Kapil Dev Singh, Addl DCP, Police Commissionerate, Kanpur West
01:45 PM	Vote of Thanks by Mr. Prerit Narayan Mishra
01:50 PM	National Anthem

## EVENT REPORT

On 31 January 2026, a guest lecture on the theme *Artificial Intelligence (AI) and Cyber Crime: New Challenges Before Law* was organised at Lecture Hall-1, Chhatrapati Shahu Ji Maharaj University, Kanpur, by the Atal Bihari Vajpayee School of Legal Studies. The programme witnessed the presence of faculty members, research scholars, and **225 law students**.

The event commenced at 12:00 PM with the arrival of the dignitaries, followed by the ceremonial lighting of the lamp. The invited guests were formally welcomed and felicitated with pots, shawls, and mementoes as a mark of respect. Thereafter, the welcome address was delivered by Dr. Shashikant Tripathi, Chief Proctor, CSJMU, who highlighted the growing importance of legal awareness in the digital era.

The lecture session included insightful addresses by cybercrime experts. **Shri Rajiv Kumar** explained the concept of *AI Voice Scam*, highlighting how artificial intelligence is used to mimic voices and create fake emergency situations to deceive victims.

**Shri Subham Yadav** elaborated on *WhatsApp Scam* and *Electricity Bill Scam*, cautioning students against sharing OTPs and responding to urgent payment messages from unknown sources.

**Shri Arun Yadav** focused on *Part-Time Job Scam*, *Chit Funds/Ponzi Scheme Scam*, and *Instant Loan Scam*, explaining how such schemes exploit individuals through false promises of easy money and financial benefits.

**Ms. Riya** addressed *Digital Arrest Scam*, *Dating App Scam*, and *Fake Gaming Apps*, highlighting how cybercriminals misuse identity, emotions, and malicious applications to commit fraud.

In addition to explaining these scams, the speakers also provided **practical cyber safety guidelines**, advising students to avoid clicking on unknown links, never share OTPs or passwords, verify suspicious communications, and download applications only from trusted sources.

The speakers also explained **preventive and response measures in case of cybercrime**, including contacting the National Cyber Crime Helpline **1930**, reporting complaints on **cybercrime.gov.in**, approaching the nearest cyber police station, and preserving digital evidence.

The session was further enriched by the chief guest, Shri Kapil Dev Singh, Additional Deputy Commissioner of Police, Police Commissionerate, Kanpur West, who delivered a special address on cybercrime investigation, digital vigilance, and the legal responsibilities of citizens in the digital space. He emphasized the importance of timely reporting and public awareness to effectively combat cyber offences.

An interactive question-and-answer session was held during the programme, during which students actively participated and raised queries on cybercrime reporting, digital evidence, legal remedies, and preventive measures.

The programme concluded with a vote of thanks proposed by Mr. Prerit Narayan Mishra, followed by the National Anthem. The guest lecture was informative, practical, and highly relevant, equipping students with both theoretical understanding and real-world awareness of emerging cyber threats and digital safety practices.









### साइबर अपराधियाँ से सावधान रहें

- इंटरनेट बैकिंग / सोशल मीडिया पर नजबूत एवं कठिन पासवर्ड का प्रयोग करें।
- सोशल मीडिया प्रोफाइलों पर **Two step verification** इस्तेमाल करें।
- अनवैरीफाइड सोर्स से कोई फाइल डाउनलोड ना करें ना ही किसी अनजान नंबर से कोई फोटो डाउनलोड करें। अपने स्मार्टफोन पर ऑटो डाउनलोड फीचर को ऑफ कर दें।
- अनऑथराइज्ड डेविंग एप तथा वेबसाइट से सावधान रहें।
- किसी अनजान नंबर से व्हाट्सएप कॉल/वीडियो कॉल अथवा फोन ना उठाएं।
- अगर किसी कस्टमर केयर नंबर से आपको कोई फीस/पैसे या लॉगिन करने के लिए भुगतान करने का मैसेज आए तो उसे पर ध्यान ना दें और न ही उससे संबंधित किसी लिंक पर क्लिक करें।
- अपना मोबाइल सिम अधिकृत सिम केंद्रों से ही खरीदें।
- मोबाइल फोन खोने एवं चोरी होने की स्थिति में अपना सिम तथा बैक खाते को तुरंत ब्लॉक कराएं।
- कोई भी पुलिस/कस्टम/इनकम टैक्स/सीबीआई का अधिकारी व अन्य कोई सरकारी संस्था आपको फोन/लैपटॉप/वीडियो पर गिटपत्तार नहीं कर सकती। ऐसे किसी भी संबंधित कॉल आने पर फोन को तुरंत डिस्कनेक्ट करें।
- किसी अनजान व्यक्ति को अपना ओटीपी/पिन/पासवर्ड कभी न बताएं।
- एसएमएस व व्हाट्सएप पर किसी ऐप का लिंक क्लिक न करें और न ही कोई APK फाइल डाउनलोड करें।
- किसी भी जानकारी या अनजान व्यक्ति को अपने फोन से व्यक्तिगत फोटो अथवा वीडियो शेयर न करें जो भविष्य में आपके लिए शर्मिंदगी का कारण बन सकता है।

### साइबर क्राइम संबंधी पुलिस कमिश्नरेट कानपुर नगर के महत्वपूर्ण CUG नंबर

थाना साइबर क्राइम	7839876675 7839863374
साइबर सेल सेंद्रल जोन	7839871341
साइबर सेल पूर्वी जोन	7839863467
साइबर सेल पश्चिम जोन	7839863270
साइबर सेल दक्षिण जोन	8879348041

### साइबर अपराध हो जाने के पश्चात निम्न कार्रवाई करें-

- सर्वप्रथम साइबर हेल्पलाइन नंबर 1930 पर कॉल करें तथा भेजें गए लिंक पर पूर्ण जानकारी अपलोड करें।
- वेबसाइट cybercrime.gov.in पर लॉगिन करके अपने शिकायत पूर्ण विवरण सहित दर्ज कराएं।
- तत्काल अपने निकटतम थाना/साइबर सेल पर संपर्क करें।
- साइबर अपराध में संलिप्त अपने फोन/डिवाइस से कुछ भी डिलीट किए बिना साइबर सेल/थाना पर संपर्क करें। शिकायत करने से न घबराएं।

1930  
DIAL  
Call this number to report cyber crimes to National Cyber Crime Reporting Portal

Cybercrime.gov.in पर करें।

## STOP THINK ACT

सुरक्षा आपकी सक्ल्य हमारा

POLICE COMMISSIONERATE KANPUR NAGAR

@kanpunagarpol | KanpurPoliceOfficial | kanpunagarpolice | @kanpunagarpolice

### गोल्डन ऑवर रिपोर्टिंग (GOLDEN HOUR REPORTING)

आपकी तुरंत शिकायत ही रिकवरी की कुंजी है।

साइबर फ्राँड से रहें सावधान! साइबर सम्बन्धित फ्राँड की शिकायत

1930  
DIAL  
Call this number to report cyber crimes to National Cyber Crime Reporting Portal

Cybercrime.gov.in पर करें।

## STOP THINK ACT

सुरक्षा आपकी सक्ल्य हमारा

POLICE COMMISSIONERATE KANPUR NAGAR

@kanpunagarpol | KanpurPoliceOfficial | kanpunagarpolice | @kanpunagarpolice

### एआई वॉइस स्केम (AI VOICE SCAM)

एआई वॉइस स्केम में कृत्रिम बुद्धिमत्ता (Artificial Intelligence) का उपयोग किसी व्यक्ति की आवाज की नकल करने के लिए किया जाता है। धोखेबाज अक्सर किसी परिवार के सदस्य का रूप धारण करके झूठी आपात स्थिति बनाते हैं ताकि पीड़ित व्यक्ति से पैसे या व्यक्तिगत जानकारी प्राप्त कर सकें। ये ठगों के मामले अब ज्यादा आम और वास्तविक भूते लगने लगे हैं क्योंकि सोशल मीडिया या अन्य रिकॉर्डिंग से थोड़ी-सी आवाज लेबर भी इन्हें बनाया जा सकता है।

### व्हाट्सएप स्केम (WHATSAPP SCAM)

ठग आपके व्हाट्सएप पर एक ओटीपी (OTP) खोजती से भेजने का बहाना बनाते हैं और फिर आपसे उसे फ्राँडवर्ड (भेजने) के लिए कहते हैं। जैसे ही आप ओटीपी साझा करते हैं, वे आपको व्हाट्सएप अकाउंट हक कर लेते हैं, आपके संदेश, व्यक्तिगत जानकारी और भविष्य में आने वाले ओटीपी तक पहुंच बना लेते हैं। कभी भी अपना ओटीपी किसी के साथ साझा न करें, चाहे संदेश कितना भी जरूरी या दोस्ताना क्यों न लगें। व्हाट्सएप कभी भी चैट के माध्यम से वेरिफिकेशन नहीं मांगता।

### डिजिटल अरेस्ट (DIGITAL ARREST)

आपको किसी व्यक्ति से वीडियो कॉल आती है जो खुद को पुलिस अधिकारी या सरकारी अधिकारी बताता है। वह आप पर कानूनी कार्रवाई की धमकी देता है और 'मामला निपटाने' के लिए पैसे की मांग करता है। यह पूरी तरह से फर्जी होता है।

### बिजली बिल स्केम (ELECTRICITY BILL SCAM)

इन ठगों में अपराधी नकली बिजली बिल भेजते हैं या मैसेज, ईमेल या कॉल के जरिए तुरंत भुगतान करने की मांग करते हैं, यह कहकर कि यदि भुगतान नहीं किया तो बिजली सेवा काट दी जाएगी।

### पार्ट-टाइम जॉब स्केम (PART TIME JOB SCAM)

आपको आसान ऑनलाइन नौकरी का ऑफर दिया जाता है, लेकिन जॉइन करने से पहले आपसे 'टेनिंग' या 'रजिस्ट्रेशन शुल्क' के नाम पर पैसे मांगे जाते हैं। जैसे ही आप पैसे देते हैं, न नौकरी मिलती है, न ठग का कोई पता चलता है। कोई भी असली नौकरी आपसे पैसे नहीं मांगती। ऐसे ऑफर से दूर रहें और तुरंत शिकायत दर्ज करें।

### एमएलएम, चिट फंड्स और पॉन्जी स्कीम्स (MLM, CHIT FUNDS, PONZI SCHEMES)

'एमएलएम चिट फंड्स' का मतलब मल्टी-लेवल मार्केटिंग (MLM) और मनी सर्कुलेशन स्कीम्स के अर्थ में है जो भारत के Prize Chits and Money Circulation Schemes (Banning) Act, 1978 के तहत प्रतिबंधित हैं। इन योजनाओं में प्रिजिडेंट जैसी संरचना होती है, जहाँ असली आय उत्पादों की बिक्री से नहीं बल्कि नए सदस्यों से लिए गए शुल्कों से आती है। ये योजनाएं धोखाधड़ीपूर्ण होती हैं और लोगों को भारी आर्थिक नुकसान पहुंचाती हैं।

### एआई वॉइस स्केम (AI VOICE SCAM)

एआई वॉइस स्केम में कृत्रिम बुद्धिमत्ता (Artificial Intelligence) का उपयोग किसी व्यक्ति की आवाज की नकल करने के लिए किया जाता है। ठग अक्सर किसी परिवार के सदस्य या परिवर्तित की आवाज में बात करते हैं और झूठी आपात स्थिति (Fake Emergency) का बहाना बनाकर पीड़ित से पैसे या व्यक्तिगत जानकारी ले लेते हैं। ये ठगों के मामले अब पहले से कहीं ज्यादा आम और भरोसेमंद लगने वाले हो गए हैं, क्योंकि इन्हें बनाने के लिए सोशल मीडिया या किसी अन्य रिकॉर्डिंग से सिर्फ थोड़ी-सी आवाज लेबर भी काफी होती है।

### इंस्टैंट लोन स्केम (INSTANT LOAN SCAM)

कुछ नकली ऐप या वेबसाइट 'तुरंत लोन' देने का झांसा देते हैं, लेकिन वास्तव में वे आपकी व्यक्तिगत जानकारी चुरा लेते हैं या उच्च ब्याज दरों में फंसा देते हैं। कुछ ऐप्स में आपके फोन को हक कर लेते हैं।

### डेटिंग ऐप स्केम (DATING APP SCAM)

ठग डेटिंग ऐप्स पर नकली प्रोफाइल बनाकर आपसे विश्वास का रिश्ता बनाने की कोशिश करते हैं। विश्वास बनने के बाद वे आपसे पैसे या व्यक्तिगत जानकारी मांगते हैं। कई बार वे भावनात्मक रूप से ब्लैकमेल या धमकी भी देते हैं। कभी भी किसी ऐसे व्यक्ति को पैसे या निजी जानकारी न भेजें जिससे आप सिर्फ ऑनलाइन मिले हों। अगर कोई अशोभनीय या सन्दिग्ध संदेश भेजे, तो तुरंत उसकी रिपोर्ट करें।

### फेक गेमिंग ऐप्स (FAKE GAMING APPS)

कुछ गेमिंग ऐप्स के अंदर हानिकारक सॉफ्टवेयर (मैलवेयर या स्पायवेयर) छिपा होता है, जो आपकी व्यक्तिगत जानकारी चुरा सकते हैं या आपकी ऑनलाइन गतिविधियों पर नजर रख सकते हैं। कई बार ये ऐप्स नकली इनाम या पुरस्कार देने का झांसा देकर आपसे जानकारी निकलवाते हैं। हमेशा सावधानी रखें:

- केवल विश्वसनीय ऐप स्टोर (जैसे Google Play या Apple App Store) से ही ऐप डाउनलोड करें।
- ऐप की रेटिंग, रिव्यू और मांगी गई परमिशन ध्यान से जांचें।

पुलिस कमिश्नरेट कानपुर नगर

The above pamphlets were distributed among all the students