



THREE-DAY CERTIFICATE COURSE ON

CYBER SECURITY & DIGITAL FORENSICS

IN BLENDED MODE (ONLINE & PHYSICAL)

REGISTER TODAY

Course Fee: Rs. 10,000/- (INR)

Eligibility: Candidates who are pursuing graduation or have graduated are eligible to register.

Programme Dates: January 9–11, 2026 (3 Days)

Last date to apply: 5 January 2026

Intake: 45 per batch

Note: Admission will be first come first served basis.



SCAN TO APPLY

**(A PRACTICAL ORIENTED, HANDS-ON,
SKILL DEVELOPMENT PROGRAM)**



LEARNING OUTCOMES

After completing this course, participants shall be able to

- Understand the fundamental principles such as confidentiality, integrity, availability (CIA triad), authentication, authorization, and non-repudiation.
- Identify Common Cyber Threats and Attacks by recognizing various forms of cyber threats including malware, phishing, ransomware, social engineering, network attacks, and insider threats.
- Apply Basic Cyber Defense Techniques for the Implementation of essential security practices for safe data handling measures.
- Analyze Network and System Vulnerabilities by Using basic tools and techniques to detect vulnerabilities, assess risks, and understand how attackers exploit weaknesses.
- Respond Effectively to Cybersecurity Incidents to handle incident response procedures and outline the steps required to contain, mitigate, and recover security breaches.
- Understand the Foundations of Digital Forensics by exploring the principles of digital evidence, chain of custody, and legal/ethical considerations in forensic investigations.
- Perform Basic Digital Forensic Techniques by using digital forensic tool kits to acquire, preserve, and analyze digital evidence from computers or mobile devices.
- Interpret Forensic Findings in the electronic evidence by documenting observations, generating simple forensic reports, and understanding how findings support investigations.
- Understand the benefits of Digital Evidence in Legal Proceedings and Challenges in handling it for increasing the conviction rates in criminal proceedings along with understating the Section 65B under the Indian Evidence Act, 1872, that governs the admissibility of electronic evidence.
- Enhance Personal and Organizational Cyber Hygiene by adopting best practices for securing personal devices, networks, and online presence while promoting cybersecurity awareness.

Course Fee: Rs. 10,000/- (INR)

Eligibility: *Candidates who are pursuing graduation or have graduated are eligible to register.*

Programme Dates: *January 9–11, 2026 (3 Days)*

Last date to apply: *5 January 2026*

Intake: *45 per batch*

Note: *Admission will be first come first served basis.*

REGISTER TODAY

CLICK HERE TO APPLY

**(A PRACTICAL ORIENTED, HANDS-ON,
SKILL DEVELOPMENT PROGRAM)**



TOPICS COVERED

- **Definition of Cyber Security and Web-technology:** Definition and basics of Computers, Electronic Devices, Operating Systems, Cyber Safety, Cyber Security, CIA Triad (Confidentiality, Integrity & Availability of Information), Fundamentals of Digital Hygiene, Types of Cyber Threats. Architecture of Cyberspace, Communication and Web technology, Internet, World Wide Web, Advent of Internet, Internet infrastructure for data transfer and governance, Internet society.
- **Regulation of Cyberspace:** Cyber Security Mechanisms, need and modes of Cryptography, Encryption, Firewalls, Passwords, Privacy, Digital Signatures- Issues and challenges of cyber security.
- **Emerging Technologies & Trends:** IPv4(Internet Protocol Version)v/s IPv6, IOT(Internet of Things), Machine Learning, Artificial Intelligence, Crypto currency and Block Chain Technology, Cloud Computing, Web 3, and Dark Web.
- **Types of Cyber Crimes:** Hacking (Computer Viruses, Time Bombs, Trojans, Malicious Code "Malware", DOS, DDOS, Web defacement, Phishing, cloning, financial frauds, social engineering attacks, malware and ransom ware attacks, zero-day and zero click attacks), Cyber Stalking, Cyber Bullying, Cyber Pornography, Child Pornography, Cyber Laundering, Online betting and games, Violation of Cyber Privacy, Voyeurism, Data Privacy, Data Theft, and Cyber Terrorism.
- **Cyber Crime Investigation:** Cyber Crime Cells, Reporting of Cyber Crimes, Cyber Investigation.
- **Electronic Evidence Retrievals:** Analysis and significance of Cyber Forensics- Introduction to Cyber Forensic Life cycle, Digital formats of data storage media- Internal architecture of existing storage media with reference to electronic evidence
- **Legislative framework and Judicial response on admissibility of electronic evidence under IT Act, BNS, BSA, BNSS, POCSO and DPDA.**

Course Fee: Rs. 10,000/- (INR)

Eligibility: *Candidates who are pursuing graduation or have graduated are eligible to register.*

Programme Dates: *January 9–11, 2026 (3 Days)*

Last date to apply: *5 January 2026*

Intake: *45 per batch*

Note: *Admission will be first come first served basis.*

REGISTER TODAY

CLICK HERE TO APPLY

**(A PRACTICAL ORIENTED, HANDS-ON,
SKILL DEVELOPMENT PROGRAM)**



PRACTICAL EXERCISES USING VIRTUAL LABS

- **Authentication Management:** Definition and importance of authentication, types of authentications – Facial, Iris, Fingerprint, Palm print, multi-factor, Use of authentication – places where authentication access should be used.
- **Password Management:** Importance of password management, creation of strong, unique & secure passwords, techniques of maintaining passwords over various platforms, updating passwords regularly, password management tools and practices.
- **Secure Internet Browsing:** Understanding secure connections (HTTPS) & avoiding untrusted networks, Web browser security settings & extensions.
- **Cyber Control Systems:** List out security controls for the computer and implement technical security controls in the personal computer. List out security controls for mobile phones and implement technical security controls in the personal mobile phone.
- **Cyber Crimes Case studies:** Demonstration of DDOS, DNS Poisoning attacks, SQL Attacks, Malware and Ransomware attacks, and creating awareness on preventive measures.
- **Cyber Crime Scene Management:** Learn the fundamentals of Digital Forensics and Incidence Response (DFIR) tool kits and its practice usage for Cyber Crime Investigation procedures on Kali Linux, Autopsy, CSI Linux Etc

MODE OF DELIVERY

- **Mode of Delivery:** Blended (both Online and Physical) Sessions commence at 10AM and ends at 5PM, all the three days of the course delivery.
- **Location for Physical mode:** Cyber Forensics Lab, Cyber Security and Digital Forensics Center - CSDFC, CNLU Campus, Patna.
- **Registration Process:** Submission of Online Application Form along with the requisite fee.

Course Fee: *Rs. 10,000/- (INR)*

Eligibility: *Candidates who are pursuing graduation or have graduated are eligible to register.*

Programme Dates: *January 9–11, 2026 (3 Days)*

Last date to apply: *5 January 2026*

Intake: *45 per batch*

Note: *Admission will be first come first served basis.*

REGISTER TODAY

CLICK HERE TO APPLY

**(A PRACTICAL ORIENTED, HANDS-ON,
SKILL DEVELOPMENT PROGRAM)**