Communication & Information Services (CIS), and University Science Instrumentation Center (USIC),
Jawaharlal Nehru University (JNU)
_____
Event Report

Two-Day Training Programme on "Proactive Cyber Security: Identifying Emerging Threats and Deploying Effective Defenses" Under ISEA Project Phase III, MeitY, Government of India was conducted by CIS and USIC in collaboration with Centre for Development of Advanced Computing (CDAC) Noida organized Two-Day Training Programme on 14th – 15th July 2025 at Convention Centre, Jawaharlal Nehru University (JNU), New Delhi.

The training was aimed at equipping the academic community, researchers, students, technical staff, and government officials with the necessary knowledge and practical tools to proactively address the growing challenges in the realm of cyber security.

Objective

The primary objective of the programme was to raise awareness and build capacity among participants in identifying emerging cyber threats and implementing effective cyber defense strategies to ensure digital safety and resilience.

Participation

The event witnessed enthusiastic participation from over **100 attendees**, including senior university officials, faculty members, researchers, administrators, non-teaching staff, and students, other institutes attendees included. The following senior management of the university also attended the programme :

- Prof. R.K. Agrawal, Chief Coordinator, CIS
- Prof. Bijoy Kumar Kuanr, Chief Coordinator, USIC
- Prof Manju Khari, Coordinator, USIC
- Shri Sanjeev Kumar, Director, CIS
- Dr. Fauzia Firdous Ozai, I/C, Health Centre
- Shri Naveen Yadav, Chief Security Officer (CSO)
- Technical personnel from various units of the university

From C-DAC Noida**,** Ms. Rekha Saraswat**,** Chief Investigator, Ms Kanti Singh, Project Lead along with other scientists and cyber security experts from CDAC conducted the sessions and facilitated engaging discussions.

Programme Overview

Day 1 Highlights:

- **Data Privacy**: Understanding and safeguarding digital footprints
- **Web Application Security**: Techniques to secure web-based platforms
- **Social Media Crimes & Safety**: Preventive measures and legal awareness
- **Mobile Security**: Identifying and countering mobile-specific threats

Day 2 Highlights:

- **Cyber Hygiene**: Practices to protect digital identity
- **Cyber Scams & Financial Frauds**: Trends, cases, and counter-strategies
- **Data Protection**: Essentials for protecting digital assets
- **Safe Browsing**: Fundamental principles for secure internet use

Outcomes & Feedback

The sessions were highly interactive, featuring in-depth discussions on real-world scenarios, case studies, and preventive strategies. The participants found the content extremely relevant and timely in the context of the growing dependence on digital technologies. The certificates of participation were distributed at the end of the programme. Feedback collected from attendees indicated a high level of satisfaction with the content, delivery, and relevance of the training sessions.

Conclusion

The training programme successfully met its objective of spreading awareness and enhancing the cyber security preparedness of the university community. The overwhelming response and active engagement of participants underscored the critical importance of such initiatives in today's digital age. The university looks forward to hosting more such awareness and capacity-building programmes in the future. The following are glimpse of the training session.

Communication & Information Services (CIS), and University Science Instrumentation Center (USIC),
Jawaharlal Nehru University (JNU)
_____