For the Students of the college - Apply Now

Add-On Course:Cyber Security and Safe Internet Practices

Course Code: ADC-

Department of Computer Science and IQAC, St.Xavier's College (Autonomous)
Ranchi

Commencement of Classes-From: Aug 2026 (Tentative)

Semester: I, III, V and VII
Duration: 30 classes (Theory) + 10 classes (Practical)
No. of Seats: 50
Course Eligibility: UG/PG (Open to students from all disciplines including Arts, Commerce, Science, Management, Law, Humanities, Social Sciences, and other professional courses)
Level: Foundation Level (No Prior Technical Knowledge Required)
Course Fee: ₹1500/- (Including admission application form fee)
Timing: 2:10 PM (Flexible) *(Course completion duration –03–04 months)*
Course Coordinator: Dr. Kamaldeep, Department of Computer Science, SXC
Course Registration: Through College Website – **www.sxcran.ac.in**

About the Course

With the increasing use of smartphones, social media, digital payments, and online services, cyber security awareness has become essential for everyone. This course introduces the fundamentals of cyber security, safe internet practices, common cyber threats, digital payment security, responsible social media usage, and cyber law awareness. Students will also learn about digital privacy, online ethics, and their rights and responsibilities in the digital world, enabling them to use technology safely, securely, and responsibly in their personal, academic, and professional lives.

Course Outcomes (COs)

After successful completion of the course, the students will be able to:

CO Code	Course Outcome
CO1	Explain the fundamental concepts of cyber security, cyber threats, vulnerabilities, and common cyber attacks.
CO2	Apply safe internet practices to protect digital devices, online accounts, and personal information.
CO3	Identify common cyber threats, online frauds, digital payment scams, and adopt appropriate preventive measures.
CO4	Demonstrate responsible digital citizenship by following ethical online behaviour, protecting privacy, and using digital technologies responsibly.
CO5	Understand basic cyber laws, digital rights, and cyber crime reporting mechanisms for safe and responsible use of digital technologies.

Program Outcomes (POs)

On successful completion of the course, the learners will be able to:

PO Code	Program Outcome
PO1	Develop digital literacy and cyber security awareness for safe use of digital technologies.
PO2	Apply critical thinking to identify and respond to cyber threats and online risks.
PO3	Demonstrate ethical, responsible, and secure behaviour while using digital platforms and social media.
PO4	Understand legal, privacy, and societal aspects related to cyber security and digital communication.
PO5	Promote lifelong learning by adopting safe digital practices and keeping pace with emerging cyber security challenges.

Learning Outcomes

After successful completion of the course, students will be able to:

1. **Understand** the fundamentals of cyber security and common cyber threats.
2. **Apply** safe internet practices to protect digital devices, personal information, and online accounts.
3. **Identify** online frauds, phishing attacks, cyber scams, and adopt appropriate preventive measures.
4. **Demonstrate** responsible digital citizenship by following ethical online behaviour and protecting privacy.
5. **Recognize** basic cyber laws, digital rights, and cyber crime reporting mechanisms for safe and responsible use of digital technologies.

Course Contents: Cyber Security and Safe Internet Practices (30 +10 Classes)

Unit	Unit Title	Course Contents	Learning Outcome	Classes
I	**Fundamentals of Cyber Security**	Introduction to Cyber Security, Information Security, Cyberspace, CIA Triad (Confidentiality, Integrity and Availability), Cyber Threats and Vulnerabilities, Types of Hackers, Common Cyber Attacks, Cyber Hygiene, Importance of Cyber Security.	**LO1:** Explain the basic concepts of cyber security, information security, cyber threats, vulnerabilities, and common cyber attacks.	6
II	**Safe Internet Practices**	Safe Web Browsing, Browser Security, Email Security, Password Security, Password Managers, Multi-Factor Authentication (MFA), Mobile Device Security, Public Wi-Fi Security, Software Updates and Patch Management, Cloud Storage Security, Data Backup and Recovery, Digital Footprints, Online Privacy.	**LO2:** Apply safe internet practices to secure digital devices, online accounts, personal information, and online communications.	6
III	**Cyber Threats and Online Frauds**	Malware (Virus, Worm, Trojan Horse, Spyware, Ransomware), Phishing, Spear Phishing, Smishing, Vishing, Social Engineering, Identity Theft, Fake Websites, QR Code Scams, UPI Frauds, Online Banking Security, Online Shopping Frauds, Fake Job and Investment Scams, Matrimonial Frauds, Cyber	**LO3:** Identify common cyber threats, online frauds, phishing attacks, malware, and digital payment scams, and recommend	6

		Bullying, Cyber Stalking, Preventive Measures.	appropriate preventive measures.	
IV	**Digital Citizenship and Responsible Technology Use**	Digital Citizenship, Digital Ethics, Responsible Internet Usage, Responsible Social Media Usage, Safe Use of Artificial Intelligence (AI) Tools, Deepfake Images and Videos, Fake News and Misinformation, Copyright, Plagiarism, Intellectual Property Rights, Digital Wellness, Emerging Trends in Cyber Security.	**LO4:** Demonstrate responsible digital citizenship by following ethical online behaviour, respecting intellectual property, protecting privacy, and using AI and social media responsibly.	6
V	**Cyber Laws and Digital Rights Awareness**	Introduction to Cyber Laws, Information Technology (IT) Act, 2000 (Overview), Digital Rights and Responsibilities, Privacy and Consent, Responsible Photography and Videography, Recording Videos in Public Places, Sharing Photos and Videos on Social Media, Identity Theft (Section 66C), Online Cheating (Section 66D), Violation of Privacy (Section 66E), Obscene Content (Sections 67 & 67A), Cyber Crime Reporting Portal, Cyber Crime Helpline (1930).	**LO5:** Understand basic cyber laws, digital rights and responsibilities, privacy and consent, and appropriate procedures for reporting cyber crimes.	6

Laboratory Exercises (10 classes)

S.No.	Practical Exercise
1	Configure browser, email, and smartphone security settings, including password management and Multi-Factor Authentication (MFA).
2	Identify phishing emails, fake websites, malicious links, QR code scams, and other common online frauds using real-life examples.
3	Configure privacy and security settings on social media platforms and demonstrate safe digital payment practices (UPI, online banking, QR code verification).
4	Analyze real-life cyber security case studies involving cyberbullying, identity theft, online shopping fraud, fake job scams, and discuss preventive measures.
5	Explore the National Cyber Crime Reporting Portal and Cyber Crime Helpline (1930), prepare a cyber awareness poster/presentation, and demonstrate the procedure for reporting cyber incidents.

24/07/26

Course Coordinator
Dr. Kamaldeep

Dept. of Computer Science St. Xavier's College Ranchi

24/7/26

Head of the Department
Dr. Swarat Chaudhuri

Dept. of Computer Science St. Xavier's College Ranchi

24/7/26

Registrar
Dr. Fr. Prabhat Kennedy Soreng, S.J

REGISTRAR
ST. XAVIER'S COLLEGE
RANCHI