

AC – 20/05/2025
Item No. – 6.18 (N) (2a) Sem. III

As Per NEP 2020

University of Mumbai



Syllabus for Basket of OE	
Faculty of Science	
Board of Studies in Computer Science	
UG Second Year Programme	
Semester	III
Title of Paper	Credits 2
I) Cyber & Digital Safety	2
From the Academic Year	2025 – 2026

Name of the Course: Cyber & Digital Safety

Sr. No.	Heading	Particulars
1	Description the course:	Introduction: With the rapid rise in digital connectivity, individuals are increasingly vulnerable to online threats. This course introduces students to essential concepts of digital safety, privacy, and responsible online behavior. It provides practical knowledge to protect personal data, secure digital devices, and navigate the internet safely. Relevance: In today's digital age, everyone is a digital citizen. Whether you're a student, professional, or homemaker, digital safety is vital for safeguarding identity, finances, and mental well-being. This course addresses the urgent need to educate individuals in navigating online spaces securely. Usefulness: The course empowers learners with practical knowledge on how to stay safe online—be it managing privacy settings on social media, identifying phishing emails, or using strong passwords. These skills are useful in daily digital activities across personal, academic, and professional spaces. Application: Students can immediately apply the concepts learned—from using secure Wi-Fi and avoiding fake news to setting up two-factor authentication and protecting children's online experiences. It also helps in developing a safety-first approach to technology use. Interest: This course connects to the everyday digital life of learners—making it highly relatable. It explores topics like deepfakes, social media responsibility, digital detox, and cyberbullying, which resonate with students from all disciplines and age groups. Connection with Other Courses: While not technical, this course complements subjects in Media Studies, Psychology, Communication, Law, and even Business. It strengthens digital literacy, a valuable

		soft skill, and supports courses related to digital ethics, digital marketing, and online communication. Demand in the Industry: Digital awareness is considered a critical life skill by employers. Companies value employees who understand safe digital practices, especially in remote and hybrid work environments. With increasing data breaches and cybercrime, demand for digitally responsible professionals is rising. Job Prospects: Although not a technical specialization, this course adds weight to any resume by demonstrating digital literacy. It prepares students for roles in education, administration, customer service, journalism, HR, and more—where safe technology use is expected and respected.
2	Vertical:	Open Elective
3	Type:	Theory
4	Credits:	2 credits
5	Hours Allotted:	30 hours
6	Marks Allotted:	50 Marks
7	Course Objectives (CO): CO 1. To introduce the foundational concepts of cyber safety and digital privacy. CO 2. To create awareness of common online threats and best practices for digital hygiene. CO 3. To equip students with skills for safe usage of social media, devices, and the internet. CO 4. To develop a mindset for ethical digital behavior and responsible technology use. CO 5. To explore emerging cyber risks including AI, deepfakes, and the role of legislation.	
8	Course Outcomes (OC): After successful completion of this course, students would be able to - OC 1. Understand key concepts in cyber security and differentiate between threats and risks. OC 2. Apply safe browsing practices and protect their digital identity across platforms. OC 3. Identify and avoid common cyber scams, phishing attacks, and fake news. OC 4. Safeguard personal devices, use secure communication tools, and manage passwords.	

	OC 5. Understand the ethical concerns and emerging trends in AI-driven cyber threats.
9	Modules: Module 1: Fundamentals of Digital Safety & Online Behavior Introduction to Digital Safety and Cyber Security: What is Digital Safety?, Everyday importance of staying safe online, Cyber Security vs. Digital Safety, Ethical and responsible use of technology Common Online Threats and How to Avoid Them: Types of online threats: viruses, phishing, scams, Understanding social engineering and digital fraud, Case examples of real-world cyber attacks Safe Internet and Social Media Use: How to browse safely: HTTPS, safe websites, online shopping tips, Social media privacy settings, Digital identity and managing your online presence, Deepfakes and misinformation, Screen time, mental health, and digital well-being Online Safety for Children and Teenagers: Common risks for young users, Using parental controls and safe browsing tools, Identifying and addressing cyberbullying, Teaching children responsible internet use Module 2: Personal Device Security, Privacy & Emerging Trends Securing Devices and Networks: How to keep your phone and laptop safe, Safe use of public Wi-Fi and VPNs, Protecting smart devices (IoT) at home, Backing up your data securely Building Good Digital Habits (Cyber Hygiene): Creating strong passwords and using multi-factor authentication, Keeping software updated and avoiding unsafe downloads, Spotting fake news and online hoaxes Understanding Data Privacy: What is personal data and why it matters, Data protection laws in simple terms (like GDPR), Using privacy-friendly tools (browsers, search engines, messaging apps), What to do if a data breach happens Cyber Safety at Work and Emerging Technologies: Staying safe while working online or remotely, Secure email and workplace communication, How AI is used in cyber security – the good and the bad, Deepfakes, AI-based scams, and how to stay alert, Introduction to how blockchain can help in digital security
10	Text Books 1. Security in the Cyber Age: An Introduction to Policy and Technology, John E. Savage, Derek S. Reveron, Cambridge University Press, 2023 2. Cyber Security and Personal Data Awareness: Leverage Personal Data safety in Cyber Threat environment, Selvaraj G, Notion Pres, 2024 3. Cyber and Digital Safety: Fundamentals and Best Practices, Maurya R K, SYBGEN Learning, 2025
11	Reference Books 1. Cyber Safety for Everyone: A comprehensive guide to online safety,

	JaagoTeens, BPB Publications, 3rd Edition, 2024		
	2. The Basics of Cyber Safety: Computer and Mobile Device Safety, John Sammons (Author), Michael Cross MD, Syngress, 2016		
	3. Cybersecurity for Everyone, David B. Skillicorn, Routledge, CRC Press, 2022		
	4. Cybersecurity for Dummies, Joseph Steinberg, Wiley, 2020		
12	Internal Continuous Assessment: 40%	Semester End Examination: 60%	
13	Continuous Evaluation through: Class Test on Module 1: 10 marks Class Test on Module 2: 10 marks	Evaluation through: A Semester End Theory Examination of 1 hour duration for 30 marks as per the paper pattern given below. Total: 30 marks	
	Average of 2 Class Tests: 10 marks Assignment on Module 1: 5 marks Assignment on Module 2: 5 marks		
	Total of 2 Assignments: 10 marks		
	Total: 20 marks		
14	Format of Question Paper:		
	Total Marks: 30		
	Duration: 1 Hour		
	Question	Based On	Options
	Q. 1	Module 1	Any 2 out of 4
Q. 2	Module 2	Any 2 out of 4	
Q. 3	Module 1 & 2	Any 2 out of 4	
		Marks	
		10	
		10	
		10	