Rajarshi Shahu Mahavidyalaya, Latur

(Autonomous)

Department of Computer Science

Course Type: SEC - II

Course Title: Cyber Security

Course Code:

Credits: 2 **Marks: 50** **Lectures: 30 Hrs.**

Learning Objectives:

LO 1. To Understand importance of cyber security in daily life and cooperative world.

LO 2. To learn and understand Cyber Crime and Cyber Law.

LO 3. To understand the Social Media security issues.

LO 4. To understand digital devices security, and learn the tools and technologies for cyber security.

Course Outcomes:

After completion of course the student will be able to-

CO 1. **U**nderstand the concept of Cyber security and issues and challenges associated with it.

CO 2. Identify the cyber-crimes, their nature, legal remedies and as to how report the crimes through available platforms and procedures.

CO 3. Describe various digital payment modes and related cyber security aspects, RBI guidelines and preventive measures against digital payment frauds.

CO 4. Implement the basic security aspects related to Computer and Mobiles.

CO 5. Use tools and technologies to protect their devices.

Unit No.	Title of Unit & Contents	Hrs.
I	**Introduction to Cyber security, Cyber Crime and Cyber Law**	**6**
	Defining Cyberspace and Overview of Computer and Web-technology, 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, Concept of cyber security, Issues and challenges of cyber security. Classification of cyber-crimes, Common cyber-crimes, cyber-crime targeting computers and mobiles, cyber-crime against women and children, financial frauds, social engineering attacks, malware and ransomware attacks, zero day and zero click attacks, Cybercriminals	

Unit No.	Title of Unit & Contents	Hrs.
	modus-operandi, reporting of cybercrimes, Remedial and mitigation measures, Legal perspective of cybercrime, IT Act 2000 and its amendments, Cyber-crime and offences, Organizations dealing with Cyber-crime and Cyber security in India	
	UO 1. to understand the concept of Cyber security and issues and challenges associated with it. UO 2. to understand the cyber-crimes, their nature, legal remedies and as to how report the crimes through available platforms and procedures.	
II	Social Media Security, E- Commerce and Digital Payments	**6**
	Introduction and types of Social media, Social media platforms, Social media monitoring, Hashtag, Viral content, Social media marketing, Social media privacy, Challenges, opportunities and pitfalls in online social network, Security issues related to social media, Laws regarding posting of inappropriate content, Best practices for the use of Social media. Introduction to E-Commerce, E-Commerce threats, E-Commerce security best practices, Introduction to digital payments, Components of digital payment and stake holders, Modes of digital payments- Banking Cards, Unified Payment Interface (UPI), e-Wallets, Unstructured Supplementary Service Data (USSD), Aadhar enabled payments, Digital payments related common frauds and preventive measures. RBI guidelines on digital payments and customer protection in unauthorized banking transactions. Relevant provisions of Payment Settlement Act,2007	
	UO 1. To appreciate various privacy and security concerns on online Social media and understand the reporting procedure of inappropriate content, underlying legal aspects and best practices for the use of Social media platforms. UO 2. Become familiar with various digital payment modes and related cyber security aspects, RBI guidelines and preventive measures against digital payment frauds	
III	Digital Devices SecurityTools and Technologies for Cyber Security	**8**
	End Point device and Mobile phone security, Password policy, Security patch management, Data backup, Downloading and management of third party software, Device security policy, Cyber Security best practices, Significance of host firewall and Ant-virus, Management of host firewall and Anti-virus, Wi-Fi security, Configuration of basic security policy and permissions.	
	UO 1. To understand the basic security aspects related to Computer and Mobiles. UO 2. To use basic tools and technologies to protect their devices.	
	Practical	**10**
	1. Online Reporting phishing emails and Demonstration of email phishing attack and preventive measures 2. Basic checklist, privacy and security settings for popular Social media platforms.	

Unit No.	Title of Unit & Contents	Hrs.
	3. Reporting and redressal mechanism for violations and misuse of social media platforms. 4. Configuring security settings in Mobile Wallets and UPIs. 5. Checklist for secure net banking and Setting, configuring and managing three password policy in the computer. 6. Setting and configuring two factor authentication in the Mobile Phones. 7. Managing Application permissions in Mobile phone. 8. Installation and configuration of computer Anti-virus. 9. Installation and configuration of Computer Host Firewall. 10. Wi-Fi security management in computer and mobile.	

Learning Resources:

1. Cyber Crime Impact in the New Millennium, by R. C Mishra , Auther Press. Edition 2010.
2. Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives by Sumit Belapure and Nina Godbole, Wiley India Pvt. Ltd. (First Edition, 2011)
3. Security in the Digital Age: Social Media Security Threats and Vulnerabilities by Henry A. Oliver, Create Space Independent Publishing Platform. (Pearson , 13th November, 2001)
4. Electronic Commerce by Elias M. Awad, Prentice Hall of India Pvt Ltd.
5. Cyber Laws: Intellectual Property & E-Commerce Security by Kumar K, Dominant Publishers.
6. Network Security Bible, Eric Cole, Ronald Krutz, James W. Conley, 2nd Edition, Wiley India Pvt. Ltd.
7. Fundamentals of Network Security by E. Maiwald, McGraw Hill.