

23CS32E2 –CYBER SECURITY

Course Category:	Professional Elective - II	Credits:	3
Course Type:	Theory	Lecture-Tutorial-Practical:	3-0-0
Prerequisite:	<ul style="list-style-type: none"> Knowledge in Cyber Security 	Sessional Evaluation: 30 Univ. Exam Evaluation: 70 Total Marks: 100	
Course Objectives:	Students undergoing this course are expected:		
	<ul style="list-style-type: none"> The course is designed to provide awareness on different cyber crimes, cyber offenses, tools and methods used in cybercrime. To familiarize various types of cyber-attacks and cyber-crimes. To give an overview of the cyber laws. To study the defensive techniques against these attacks 		

Course Outcomes:	Upon successful completion of the course, the students will be able to:	
	CO1	Classify the cybercrimes and understand the Indian ITA 2000.
	CO2	Analyse the vulnerabilities in any computing system and find the solutions
	CO3	Predict the security threats of the future....
	CO4	Investigate the protection mechanisms
	CO5	Design security solutions for organizations.
Course Content:	<u>UNIT-I</u> Introduction to Cyber crime: Introduction, Cybercrime, and Information Security, Who are Cybercriminals, Classifications of Cybercrimes, And Cybercrime: The legal Perspectives and Indian Perspective, Cybercrime and the Indian ITA 2000, A Global Perspective on Cybercrimes.	
	<u>UNIT-II</u> Cyber Offenses: How Criminals Plan Them: Introduction, How Criminals plan the Attacks, Social Engineering, Cyber stalking, Cyber cafe and Cybercrimes, Botnets: The Fuel for Cybercrime, Attack Vector, Cloud Computing	
	<u>UNIT-III</u> Cyber crime: Mobile and Wireless Devices: Introduction, Proliferation of Mobile and Wireless Devices, Trends in Mobility, Credit card Frauds in Mobile and Wireless Computing Era, Security Challenges Posed by Mobile Devices, Registry Settings for Mobile Devices, Authentication service Security, Attacks on Mobile/Cell Phones.	
	Mobile Devices: Security Implications for Organizations, Organizational Measures for Handling Mobile, Organizational Security Policies an Measures in Mobile Computing Era, Laptops.	
	<u>UNIT-IV</u> Tools and Methods Used in Cyber crime: Introduction, Proxy Servers and Anonymizers, Phishing, Password Cracking, Key loggers and Spywares, Virus and Worms, Trojan Horse and Backdoors, Steganography, DoS and DDoS attacks, SQL Injection, Buffer Overflow	
	<u>UNIT-V</u> Cyber Security: Organizational Implications: Introduction, Cost of Cybercrimes and IPR issues, Web threats for Organizations, Security and Privacy Implications, Social media	

	marketing: Security Risks and Perils for Organizations, Social Computing and the associated challenges for Organizations.
Text Books & References Books:	<p>TEXTBOOKS:</p> <ol style="list-style-type: none"> 1. Cyber Security: Under standing Cyber Crimes, Computer Forensics and Legal Perspectives, Nina Godbole and Sunil Belapure, Wiley INDIA <p>REFERENCE BOOKS:</p> <ol style="list-style-type: none"> 1. Cyber Security Essentials, James Graham, Richard Howard and Ryan Otson, CRC Press. 2. Introduction to Cyber Security , Chwan –Hwa (john) Wu ,J. DavidIrwin.CRC Press T&F Group
E-Resources:	<ol style="list-style-type: none"> 1. http://nptel.ac.in/courses/106105031/40 2. http://nptel.ac.in/courses/106105031/39 3. http://nptel.ac.in/courses/106105031/38