

Cyber Security

Course Code	20CS4702C	Year	IV	Semester	I
Course Category	Elective	Branch	CSE	Course Type	Theory
Credits	3	L-T-P	3-0-0	Prerequisites	Cryptography and Information Security
Continuous Internal Evaluation :	30	Semester End Evaluation:	70	Total Marks:	100

Course Outcomes		Blooms Level
Upon successful completion of the course, the student will be able to:		
CO1	Understand the basic concepts of cybercrime and offences	L2
CO2	Apply various methods and tools to identify various cyber crimes	L3
CO3	Apply different security measures on mobile devices	L3
CO4	Analyze the cyber security requirements/measures for an IT Infrastructure	L4

Contribution of Course Outcomes towards achievement of Program Outcomes & Strength of correlations														
	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2
CO1	√													
CO2						√	√		√	√				√
CO3						√	√	√						√
CO4						√	√	√						√

Syllabus		Mapped CO
Unit No.	Contents	
I	Introduction to Cybercrime: Introduction, Cybercrime, and Information Security, Who are Cybercriminals, Classifications of Cybercrimes.	CO1
II	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, and Cloud Computing.	CO1, CO2
III	Cybercrime: 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, MobileDevices: Security Implications for Organizations, Organizational Measures for Handling Mobile, Organizational Security Policies and Measures in Mobile Computing Era, Laptops.	CO1,CO2,CO3
IV	Tools and Methods Used in Cybercrime: Introduction, Proxy Servers and Anonymizers, Phishing, Password Cracking, Keyloggers and Spywares, Virus and Worms, Trojan Horse and Backdoors, Steganography, DoS and DDoS attacks, SQL Injection, Buffer Overflow.	CO1, CO2, CO3

V	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.	CO1, CO4
----------	--	-----------------

Learning Resources	
Text Books	
1. Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives, Nina Godbole and Sunil Belapure, First edition, Wiley INDIA,2011.	
References	
1. James Graham, Richard Howard and Ryan Otson, Cyber Security Essentials, First edition, CRC Press,2011.	
2. Chwan-Hwa(John) Wu,J.David Irwin, Introduction to Cyber Security, First edition, CRC Press T&F Group,2013.	
e-Resources & other digital material	
1. https://www.coursera.org/learn/intro-cyber-attacks?specialization=intro-cyber-security .	
2. https://www.coursera.org/learn/introduction-cybersecurity-cyber-attacks?specialization=it-fundamentals-cybersecurity .	
3. https://www.coursera.org/learn/cybersecurity-for-everyone .	