20CS4702C –CYBER SECURITY

SYLLABUS

Offering Branches	CSE		
Course Category:	Professional Elective	**Credits:**	3
Course Type:	Theory	**Lecture-Tutorial-Practical:**	3-0-0
Prerequisites:	Computer Networks, Operating Systems	**Continuous Evaluation:**	30
		Semester End Evaluation:	70
		Total Marks:	100
Course Outcomes			
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	
Course Content			
UNIT-1	**Introduction to Cybercrime:** Introduction, Cybercrime, and Information Security, Who are Cybercriminals, Classifications of Cybercrimes.	**CO1**	
UNIT-2	**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**	
UNIT-3	**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, Organizational Measures for Handling Mobile, Organizational Security Policies an Measures in Mobile Computing Era, Laptops.	**CO1,CO2,CO3**	
UNIT-4	**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**	
UNIT-5	**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, 2011, Wiley INDIA.
Reference Books	1. James Graham, Richard Howard and Ryan Otson, Cyber Security Essentials, First edition, 2011, CRC Press. 2. Chwan-Hwa(John) Wu,J.David Irwin, Introduction to Cyber Security, First edition, 2013, CRC Press T&F Group.
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 4. https://github.com/WebGoat/WebGoat 5. https://owasp.org/www-project-webgoat/#:~:text=WebGoat%20is%20a%20deliberately%20insecure,and%20popular%20open%20source%20components.

CSE: 1) 2) 3)

Module Coordinator:

HOD, CSE

MICRO SYLLABUS

20CS4702C –CYBER SECURITY

Offering Branches	CSE		
Course Category:	Professional Elective	**Credits:**	3
Course Type:	Theory	**Lecture-Tutorial-Practical:**	3-0-0
Prerequisites:	Computer Networks, Operating Systems	**Continuous Evaluation:**	30
		Semester End Evaluation:	70
		Total Marks:	100

Course Outcomes		
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

	Course Content	
UNIT-1	**Introduction to Cyber Crime (CHAPTER 1 of Textbook - 1.1 to 1.5)** Introduction Cybercrime: Definition and Origins of the Word Cybercrime and Information Security Who are Cybercriminals? Classifications of Cybercrimes • E-Mail Spoofing • Spamming • Cyber defamation • Internet Time Theft • Salami Attack/Salami Technique • Data Diddling • Forgery • Web Jacking • Newsgroup Spam/Crimes Emanating from Usenet Newsgroup • Industrial Spying/Industrial Espionage • Hacking • Online Frauds • Pornographic Offenses • Software Piracy • Computer Sabotage • E-Mail Bombing/Mail Bombs	**CO1**

	• Usenet Newsgroup as the Source of Cybercrimes • Computer Network Intrusions • Password Sniffing • Credit Card Frauds • Identity Theft	
UNIT-2	**Cyberoffenses: How Criminals Plan Them (CHAPTER 2 of Textbook)** Introduction • Categories of Cybercrime How Criminals Plan the Attacks • Reconnaissance • Passive Attacks • Active Attacks • Scanning and Scrutinizing Gathered Information • Attack (Gaining and Maintaining the System Access) Social Engineering • Classification of Social Engineering Cyber stalking • Types of Stalkers • Cases Reported on Cyber stalking • How Stalking Works? • Real-Life Incident of Cyber stalking Cybercafé and Cybercrimes Botnets: The Fuel for Cybercrime • Botnet Attack Vector Cloud Computing • Why Cloud Computing? • Types of Services • Cybercrime and Cloud Computing	**CO1,CO2**
UNIT-3	**Cybercrime: Mobile and Wireless Devices (CHAPTER 3 of Textbook)** Introduction Proliferation of Mobile and Wireless Devices Trends in Mobility Credit Card Frauds in Mobile and Wireless Computing Era • Types and Techniques of Credit Card Frauds Security Challenges Posed by Mobile Devices Registry Settings for Mobile Devices Authentication Service Security • Cryptographic Security for Mobile Devices • LDAP Security for Hand-Held Mobile Computing Devices • RAS Security for Mobile Devices • Media Player Control Security • Networking API Security for Mobile Computing Applications Attacks on Mobile/Cell Phones	**CO1,CO2,CO3**

	• Mobile Phone Theft • Mobile Viruses • Mishing • Vishing • Smishing • Hacking Bluetooth Mobile Devices: Security Implications for Organizations • Managing Diversity and Proliferation of Hand-Held Devices • Unconventional/Stealth Storage Devices • Threats trough Lost and Stolen Devices • Protecting Data on Lost Devices • Educating the Laptop Users Organizational Measures for Handling Mobile Devices-Related Security Issues • Encrypting Organizational Databases • Including Mobile Devices in Security Strategy Organizational Security Policies and Measures in Mobile Computing Era • Importance of Security Policies relating to Mobile Computing Devices • Operating Guidelines for Implementing Mobile Device Security Policies • Organizational Policies for the Use of Mobile Hand-Held Devices Laptops • Physical Security Countermeasures	
UNIT-4	**Tools and Methods Used in Cybercrime (CHAPTER 4 of Textbook – 4.1 to 4.11)** Introduction Proxy Servers and Anonymizers Phishing • How Phishing Works? Password Cracking • Online Attacks • Offline Attacks • Strong, Weak and Random Passwords • Random Passwords Key loggers and Spywares • Software Key loggers • Hardware Key loggers • Antikeylogger • Spywares Virus and Worms • Types of Viruses Trojan Horses and Backdoors • Backdoor • How to Protect from Trojan Horses and Backdoors Steganography	**CO1,CO2,CO3**

	• Steganalysis DoS and DDoS Attacks • DoS Attacks • Classification of DoS Attacks • Types or Levels of DoS Attacks • Tools Used to Launch DoS Attack • DDoS Attacks • How to Protect from DoS/DDoS Attacks SQL Injection • Steps for SQL Injection Attack • How to Prevent SQL Injection Attacks Buffer Overflow • Types of Buffer Overflow • How to Minimize Buffer Overflow Attacks on Wireless Networks • Traditional Techniques of Attacks on Wireless Networks • Theft of Internet Hours and Wi-Fi-based Frauds and Misuses • How to Secure the Wireless Networks	
UNIT-5	**Cyber security: Organizational Implications (CHAPTER 9 of Textbook – 9.1 to 9.6)** Introduction • Insider Attack Example 1: Heartland Payment System Fraud • Insider Attack Example 2: Blue Shield Blue Cross (BCBS) Cost of Cybercrimes and IPR Issues: Lessons for Organizations • Organizations have Internal Costs Associated with Cyber security Incidents • Organizational Implications of Software Piracy Web Threats for Organizations: The Evils and Perils • Overview of Web Threats to Organizations Security and Privacy Implications from Cloud Computing Social Media Marketing: Security Risks and Perils for Organizations • Understanding Social Media Marketing • Best Practices with Use of Social Marketing Tools Social Computing and the Associated Challenges for Organizations	**CO1,CO4**
	Learning Resources	
Text Books	Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives, Nina Godbole and Sunil Belapure, First edition, 2011, Wiley INDIA.	

CSE: 1) 2) 3)

Module Coordinator:

HOD, CSE