Course Code:	**Subject Title: Cyber Security**
	Year and Semester: IV Year I Semester

Course Objectives:
1. To understand various types of cyber-attacks and cyber-crimes
2. To learn threats and risks within context of the cyber security
3. To have an overview of the cyber laws & concepts of cyber forensics
4. To study the defensive techniques against these attacks.
5. To Analyze the Cyber Security needs of the Organizations.

Course Outcomes:
CO 1. Analyze and evaluate the cyber security needs of an organization.
CO 2. Understand Cyber Security Regulations and Roles of International Law.
CO 3. Design and develop a security architecture for an organization.
CO 4. Understand fundamental concepts of data privacy attacks
CO 5. Analyze the cyber security needs of an organization.

[12 hrs]

UNIT-I: Introduction of Cybercrime: Definition and Origins of the Word, Cybercrime and Information Security, Who are Cybercriminals? Classifications of Cybercrimes: Email Spoofing, Spamming, Internet Time Theft, Salami Attack/Salami Technique, Data Diddling, Forgery, Web Jacking, Newgroup Spam, Industrial Espionage, Hacking, Online Frauds, Pornographic offenses, Software Piracy, Computer Sabotage, E-Mail bombing, computer network intrusions, password sniffing, credit card frauds, identity theft, Cybercrime Era: Survival mantra for the Netizens.

[10 hrs]

UNIT-II: Cyber offenses: Criminals Plan: Categories of Cybercrime, Cyber Attacks: Reconnaissance, Passive Attack, Active Attacks, Scanning/Scrutinizing gathered Information, Attack, Social Engineering: Classification of Social Engineering, Cyberstalking: Types of Stalkers, Working of Stalking, Real-Life Incident of Cyber stalking, Cybercafe and Cybercrimes, Botnets: The Fuel for Cybercrime, Botnet, Attack Vector: Theft, viruses, mishing, vishing, smishing, hacking Bluetooth, Cybercrime and cloud computing.

[12 hrs]

UNIT-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, Mobile Devices: Security Implications for Organizations, Organizational Measures for Handling Mobile, Organizational Security Policies and Measures in Mobile Computing Era, Laptops.

[10 hrs]

UNIT-IV: Tools and Methods Used in Cybercrime: Introduction, Proxy Servers and Anonymizers, Phishing, Password Cracking, Key loggers and Spywares, Virus and Worms, Trojan Horses and Backdoors, Steganography, DoS and DDoS Attacks, SQL Injection, Buffer Overflow, Attacks on Wireless Networks.

[10 hrs]

UNIT-V: Cybercrimes and Cyber security: Organizational Implications–Introduction–Insider threats, Privacy, Key challenges to organizations, Cost of Cybercrimes and IPR issues, Incident Handling: Definitions, Why Organizations need Incident Response systems, Examples of incidents, what organizations can do to protect, best practices for organizations.

TEXT BOOKS: 1. Cyber Security: Understanding Cyber Crimes, Computer Forensics and Legal Perspectives, Nina Godbole, SunitBelapure, Wiley India Publications.

REFERENCES: [1] James Graham, R Howard, R Olson, "Cyber Security Essentials" CRC Press, 2018 [2] Michael E Whitman, Herbert J Mattord, "Principles of Information Security", 4th Edition, Cengage Learning, 2012 [3] William Stallings, “Cryptography and Network Security- Principles and Practice”, 7th Edition, Pearson Education, 2017

E-RESOURCES AND OTHER DIGITAL MATERIAL

[1] MITOPENCOURSEWARE Computer Systems Security https://ocw.mit.edu/courses/6-858-computer-systems-security-fall- 2014/video_galleries/videolectures/ [2] Oxford Home Study Center, Cyber Security short course available@ https://www.oxfordhomestudy.com/courses/cyber-security-courses/free-cyber-security-online

Micro Syllabus of Cyber Security

UNIT - I: Introduction of Cybercrime: Definition and Origins of the Word, Cybercrime and Information Security, who are Cybercriminals? Classifications of Cybercrimes: Email Spoofing, Spamming, Internet Time Theft, Salami Attack/Salami Technique, Data Diddling, Forgery, Web Jacking, Newgroup Spam, Industrial Espionage, Hacking, Online Frauds, Pornographic offenses, Software Piracy, Computer Sabotage, E-Mail bombing, computer network intrusions, password sniffing, credit card frauds, identity theft, Cybercrime Era: Survival mantra for the Netizens.

Unit	Module	Micro Content
UNIT-I	**Introduction of Cybercrime**	Cybercrime: Definition and Origins of the Word
		Cybercrime and Information Security
		Who are Cybercriminals?
		Classifications of Cybercrimes: Email Spoofing, Spamming
		Internet Time Theft, Salami Attack/Salami Technique
		Data Diddling, Forgery, Web Jacking
		Newgroup Spam, Industrial Espionage, Hacking
		Online Frauds, Pornographic offenses, Software Piracy
		Computer Sabotage, E-Mail bombing
		Computer network intrusions, Password sniffing
		Credit card frauds, Identity theft
		Cybercrime Era: Survival mantra for the Netizens

UNIT – II: Cyber offenses: How Criminals Plan Them: Categories of Cybercrime,
Cyber Attacks: Reconnaissance, Passive Attack, Active Attacks, Scanning/Scrutinizing

gathered Information, Attack, Social Engineering: Classification of Social Engineering, Cyberstalking: Types of Stalkers, Working of Stalking, Real-Life Incident of Cyber stalking, Cybercafe and Cybercrimes, Botnets: The Fuel for Cybercrime, Botnet, Attack Vector: Theft, viruses, mishing, vishing, smishing, hacking Bluetooth, Cybercrime and cloud computing.

Unit	Module	Micro Content
UNIT-III	**Cybercrime: Mobile and Wireless Devices**	Categories of Cybercrime
		How criminals plan the attacks: Reconnaissance, Passive Attack
		Active Attacks, Scanning/Scrutinizing gathered Information
		Attack (Gaining & Maintaining the System Access)
		Social Engineering: Classification of Social Engineering
		Cyberstalking: Types of Stalkers, Working of Stalking
		Real-Life Incident of Cyber stalking
		Cybercafe and Cybercrimes
		Botnets: The Fuel for Cybercrime
		Botnet
		Attack Vector
		Cloud computing: Why cloud computing
		Types of Services
		Cybercrime and cloud computing

UNIT – III: Cybercrime: Mobile and Wireless Devices: Introduction, Proliferation of Mobile andWireless 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: SecurityImplications for Organizations, Organizational Measures for Handling Mobile, OrganizationalSecurity Policies and Measures in Mobile Computing Era, Laptops.

Unit	Module	Micro Content
UNIT-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:
		Types and Techniques of Credit Card Frauds
		Security Challenges Posed by Mobile Devices

		Registry Settings for Mobile Devices
		Authentication Service Security:
		Cryptography 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, Mobile Devices:
		Mobile Phone Theft, Mobile Viruses
		Mishing, Vishing, Smishing, Hacking Bluetooth
		Mobile Devices: Security Implications for Organizations: Managing Diversity & Proliferation of Devices
		Unconventional/ Stealth Storage Devices
		Threats through Lost & 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 Measures for Handling 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 Handheld Devices
		Laptops: Physical Security Countermeasures

UNIT – IV: Tools and Methods Used in Cybercrime: Introduction, Proxy Servers and Anonymizers, Phishing, Password Cracking, Key loggers and Spywares, Virus and Worms, Trojan Horses and Backdoors, Steganography, DoS and DDoS Attacks, SQL Injection, Buffer Overflow, Attacks on Wireless Networks.

Unit	**Module**	**Micro Content**
UNIT-IV	**Tools and Method s Used in Cybercrime**	Introduction
		Proxy Servers andAnonymizer
		Phishing: How Phishing Works
		Password Cracking: Online Attacks, Offline Attacks
		Strong, Weak and Random Passwords
		Key loggers and Spywares: Software keyloggers
		Hardware Keyloggers, Anti Keylogger, Spywares
		Virus and Worms: Types of Viruses
		Trojan Horses and Backdoors: Backdoor
		How to Protect them from Trojan Horses and Backdoors
		Steganography: 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 and DDoS Attacks
		SQL Injection: Steps for SQL Injection Attack
		How to prevent SQL Injection Attacks
		BufferOverflow: Types of BufferOverflow
		How to minimize BufferOverflow
		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 - V: Cybercrimes and Cyber security: Organizational Implications–Introduction–Insider threats, Privacy, Key challenges to organizations, Cost of Cybercrimes and IPR issues, Incident Handling: Definitions, Why Organizations need Incident Response systems, Examples of incidents, what organizations can do to protect, best practices for organizations.

Unit	**Module**	**Micro Content**
UNIT-V	**Cybercrimes and Cyber security**	Organizational Implications
		Introduction: Insider threats
		Privacy
		Key challenges to organizations
		Cost of Cybercrimes and IPR issues
		Incident Handling: Definitions
		Why Organizations need Incident Response systems
		Examples of incidents
		What organizations can do to protect
		Best practices for organizations