Uka Tarsadia University

B. Tech.

Semester IV

INTRODUCTION TO CYBER SECURITY
CY4002

EFFECTIVE FROM July-2022

Syllabus version: 1.00

Subject Code	Subject Title	Teaching Scheme			
		Hours		Credits	
		Theory	Practical	Theory	Practical
CY4002	Introduction to Cyber Security	3	2	3	1

Subject Code	Subject Title	Theory Examination Marks		Practical Examination Marks	Total Marks
		Internal	External	CIE	
CY4002	Introduction to Cyber Security	40	60	50	150

Objectives of the course:

- To unfold the fundamentals of cyber security, cybercrimes, and cyber forensics.
- To introduce various security challenges, phishing, and tools and methods used for cybercrime.
- To expose students with legal and ethical perspectives of cyber security and cybercrimes.

Course outcomes:

Upon completion of the course, the student shall be able to,

CO1: Understand the fundamentals of cyber crimes.
CO2: Understand the basics of cyber offenses.
CO3: Understand and illustrate security challenges with mobile and wireless devices.
CO4: Understand and apply tools and methods against cyber crime.
CO5: Understand phishing and ID theft, and demonstrate computer forensics.
CO6: Comprehend legal and ethical perspectives of cyber security and cybercrimes.

Sr. No.	Topics	Hours
	Unit – I	
1	**Introduction to Cyber Crimes:** Cybercrime and Information security, Cyber criminals, Classification of cyber crimes, The legal perspective of cybercrime, Cybercrime on Indian and global perspectives.	6
	Unit – II	

2	**Cyber Offenses:** Introduction to cyber offences, Planning of attacks, Social engineering, Cyber stalking, Botnets, Attack vector, Cyber crime and Cloud computing.	8
Unit – III		
3	**Security Challenges with Mobile and Wireless Devices:** Proliferation of mobile and wireless devices, Trends in mobility, Credit card frauds in mobile and wireless computing era, Security challenges posed by mobile devices, Authentication service security, Attacks of cell phones, Security implications for organization and Organizational measures for handling mobile device related security issues, Organizational security policy and measures in mobile computing era.	8
Unit – IV		
4	**Tools and Methods used in Cybercrime:** Proxy servers and Anonymizers, Phishing, Password cracking, Key loggers and Spywares, Virus and Worms, Trojan horses and Backdoors, Stenography, DoS and DDos attacks, SQL injection, Buffer overflow, Attacks on wireless networks.	6
Unit – V		
5	**Phishing and Identity Theft:** Introduction to phishing, Identity theft. **Computer Forensics:** Historical background of cyber forensics, Digital forensics science, The need of computer forensics, Cyber forensics and digital evidence, Forensics analysis of e-mail, Digital forensics life cycle, Chain of custody concept, Network forensics, Computer forensics and stenography, OSI 7 layer model, Forensics and social networking sites, Challenges in computer forensics, Special tools and techniques.	8
Unit – VI		
6	**Cybercrimes and Cyber security – The legal perspectives:** Cybercrime and the legal landscape around the world, Cyber laws in Indian context, The Indian IT act, Digital signatures and the Indian IT act, Amendments to Indian IT act, Cybercrimes and punishments, Intellectual property in cyberspace, The ethical dimension of cybercrimes, Psychology and mindset of hackers, Sociology of cybercriminals.	9

Sr. No.	Introduction to Cyber Security (Practicals)	Hours
1	Case study: Official website of Maharashtra Government hacked.	4
2	Case study: E-mail spoofing instances.	4
3	Case study: E-mail bombing involving a Foreigner.	4
4	Case study: Job racket exposed by Mumbai city cybercrime cell.	4
5	Case study: Infinity E-search BPO case.	2
6	Case study: Parliament attack.	4
7	Case study: The petrol pump fraud.	4
8	Case study: Game source code stolen.	4

Text book:

1. Nina Godbole and Sunit Belapure, "Cyber Security – Understanding Cybercrimes, Compter Forensics and Legal Perspectives", Wiley Publication.

Reference books:

1. Marjie T. Britz - Computer Forensics and Cyber Crime: An Introduction - Prentice Hall.
2. George M. Mohay - Computer and intrusion forensics - Artech House.

Course objectives and Course outcomes mapping:

- To unfold the fundamentals of cyber security, cybercrimes, and cyber forensics: CO1, CO2, CO3 and CO5.
- To introduce various security challenges, phishing, and tools and methods used for cybercrime: CO4 and CO5.
- To expose students with legal and ethical perspectives of cyber security and cybercrimes: CO6.

Course units and Course outcomes mapping:

Unit No.	Unit Name	Course Outcomes					
		CO1	CO2	CO3	CO4	CO5	CO6
1	Introduction to Cyber Crimes	✓					
2	Cyber Offenses		✓				
3	Security Challenges with Mobile and Wireless Devices			✓			
4	Tools and Methods used in Cybercrime				✓		
5	Phishing, Identity Theft and Computer Forensics					✓	
6	Cybercrimes and Cyber security – The legal perspectives						✓

Programme outcomes:

PO 1: Engineering knowledge: An ability to apply knowledge of mathematics, science, and engineering.

PO 2: Problem analysis: An ability to identify, formulates, and solves engineering problems.

PO 3: Design/development of solutions: An ability to design a system, component, or process to meet desired needs within realistic constraints.

PO 4: Conduct investigations of complex problems: An ability to use the techniques, skills, and modern engineering tools necessary for solving engineering problems.

PO 5: Modern tool usage: The broad education and understanding of new engineering techniques necessary to solve engineering problems.

PO 6: The engineer and society: Achieve professional success with an understanding and appreciation of ethical behavior, social responsibility, and diversity, both as individuals and in team environments.

PO 7: Environment and sustainability: Articulate a comprehensive world view that integrates diverse approaches to sustainability.

PO 8: Ethics: Identify and demonstrate knowledge of ethical values in non-classroom activities, such as service learning, internships, and field work.

PO 9: Individual and team work: An ability to function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.

PO 10: Communication: Communicate effectively on complex engineering activities with the engineering community and with society at large, such as, being able to comprehend and write effective reports and design documentation, make effective presentations, and give/receive clear instructions.

PO 11: Project management and finance: An ability to demonstrate knowledge and understanding of the engineering and management principles and apply these to one's own work, as a member and leader in a team, to manage projects and in multidisciplinary environments.

PO 12: Life-long learning: A recognition of the need for, and an ability to engage in life-long learning.

Programme outcomes and Course outcomes mapping:

Programme Outcomes	Course Outcomes					
	CO1	CO2	CO3	CO4	CO5	CO6
PO1						

PO2				✓		
PO3				✓		
PO4			✓	✓		✓
PO5				✓		
PO6						
PO7						
PO8						✓
PO9						
PO10						
PO11						
PO12	✓					✓