Course Title:	**Introduction to Cyber Security**	Semester	I/II
Course Code:	**BETCK105I/ BETCK205I**	CIE Marks	50
Course Type (Theory/Practical/Integrated)	Theory	SEE Marks	50
		Total Marks	100
Teaching Hours/Week (L:T:P: S)	3-0-0-0	Exam Hours	03
Total Hours of Pedagogy	40 hours	Credits	03

Course Learning Objectives

CLO 1. To familiarize cybercrime terminologies and perspectives
CLO 2. To understand Cyber Offenses and Botnets
CLO 3. To gain knowledge on tools and methods used in cybercrimes
CLO 4. To understand phishing and computer forensics .

Teaching-Learning Process

These are sample Strategies, which teachers can use to accelerate the attainment of the various course outcomes.

1. Chalk and Board
2. Demonstration
3. Interactive learning
4. Videos and online material .

Module-1:Introduction to Cybercrime(8 hours)

Self-study: Hacking applications

Introduction to Cybercrime:
Cybercrime: Definition and Origins of the Word Cybercrime and Information Security, Who are Cybercriminals? Classifications of Cybercrimes, An Indian Perspective, Hacking and Indian Laws., Global Perspectives.

Applications:detecting Hackers, remedies for controlling Hackers
Text Book 1: Chapter 1: 1.1,1.2, 1.3, 1.4,1.5, 1.8,1.9

(RBTLevels:L1,L2and L3)

Module-2:Cyber Offenses(8 hours)

Cyber Offenses:
How Criminals Plan Them: Introduction, How criminals plan the attacks, Social Engineering, Cyber Stalking, Cyber cafe & cybercrimes.
Botnets: The fuel for cybercrime, Attack

Applications: identify criminals and plan the attacks
Text Book 1 :Chapter 2: 2.1, 2.2, 2.3, 2.4, 2.5
(RBTLevels:L2and L3)

Module-3:Tools and Methods used in Cybercrime(8hours)

Tools and Methods used in Cybercrime: Introduction, Proxy Servers, Anonymizers, Phishing, Password Cracking, Key Loggers and Spyways, Virus and Worms, Trozen Horses and Backdoors, Steganography, DoS and DDOS Attacks, Attacks on Wireless networks.

Applications: identifying malicious node in wireless networks.
Text Book 1 Chapter 4: 4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 4.74.8, 4.9, 4.12
(RBT Levels:L2, L3 and L4)

Module-4:Phishing and Identity TheftContracts(8hours)

Self-study: phishing scam case study

Phishing and Identity Theft: Introduction, methods of phishing, phishing, phishing techniques, spear phishing, types of phishing scams, phishing toolkits and spy phishing, counter measures, Identity Theft
Applications: phishing, phishing scams.

Text Book 1: Chapter 5: 5.1, 5.2, 5.3
(RBT Levels:L2, L3 and L4)

Module-5:Understanding Computer Forensics(8hours)

Understanding Computer Forensics: Introduction, Historical Background of Cyber forensics, Digital Forensics Science, Need for Computer Forensics, Cyber Forensics and Digital Evidence, Digital Forensic Life cycle, Chain of Custody Concepts, network forensics.

Applications: methods ofDigital Forensics
Text Book 1:Chapter 7: 7.1, 7.2, 7.3, 7.4, 7.5, 7.7, 7.8, 7.9

(RBT Levels:L1, L2, and L4)

Course outcome

At the end of the course, the student will be able to:

CO1:Understand the cybercrime, Classifications of Cybercrimes and hacking and Indian and Global Perspectives.
CO2: analyze criminals, understand Cyber offenses and Botnets.
CO3: Illustrate Tools and Methods used on Cybercrime
CO4: Explain Phishing and Identity Theft
CO5: Justify the need of computer forensics, Digital Evidence, and Chain of Custody Concepts

Course Assessment and Evaluation Details(both CIE and SEE)

Continuous Internal Evaluation: 50 marks		
Theory Assessment Tool	**Marks**	**Reduced marks**
IAT-1	25	25
IAT-2	25	
Assessment-1(activity based)	25	25
Assessment-2(activity based)	25	
Semester End Examination(SEE):50marks		
SEE	**Marks**	**Reduced marks**
Course end examination (Answer any one question from each unit – Internal choice)	100	50

Activity Based Learning/Practical Based learning

Suggested Activities are:

Practical-Based Learning (PBL) are highly effective strategies for teaching Cyber Security and Computer Forensics, as they allow students to engage directly with real-world scenarios

Suggested Learning Resources:

Suggested Learning Resources:

Text Book:

1. Sunit Belapure and Nina Godbole, "Cyber Security: Understanding Cyber Crimes, Computer Forensics And Legal Perspectives", Wiley India Pvt Ltd, ISBN: 978-81-265- 21791, 2011, First Edition (Reprinted 2018)

Reference Books:

1. Cyber Security Understanding Cyber Crimes, Computer Forensics and Legal Perspectives by Sumit Belapure and Nina Godbole, Wiley India Pvt. Ltd, 1st Edition 2011, Reprint 2022, ISBN:978-81-265-2179-1

Web links and Video Lectures (e-Resources):

1.https://www.youtube.com/watch?v=yC_hFm0BX28&list=PLxApjaSnQGi6Jm7LLSxvmNQjS_rt9swsu
2.https://www.youtube.com/watch?v=nzZkKoREEGo&list=PL9ooVrP1hQOGPQVeapGsJCktzIO4DtI4_
3. https://www.youtube.com/watch?v=6wi5DI6du4&list=PL_uaeekrhGzJlB8XQBxU3z_-hDwT95xlk
4. https://www.youtube.com/watch?v=KqSqyKwVuA8

COs and POs Mapping (CO-PO mappings are only Indicative)

COs	Pos											
	1	2	3	4	5	6	7	8	9	10	11	12
CO1	3	3										
CO2	2	2		3		3				3		
CO3				3	3	3						
CO4	3			3	3				3	2		3
CO5					3	3				3		3

Level 3-HighlyMapped, Level 2-Moderately Mapped, Level 1-Low Mapped, Level 0-Not Mapped