2021 SCHEME

Basavarajeswari Group of Institutions

BALLARI INSTITUTE OF TECHNOLOGY & MANAGEMENT

(Autonomous Institute under Visvesvaraya Technological University, Belagavi)

USN											Course Code	2	1	C	S	6	5	4

Sixth Semester B.E. Degree Examinations, September/October 2024

INTRODUCTION TO CYBER SECURITY

Duration: 3 hrs **Max. Marks: 100**

***Note:** 1. Answer any* **FIVE** *full questions choosing ONE full Question from each Module.*
2. Missing data, if any, may be suitably assumed

Q. No		Question	Marks	(RBTL:CO:PI)
		Module-1		
1.	**a.**	Define the following terms: (i) Phishing (ii) Cybernetics (iii) Cybersquatting (iv) Cyber terrorism (v) Cyberwarfare.	**05**	**(1:1:1.2.1)**
	b.	Explain the categorization of cybercriminals.	**07**	**(2:1: 1.2.1)**
	c.	Describe various types of cybercrimes against an individual.	**08**	**(2:1:1.2.2)**
		OR		
2.	**a.**	Summarize on: (i) The legal perspectives on cybercrime. (ii) An Indian perspective on cybercrime.	**08**	**(2:1:2.1.2)**
	b.	Explain the role of extended enterprise with respect to cybercrime.	**06**	**(2:1: 1.2.1)**
	c.	Outline the impact of the 5P Netizen mantra on enhancing cyber security.	**06**	**(2:1: 1.2.2)**
		Module-2		
3.	**a.**	Explain the phases involved in the planning of a cybercrime.	**08**	**(2:2: 2.1.2)**
	b.	Differentiate the passive and active attacks involved in a cyberattack.	**06**	**(2:2: 2.1.3)**
	c.	Describe the classification of cybercrimes with examples.	**06**	**(2:2: 1.2.1)**
		OR		
4.	**a.**	Define social engineering. Explain the different ways of social engineering that attackers use to gather unauthorized personal information.	**08**	**(2:2: 2.1.2)**
	b.	Outline the safety and security measures while using the compute in a cybercafe.	**06**	**(2:2: 1.2.1)**
	c.	Discuss how botnets can be used as a fuel to cybercrimes.	**06**	**(2:2: 1.2.2)**
		Module-3		
5.	**a.**	Describe the different approaches involved in password cracking.	**08**	**(2:3: 1.2.1)**
	b.	Compare between a proxy server and an anonymizer.	**06**	**(2:3: 2.1.3)**

Note: (RBTL - Revised Bloom's Taxonomy Level: CO - Course Outcome: PI– Performance Indicator)

	c.	Outline the concept of Trojan horses and backdoors.	**06**	**(2:3: 2.1.3)**

OR

6.	**a.**	Distinguish between a Virus and a Worm.	**08**	**(2:3: 1.2.1)**
	b.	Define a DoS attack. Explain different levels of DoS attacks.	**06**	**(2:3: 2.1.2)**
	c.	Discuss the traditional techniques of attacks on wireless networks.	**06**	**(2:3: 1.2.2)**

Module-4

7.	**a.**	Explain the four different methods of phishing that reveal personal information on Internet.	**08**	**(2:4: 1.2.1)**
	b.	Discuss in detail the spear phishing technique.	**06**	**(2:4: 2.1.2)**
	c.	Describe any six types of phishing scams.	**06**	**(2:4: 2.1.3)**

OR

8.	**a.**	Describe the countermeasures to prevent being a victim of phishing attack.	**08**	**(2:4: 1.2.1)**
	b.	Discuss the countermeasures to prevent being a victim of identity theft.	**06**	**(2:4: 1.2.2)**
	c.	Differentiate between Spam and Hoax mails.	**06**	**(2:4: 2.1.3)**

Module-5

9.	**a.**	Define digital forensics science. Discuss the need for computer forensics in investigation of cybercrime.	**08**	**(2:5: 1.2.1)**
	b.	Explain difference between forensics policy and security policy.	**06**	**(2:5: 2.1.3)**
	c.	Explain the rules of identifying the digital evidence in computer forensics.	**06**	**(2:5: 2.1.2)**

OR

10	**a.**	Explain the phases in the computer forensics life cycle.	**08**	**(2:5: 1.2.2)**
	b.	Outline the precautions to be taken while collecting electronic evidence.	**06**	**(2:5: 1.2.1)**
	c.	Explain the chain of custody concepts in cyber forensics.	**06**	**(2:5:2.1.3)**

** ** **

Note: (RBTL - Revised Bloom's Taxonomy Level: CO - Course Outcome: PI– Performance Indicator)