VIT Vidyalankar Institute of Technology Accredited A+ by NAAC (Autonomous College Affiliated to University of Mumbai)	*End Semester Examination (CBSGS-C scheme) -(2022-23)*	
Date:	Branch: All Branches	Time: 2 Hr.
Semester: 7	Subject: Cyber Security and Laws	Marks: 50

N B. :- All Questions are Compulsory	CO	BL
Q. 1)	**Attempt any Five (2 Marks Each)**		
a)	**Define malware & mention it's type.** Adware: It is a software application that automatically displays or downloads advertising material while program is running. Spyware: It is a type of program that is installed with or without your permission or knowledge on your personal computer to collect information about users. **Phishing** Phishing is a type of social engineering used by cybercriminals to trick the users and acquire their sensitive information which is then used for cybercrimes such as financial breaches and data theft. There are varied types of phishing — email spoofing, URL spoofing, website spoofing, smishing, vishing and more. The most common ones are done through email, phone and SMS.	CO1	4
b)	**List different types of viruses.** A virus is a fragment of code embedded in a legitimate program. Viruses are self-replicating and are designed to infect other programs. They can wreak havoc in a system by modifying or destroying files causing system crashes and program malfunctions. On reaching the target machine a virus dropper(usually a trojan horse) inserts the virus into the system. Concept virus, CIH, Melissa Virus, Morris Worm, ILOVEYOU, Anna Kournikova Worm, Blaster Worm, Code red, Storm , Netsky & Sasser, Nimada Worm	CO2	2,4
c)	**How to get protection against viruses, Worms, Trojans & Malwares?** 1. Keep up-to-date. Update your system, browser, and important apps regularly, taking advantage of automatic updating when it's available. ... 2. Antivirus software. ... 3. Antispyware software. ... 4. Firewalls. ... 5. Choose strong passwords. ... 6. Use stronger authentication. ... 7. Be careful what you click. ... 8. Shop safely.	CO3	2
d)	**Define DoS & DDoS.** A DoS attack is characterized by using a single computer to launch the attack. A distributed denial-of-service (DDoS) attack is a type of DoS attack that comes from many distributed sources, such as a botnet DDoS attack.	CO4	2
e)	**Discuss the various amendments done to the Indian IT Act 2000** **Ans:** • A major amendment was made in 2008. It introduced Section 66A which penalized sending "offensive messages". • It also introduced Section 69, which gave authorities the power of "interception or monitoring or decryption of any information through any computer resource". • Additionally, it introduced provisions addressing - pornography, child porn, cyber terrorism and voyeurism. The amendment was passed on 22 December 2008 without any debate in Lok Sabha. The next day it was passed by the Rajya Sabha. It was signed into law by President Pratibha Patil, on 5 February 2009	CO1	4
f)	**Summarize about Gramm Leach Bliley Act** GLBA Ans: Definition and Use Cases/ Examples	CO2	2
g)	**Write the features of Information Technology Act, 2000.**	CO3	4

	Provides legal recognition to records in the electronic form Provide legal recognition to e-commerce & electronic transaction in India Provides legal recognition to digital signatures issued & authenticated by the certifying authorities It is applicable to cybercrime & contraventions committed in India & outside India by any person It has appointment adjudicating officers for holding inquiries under the Act. It elaborates on offenses, penalties & breaches • It has established the cyber appellate to hear appeals		
h)	**Why we need Indian Cyberlaw.** Consumers depend on cyber laws to protect them from online fraud. Laws are made to prevent identity theft, credit card theft, and other financial crimes that happen online. A person who commits identity theft may face confederate or state criminal charges. They might also encounter a civil action brought by a victim.	CO4	2
Q. 2)	**Attempt any One (10 Marks Each)**		
a)	**Explain Keyloggers in details: what are types of keyloggers. Also explain the functions of anti-keylogger.** Define:- It is a computer program that records every keystroke made by a computer user, especially in order to gain fraudulent access to passwords and other confidential information. Types : Software Keyloggers & Hardware Keyloggers explain in details An anti-keylogger (or anti–keystroke logger) is a type of software specifically designed for the detection of keystroke logger software; often, such software will also incorporate the ability to delete or at least immobilize hidden keystroke logger software on a computer. List the functions of anti-loggers.	CO1	2
b)	**What is Electronic Data Interchange? How does it work? Explain the Legal aspects of Electronic Data taking into consideration the electronic payment systems in India.** **Ans:** 1. Definition of EDI **(2M)** 2. Working **(5M)** 3. Types of Evidence **(3M)** **With the help of examples, illustrate how an Identity Theft attack takes place.** **Ans:** 1. Definition of ID Theft **(2M)** 2. How does it work? **(6M)** 3. Examples or Case Studies **(2M)**	CO1	2
Q 3)	**Attempt any One. (10 Marks Each)**		
a)	**What is Health Insurance Portability and Accountability Act (HIPAA). Explain all 3 categories of security standards of HIPAA.** The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is a federal law that required the creation of national standards to protect sensitive patient health information from being disclosed without the patient's consent or knowledge. The US Department of Health and Human Services (HHS) issued the HIPAA Privacy Rule to implement the requirements of HIPAA. The HIPAA Security Rule protects a subset of information covered by the Privacy Rule. Under HIPAA, protected health information is considered to be individually identifiable health information relating to the past, present, or future health status of an individual that is created, collected, or transmitted, or maintained by a HIPAA-covered entity in relation to the provision of healthcare, payment for healthcare services, or use in healthcare operations (PHI healthcare business uses). Information such as diagnoses, treatment information, medical test results, and prescription information are considered health information under HIPAA, and when these types of information are maintained in a "designated record set" with identifiers such as birth dates, gender, ethnicity, and contact and emergency contact information, all of the information maintained in the set is consider protected health information under HIPAA law. Administrative, Physical & Technical security standards in detail	CO2	4
b)	Explain DDoS attack in details with its operation & type. How to get protection from DDoS.	CO2	4

	A Distributed Denial of Service (DDoS) attack is a non-intrusive internet attack designed to harm the targeted website. It is a malicious attempt to disrupt the regular traffic of a targeted server, service, application, or network by swamping the website or its surrounding infrastructure with a flood of user traffic. Types, Prevention, and Remediation. A distributed denial-of-service (DDoS) attack occurs when a group of systems flood a server with fraudulent traffic. Eventually, the server is overwhelmed, causing it to either go down, or become unresponsive, even to legitimate requests. How to get protection against DDoS? Intrusion-detection systems: IDS solutions will provide some anomaly-detection capabilities so they will recognize when valid protocols are being used as an attack vehicle. They can be used in conjunction with firewalls to automatically block traffic.		
Q 4)	**Attempt any One (10 Marks Each)**		
a)	**What is Steganography? What are the Various modes in which Steganography could be implemented. How is it different from Cryptography?** **Ans:** 1. Definition of Steganography **(2M)** 2. Steganography Techniques **(5M)** Depending on the nature of the cover object(actual object in which secret data is embedded), steganography can be divided into five types: • Text Steganography • Image Steganography • Video Steganography • Audio Steganography • Network Steganography • Difference between Steganography and Cryptography **(3M)**	CO3	4
b)	**FISMA** **Ans:** **Definition and Use Cases/ Examples**	CO3	4
c)	**Short note on SQL injection & its types** SQL injection is a technique used to exploit user data through web page inputs by injecting SQL commands as statements. Basically, these statements can be used to manipulate the application's web server by malicious users. • SQL injection is a code injection technique that might destroy your database. • SQL injection is one of the most common web hacking techniques. • SQL injection is the placement of malicious code in SQL statements, via web page input. Types: Piggy-backed queries Tautologies Union query Blind Injection		
Q 5)	**Write Short Notes on: Attempt any Two (5 Marks Each)**		
a)	**Define Phishing and explain the techniques to launch phishing attack.** Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message. The recipient is then tricked into clicking a malicious link, which can lead to the installation of malware, the freezing of the system as part of a ransomware attack or the revealing of sensitive information. An attack can have devastating results. For individuals, this includes unauthorized purchases, the stealing of funds, or identify theft. Email Phishing Scam Spear Phishing	CO4	2
b)	**Explain various Indian laws related to electronic banking.** Banker's Books Evidence Act 1891 Reserve bank of India Act 1934 Payment & settlement Systems Act, 2007	CO4	2

c)	**Write a short note on electronic contract & its types.** Contracts have been a staple in most of our lives, from signing terms and conditions we haven't got the time to read, to watching lawyers argue about contracts in our favorite courtroom dramas. Contracts are one of the myriad ways in which the law permeates our lives. Types of electronic contracts explain in details (Definition, features & Examples) **1.** Shrink-wrap contracts **2.** Click Wrap Contract **3.** Brows Wrap Contract	CO4	2