V. M. SALGAOCAR INSTITUTE
of
INTERNATIONAL HOSPITALITY EDUCATION

B.Sc. International Hospitality Management

Type: Semester End Assessment (SEA) Date: 10/04/2025

Batch and Semester: 2024-2027 & II Total Marks: 40 Time Duration: 01 Hour

Course Name: Awareness of Cyber Crimes and Security Course Code: VAC-110

Faculty: Dr. Sadhvi Manerikar

This paper contains 02 pages in addition to the cover page.

Full Name of the Student: _____

Permanent Registration Number: _____ Class: _____

Marks Obtained: _____ Faculty Signature: _____ Invigilator Signature: _____

Main Answer sheet	Number of Supplements	Total number of Answer sheets
01		

- Carefully read each question at the outset of the paper. All queries must be addressed to the faculty within the first 10 minutes of the examination.
- Students are expected to maintain complete silence in the examination hall and should not interact or communicate with their peers.
- Students will carry only their essential stationery like pens, pencils, ruler and simple calculators into the examination hall.
- Bags, eatables, drinks, etc. will not be allowed inside the hall with the exception of a bottle of water.
- Cell phones, electronic data banks, scientific calculators and smart/beeping watches are prohibited in the examination hall.
- Students will answer the examination with only blue/ black ball point pens unless informed differently by faculty. Avoid usage of green or red ink pens on the answer sheet.
- Dictionaries will not be allowed into the examination hall unless informed differently by faculty.

Q.1. Answer the following **(4 x 2 Marks) = 8 Marks**

i. What is identity theft, and how does it impact both individuals and organizations?
ii. Mention and elaborate on any method used by the attacker to steal credit card information.
iii. What is a zero-day attack?
iv. What is Lottery/Gift fraud? Explain with an example.

Q.2 A) i. Name any three cybercrimes that can be carried out against an individual and explain briefly. **3 marks**

OR

Q.2 A) ii. Define any three cybercrimes that can be committed against an organization. **3 Marks**

Q.2 B) i. Define CIA triad and explain. **3 Marks**

Q.2 C) i. Identify the ways to prevent ATM Frauds/Scams. **2 Marks**

Q.3 A) i. Summarize briefly the various phases of cyberattack. **3 marks**

OR

Q.3 A) ii. Why is information classification necessary? Which are the different classification levels? **3 Marks**

Q.3 B) Explain how to protect a computer from unauthorized access. **3 Marks**

Q.3 C) i. Articulate the various motives behind cybercrime **2 Marks**

Q.4 A) i. Differentiate between active sniffing and passive sniffing **2 Marks**
ii. Explain what is catfishing **1 Mark**

OR

Q.4 A) iii. Explain briefly what is a virus, spyware, malware, and ransomware. **3 Marks**

Q.4 B) What is meant by physical, logical and administrative controls in cybersecurity. Give an example for each **3 Marks**

Q.4 C) i. Briefly describe any 2 types of banking frauds. **2 Marks**

Q.5 A) i. Describe all the phases of cyber-attack briefly **3 Marks**

OR

Q.5 A) ii. Identify any three types of Intellectual Property frauds. Give an example for each. **3 Marks**

Q.5 B) John is a senior executive at a large tech company. He receives an email that appears to be from a trusted colleague, Sarah. The email is well-crafted, using John's name, a familiar tone, and includes specific details about a new project they've been working on. The email asks John to download a file attached to the message, which supposedly contains important documents related to the project. The email looks convincing, with no obvious signs of fraud. The attachment is a Word document. John, trusting the sender, opens the document without suspicion.

i. What is/are the type of cybercrime(s) demonstrated in this scenario?
ii. What measures could John have taken to prevent this cybercrime from happening? **3 Marks**

Q.5 C) Mark is active on social media and frequently posts updates about his life. One day, he notices strange messages being sent from his account to his friends. They include links that seem suspicious, and some of the messages don't sound like something Mark would write. He tries to log into his account but finds that his password has been changed. Mark realizes that his social media account has been hacked, and the hacker is using it to send spam and phishing links to his contacts.

i. How did the hacker likely gain access to Mark's account?
ii. How can Mark prevent his social media account from being hacked again in the future? **2 Marks**