Total No. of Questions: 25 Total No. of Printed Pages: 4

AISSMS College of Hotel Management and Catering Technology, Pune

Seat No: [0607]/HSVSC358/2025/BSCHS_SEM5

TYBSCHS (Fifth Semester) Examination, 2025
HSVSC358 –CYBER SECURITY SYSTEM
(2023 Pattern)

Time: 1 Hour Maximum Marks: 25

Instructions: -
(i) Select Correct Options
(ii) All questions are compulsory.

Q1. What is the primary function of a mobile phone's antenna? [1]
a) To convert electro-magnetic signals to electrical signals and vice versa
b) To display visual content
c) To store digital data
d) To manage the operating system of the mobile phone

Q2. What is the primary function of a Network Interface Card (NIC)? [1]
a) To store data permanently
b) To process audio signals
c) To connect the computer to a network
d) To display visual output on the monitor

Q3. Which of the following is NOT a type of primary data storage? [1]
a) Read Only Memory (ROM)
b) Random Access Memory (RAM)
c) Solid State Drive (SSD)
d) Cache Memory

Q4. What is the primary purpose of the handoff procedure in mobile communication systems? [1]
a) To allow seamless call continuity when moving from one cell to another
b) To increase the speed of data transmission
c) To enable mobile devices to connect to different networks
d) To manage battery power usage

Q5. Which term refers to the act of using cyberspace to create, display, distribute, or publish obscene materials without consent? [1]
a) Cyber pornography
b) Cyber espionage
c) Cyber terrorism
d) Cyberstalking

Q6. What is the primary motive behind phishing attacks? [1]

a) To disrupt a network's services

b) To infect a computer with a virus

c) To create fake profiles on social media

d) To steal sensitive information such as passwords or credit card details

Q7. Which of the following is NOT a characteristic of cybercrime? [1]

a) Physical evidence

b) Trans-boundary nature

c) Dynamic modus operandi

d) Anonymity

Q8. Which of the following is a common type of financial fraud? [1]

a) Cyberbullying

b) Cyberstalking

c) E-wallet fraud

d) Phishing

Q9. How can opportunity in the Fraud Triangle be best described? [1]

a) As a financial motive for engaging in fraudulent activities

b) As a personal justification for committing fraud

c) As the perceived unfair treatment by the employer

d) As a flaw in the company's internal control system that allows fraud to occur

Q10. Which social media platform is known for allowing users to send and receive short messages called ""tweets""? [1]

a) Facebook

b) LinkedIn

c) Instagram

d) Twitter

Q11. What action can you take if you encounter a fake profile, page, or group on a social media platform? [1]

a) Share it with friends

b) Ignore it

c) Report it to a local law enforcement agency

d) Contact a social media nodal officer via email

Q12. Which element of the Fraud Triangle involves an individual's personal drive or reason for committing fraud? [1]

a) Justification

b) Opportunity

c) Rationalization

d) Motive

Q13. How do fraudsters typically operate in URL/SMS/Email/Instant Messaging/Call driven frauds? **[1]**

a) By installing malware on victims' computers

b) By compromising ATMs

c) By hacking into email accounts

d) By circulating fake messages to induce victims into paying charges

Q14. What is a key risk associated with sending emails? **[1]**

a) Improved collaboration

b) Better record-keeping

c) Unauthorized access and email spoofing

d) Increased communication efficiency

Q15. In the case study of ticketing fraud, what was the primary role of the Tatkal Turbo Software? **[1]**

a) Intercepting OTPs

b) Sending phishing emails

c) Hacking social media accounts

d) Auto-filling payment details

Q16. What is cyber sexting? **[1]**

a) Sharing business-related documents

b) Posting images of pets online

c) Sending regular text messages

d) Sharing sexually explicit images and videos via electronic devices

Q17. What does ""Revenge Porn"" refer to? **[1]**

a) The sharing of intimate images with consent

b) The distribution of explicit images with the aim to entertain

c) The sale of explicit content for commercial gain

d) The distribution of sexually explicit images or videos to damage someone's reputation

Q18. Which of the following is NOT a suggested countermeasure to prevent online harassment? **[1]**

a) Keeping software updated

b) Using encryption for social media accounts

c) Over-sharing personal information online

d) Applying strong privacy settings

Q19. Which of the following is a common method used to distribute malicious apps? **[1]**

a) Phone calls

b) Links sent via SMS, email, or social media

c) Physical mail

d) Direct email attachments

Q20. What is the primary motive behind the harassment by instant loan apps? [1]

a) To facilitate genuine loan recovery

b) To offer financial counseling

c) To provide educational loans

d) To extort additional money and cause social humiliation

Q21. What does a ransomware attack typically do to the victim's data? [1]

a) Encrypts the files and demands a ransom for decryption

b) Copies files to an external server

c) Corrupts files without encryption

d) Deletes all files

Q22. What is matrimonial fraud? [1]

a) A scheme to manipulate individuals through fake matrimonial claims

b) Fraud related to financial investments

c) Identity theft in social networks

d) A type of business scam

Q23. What action should be taken if you receive an unsolicited email asking for sensitive information? [1]

a) Report the email to the relevant authorities

b) Ignore the email

c) Click on any links provided to check their authenticity

d) Respond with the requested information

Q24. What is ransomware? [1]

a) A network security protocol

b) A type of hardware device

c) A type of physical malware

d) A software that encrypts files and demands a ransom for decryption

Q25. What does the term ""vishing"" refer to? [1]

a) Voice phishing over the telephone

b) Phishing through text messages

c) Phishing using social media

d) Spoofing email addresses

*****