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

AISSMS College of Hotel Management and Catering Technology, Pune

Seat No:

[0607]/HSVSC238/2025/BSCHS_SEM3

(BSCHS_SEM3) Examination, 2025

HSVSC238 –CYBER SECURITY SYSTEM

(Rev. 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 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

Q2. What are the two main components of a computer system? [1]

a) RAM and Hard Drive

b) Keyboard and Monitor

c) Input and Output Devices

d) Hardware and Software

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. 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

Q6. What is the primary function of video social media platforms? [1]

a) Sharing short-lived posts
b) Listening to live conversations
c) Watching videos
d) Shopping from profiles

Q7. Which of the following is a form of psychological trick used in cybercrimes? [1]

a) DDoS attacks
b) Data breaches
c) Cyber warfare
d) Job-related frauds

Q8. What is the primary definition of cybercrime according to the IT Act 2008? [1]

a) Crime involving traditional forms of theft and violence
b) Crime involving the theft of physical objects
c) Crime carried out using computers, digital devices, and networks
d) Crime committed using physical methods

Q9. What could be a potential motive for committing fraud? [1]

a) Feeling a strong need for financial gain
b) None of the above
c) The opportunity to exploit a lack of oversight
d) Rationalizing actions as a form of compensation

Q10. 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

Q11. What is the primary function of Instagram? [1]

a) To post job openings and CVs
b) To send and receive short text messages
c) To connect people globally
d) To share images and short films using hashtags

Q12. What is a significant disadvantage of social media mentioned in the module? [1]

a) The ability for individuals to impersonate others by creating fake profiles
b) Limited user engagement
c) High cost of platform usage
d) Difficulty in accessing information

Q13. In OTP frauds, what information is typically requested from victims? [1]

a) Debit/Credit card number and OTP
b) Personal Identification Number (PIN)
c) Bank Account Number
d) Social Security Number

Q14. What should be avoided to mitigate the risks associated with social media? [1]

a) Using strong passwords

b) Reviewing app permissions

c) Regularly updating privacy settings

d) Disclosing personal information like home address or family details

Q15. What type of fraud is characterized by an attacker sending threatening messages demanding money to avoid sharing explicit content online? [1]

a) SIM Swapping

b) Lottery Fraud

c) Cyber Stalking and Extortion

d) Supply Chain Fraud

Q16. What kind of information is collected through the fake job website? [1]

a) Personal identification numbers

b) Social security numbers

c) Registration fees for job applications

d) Bank account details

Q17. What is one key indicator of a vishing attack? [1]

a) Receiving unsolicited emails

b) Receiving a suspicious phone call requesting personal information

c) Receiving a fake invoice in the mail

d) Receiving an SMS with a link

Q18. 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

Q19. 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

Q20. What is the main objective of a phishing scam? [1]

a) To gain physical access to the victim's home

b) To solicit donations for charity

c) To sell fake products online

d) To obtain sensitive personal or financial information

Q21. What is the first step in the modus operandi of profile hacking? [1]

a) Submit fraudulent messages

b) Obtain credentials

c) Hide evidence

d) Reconnaissance and compromise

Q22. Which modus operandi involves a cybercriminal recording private moments during a video call? [1]

a) Hacking email accounts

b) Sending spam messages

c) Blackmailing victims with recorded private moments

d) Creating fake social media profiles

Q23. What is the primary concern in cases involving abusive or threatening calls? [1]

a) Financial loss

b) Emotional distress

c) Data breach

d) Identity theft

Q24. What is the purpose of the fake websites created by the perpetrators? [1]

a) To sell counterfeit products

b) To provide genuine job offers

c) To collect donations for charity

d) To fraudulently collect registration fees for fake job applications

Q25. What type of card technology makes it harder for fraudsters to use stolen data? [1]

a) Prepaid cards

b) Magnetic stripe cards

c) Contactless cards

d) EMV cards (Chip cards)

*****