

Total No. of Questions: 50

Total No. of Printed Pages: 8

AISSMS College of Hotel Management and Catering Technology, Pune

Seat No:

[0607]/PE704B/2025/BHMCT_SEM7

Final Year (Seventh Semester) Examination, 2025
PE704B - INTRODUCTION TO CYBER SECURITY
(2021 Pattern)

Time: 2 Hours

Maximum Marks: 50

Instructions: -

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

- Q1. Which mobile communication system uses Time Division Multiple Access (TDMA)? [1]
- a) GSM
 - b) LTE
 - c) CDMA
 - d) UMTS
- Q2. Which device is used to capture an exact digital copy of a photograph or document? [1]
- a) Webcam
 - b) Microphone
 - c) Scanner
 - d) Printer
- Q3. What type of software provides an interface between the computer hardware and the user? [1]
- a) Utility Programs
 - b) System Software
 - c) Firmware
 - d) Application Software
- Q4. What is the primary function of a hub in a computer network? [1]
- a) To amplify or regenerate a signal
 - b) To provide a direct connection between the source and destination
 - c) To connect two different networks
 - d) To serve as a central connection point for network devices and broadcast messages to all ports

- Q5. What type of transmission medium does NOT use a physical path for sending data? [1]
- a) Twisted pair cables
 - b) Coaxial cable
 - c) Fibre optic cable
 - d) Radio waves
- Q6. Which type of website is accessible only within an organization's intranet? [1]
- a) Restricted Website
 - b) Internet Website
 - c) Accessible Website
 - d) Public Website
- Q7. Which of the following devices is used to connect different networks together? [1]
- a) Modem
 - b) Router
 - c) Switch
 - d) Network Interface Card
- Q8. 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
- Q9. Which social media platform type is used for sharing tiny content like short sentences and video links? [1]
- a) Social dating apps
 - b) Social audio platforms
 - c) Micro-Blogs and Discussion forums
 - d) Disappearing content formats
- Q10. What is 'skimming' in the context of cybercrimes? [1]
- a) Capturing card information using a skimming device to clone debit/credit cards
 - b) Accessing secure networks using unauthorized credentials
 - c) Sending malicious software via email
 - d) Creating fake social media profiles
-
- Q11. 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

- Q12.** 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
- Q13.** 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
- Q14.** Which type of social media platform allows users to start a live video online in real time? [1]
- a) Social gaming platforms
 - b) Social media live streams
 - c) Inspirational social media platforms
 - d) Closed/private community social media platforms
- Q15.** Which type of cybercrime involves stealing or misusing sensitive personal information such as credit card details? [1]
- a) Cyber terrorism
 - b) Phishing
 - c) Identity theft
 - d) Cyberstalking
- Q16.** Which scenario best illustrates the opportunity component of the Fraud Triangle? [1]
- a) A worker rationalizes theft by claiming they are overworked
 - b) An employee is motivated to commit fraud due to a gambling addiction
 - c) An individual uses their access to company systems to manipulate financial records
 - d) An employee feels underpaid and justifies their actions by believing they are owed more money
- Q17.** Which of the following is an example of a motive in the Fraud Triangle? [1]
- a) Feeling underpaid
 - b) Lack of proper internal controls
 - c) Belief that the company is too large
 - d) Opportunity to manipulate financial records
- Q18.** 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

- Q19. 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
- Q20. Rationalization in the Fraud Triangle involves. [1]
- a) The opportunity to commit fraud due to lack of oversight
 - b) The individual's beliefs that justify their dishonest behavior
 - c) The personal drive or need that prompts fraudulent actions
 - d) A flaw in the company's internal control system
- Q21. 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
- Q22. 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
- Q23. What is a primary risk associated with sharing information on social media? [1]
- a) Enhanced privacy
 - b) Increased job opportunities
 - c) Identity theft and cyberstalking
 - d) Improved social connections
- Q24. 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
- Q25. 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
- Q26. Which of the following is NOT a common type of Internet-based cybercrime? [1]
- a) Identity Theft
 - b) Physical Theft
 - c) Job Frauds
 - d) Fintech Frauds

- Q27. What is a primary method used by criminals in fintech frauds at the individual level? [1]
- a) Ransomware Attacks
 - b) Phishing, vishing, and smishing
 - c) Business Email Compromise
 - d) Compromising bank servers
- Q28. What precaution can you take to protect yourself from social media risks? [1]
- a) Set privacy settings to restrict access to your information
 - b) Share your location regularly
 - c) Keep your social media profiles public
 - d) Post personal information frequently
- Q29. 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
- Q30. What is a Business Email Compromise (BEC) attack designed to do? [1]
- a) Send spam emails
 - b) Encrypt email communications
 - c) Improve email deliverability
 - d) Trick individuals into wiring payments to fraudulent accounts
- Q31. What is a common tactic used by scammers in Lottery Fraud? [1]
- a) Sending a fraudulent check
 - b) Hacking into email accounts
 - c) Installing malware on the victim's computer
 - d) Offering a commission for transferring money
- Q32. 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
- Q33. 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

- Q34. 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
- Q35. 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
- Q36. What should you do if you find an unauthorized transaction in your account? [1]
- a) Attempt to reverse the transaction yourself
 - b) Wait for a month to see if the transaction is reversed
 - c) Call the bank immediately
 - d) Ignore it
- Q37. 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
- Q38. 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
- Q39. What is a characteristic of work from home job fraud? [1]
- a) Offering free training and resources
 - b) Tricking individuals into working without payment or paying to start a non-existent business
 - c) Providing guaranteed job placements
 - d) Providing substantial salary increases
- Q40. 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

- Q41. 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
- Q42. What is a common characteristic of cryptocurrency fraud? [1]
- a) Fake websites displaying false profits
 - b) Real-time tracking of investments
 - c) Genuine investment opportunities
 - d) Reliable cryptocurrency exchanges
- Q43. What type of threats are commonly involved in cyberstalking? [1]
- a) Threats related to job security
 - b) Threats to public speaking engagements
 - c) Direct or implied threats of physical harm
 - d) Financial threats
- Q44. What is a common tactic used by fraudsters in matrimonial scams? [1]
- a) Offering high returns on investments
 - b) Requesting money under false pretenses, such as medical emergencies
 - c) Selling fake products online
 - d) Using phishing emails to gain personal information
- Q45. Which technology is commonly used by digital wallets for secure transactions? [1]
- a) RFID (Radio-Frequency Identification)
 - b) GPS (Global Positioning System)
 - c) QR Code (Quick Response Code)
 - d) NFC (Near Field Communication)
- Q46. What reason do scammers give for requiring advance payments in delivery / parcel scams? [1]
- a) Indian customs clearance and anti-terrorism certificate
 - b) Processing fees for lottery winnings
 - c) Legal fees for lottery registration
 - d) Bank fees for transferring money
- Q47. What is an effective countermeasure to prevent profile hacking? [1]
- a) Frequently change your profile details
 - b) Use the same password for all accounts
 - c) Look for evidence of a real-world presence like an address or phone number
 - d) Share your passwords with trusted friends

- Q48. 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
- Q49. 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
- Q50. What is job fraud? [1]
- a) A scam where job seekers are deceived into paying for non-existent job opportunities
 - b) A legitimate job offers
 - c) An authorized job placement service
 - d) A promotional job advertisement
