Total No. of Questions: 50 **Total No. of Printed Pages: 7**

AISSMS College of Hotel Management and Catering Technology, Pune

Seat No:

[0607]/PE704B/2026/BHMCT_SEM7

Final Year (Seventh Semester) Examination, 2026

PE704B - INTRODUCTION TO CYBER SECURITY

(2021 Pattern)

Time: 2 Hours **Maximum Marks: 50**

Instructions: -

(i) Select Correct Options.

(ii) All questions are compulsory.

Q1. What feature is common to both smartphones and tablets? **[1]**

a) Voice and video calling

b) Physical keyboards

c) Non-touchscreen displays

d) Limited internet access

Q2. Which of the following mobile operating systems is developed by Google? **[1]**

a) BlackBerry OS

b) Windows Mobile

c) Android OS

d) iOS

Q3. 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

Q4. Which mobile communication system uses Time Division Multiple Access (TDMA)? **[1]**

a) GSM

b) LTE

c) CDMA

d) UMTS

Q5. Which device is used to capture an exact digital copy of a photograph or document? **[1]**

a) Webcam

b) Microphone

c) Scanner

d) Printer

Q6. 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

Q7. 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

Q8. What is meant by the term 'CIA triad' in cybersecurity? **[1]**

a) Confidentiality, Integrity, Availability
b) Confidentiality, Identification, Authentication
c) Control, Integrity, Authorization
d) Cryptography, Identification, Authorization

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

a) Cyberbullying
b) Cyberstalking
c) E-wallet fraud
d) Phishing

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. The practice of using computer networks to secretly gather classified, sensitive, or confidential information from various organizations without their knowledge or consent is called? **[1]**

a) Cyber pornography
b) Cyber espionage
c) Cyber terrorism
d) Cyberstalking

Q14. 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

Q15. 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

Q16. 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

Q17. 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

Q18. What is a typical example of Social Media Matrimony Fraud? **[1]**

a) An impersonator creating fake profiles to spread false news
b) A fraudster posing as a wealthy individual to solicit donations
c) A hacker accessing confidential business information through fake profiles
d) A scammer posing as a prospective groom to deceive victims into giving money

Q19. 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

Q20. 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

Q21. What are the three elements of the Fraud Triangle? **[1]**

a) Desire, Rationalization, Opportunity
b) Motive, Perception, Opportunity
c) Intent, Rationalization, Access
d) Motive, Rationalization, Opportunity

Q22. 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

Q23. 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

Q24. What device is used in illegal telecom exchanges to route international calls through the internet? **[1]**

a) Network Router
b) SIM Box
c) Phishing Box
d) VoIP Device

Q25. Which type of fintech fraud involves targeting financial and banking organizations? **[1]**

a) Fraud at State Level
b) Fraud at Corporate Level
c) Fraud at Individual Level
d) Fraud at Organization Level

Q26. 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

Q27. 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

Q28. 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

Q29. 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

Q30. 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

Q31. 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

Q32. 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

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 one effective preventive measure against receiving abusive calls? **[1]**

a) Blocking the number
b) Changing your phone number frequently
c) Responding to the caller
d) Ignoring the calls

Q36. What role does Artificial Intelligence play in the email hacking scenario described? **[1]**

a) It encrypts email communications.
b) It directly hacks email accounts.
c) It prevents unauthorized access to email accounts.
d) It helps in creating convincing text in phishing emails.

Q37. 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

Q38. 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

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. 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

Q41. 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

Q42. 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

Q43. 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)

Q44. 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

Q45. 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

Q46. What should be done if you receive a suspicious email about a cryptocurrency investment? **[1]**

a) Checking it regularly

b) Storing it on your laptop or smartphone

c) Keeping it in a secure place

d) Sharing it with trusted individuals

Q47. 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)

Q48. What is the primary technique used by offenders in ATM card skimming? **[1]**

a) Data capture from the magnetic strip of an ATM card

b) Phishing

c) Social engineering

d) Password cracking

Q49. 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

Q50. 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

*****