NA6S-6109-B-24
B.A. VI Semester (NEP) Degree Examination
COMPUTER SCIENCE
Cyber Security
Paper : SEC4BT

Maximum Time : 2 Hours

Roll No.

Maximum Marks : 60
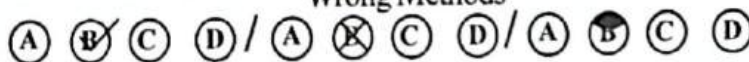
Answer Sheet No.

INSTRUCTIONS

PLEASE READ THE FOLLOWING INSTRUCTIONS CAREFULLY

1. Mark the Roll Number and Answer Sheet No. in the space provided on the Question Booklet and on the Answer Sheet.

2. Candidates are not allowed to carry any papers, notes, books, calculators, mobile phones, blue tooth, scanning devices etc. in the Examination Hall. Any candidate found using or in possession of such unauthorized material or indulging in copying or impersonation or adopting unfair means/reporting late/ without Roll No Slip will not be permitted to take the written Test.

3. Strictly follow the instructions given by the Centre Supervisor/Room Invigilator and those given on the Question Booklet.

4. Use ONLY blue/black ball point pen for darkening the circles on the OMR Answer Sheet. Use of eraser, whitener (fluid) and cutting is not allowed on the OMR Answer Sheet.

5. After finishing the examination, hand over OMR answer sheet to the Room Invigilator.

6. This Question Booklet contains a total of **60 objective type questions carrying one (1) mark each** and the maximum **time alloted for the test is 120 minutes.**

7. The test is Objective type. Each objective question is followed by four responses. Choose the correct/ best response and mark your response on the OMR Answer Sheet and not in the Question Booklet.

8. **There will be no Negative Marking. One mark will be awarded for each correct answer.**

9. Completely darken the CIRCLE so that the alphabet inside the CIRCLE is not visible as shown in the example below

   Correct Method   Wrong Methods
   Ⓐ ● Ⓒ Ⓓ   Ⓐ ⓑ̸ Ⓒ Ⓓ / Ⓐ ⓧ Ⓒ Ⓓ / Ⓐ ⓑ Ⓒ Ⓓ

10. Darken ONLY ONE CIRCLE for each answer. If you darken more than one circle, it will be treated as a wrong answer.

11. Mark answer only in the space provided. DO NOT make any stray mark any where on the OMR Answer Sheet. DO NOT fold or wrinkle the OMR Answer Sheet. Rough work MUST NOT be done on the answer sheet. Use your test booklet for this purpose.

DO NOT OPEN THIS BOOKLET UNTIL TOLD TO DO SO

1. What does CPU stands for in computing?

A) Central Processing Unit

B) Computer Processing Unit

C) Central Programming Unit

D) Computer Programming Unit

2. Which of the following is an example of an input device?

A) Monitor

B) Printer

C) Keyboard

D) Speakers

3. What is the function of RAM(Random Access Memory) in a computer?

A) Long-term storage of data and programs.

B) Processing and executing instructions

C) Providing power to the computer

D) Storing frequently accessed data for quick retrieval by the CPU.

4. Which component of a computer is responsible for displaying visual output?

A) CPU

B) RAM

C) Monitor

D) Hard Disk Drive (HDD)

5. What is the purpose of an Operating System (OS) on a computer?

A) Storing and organizing files.

B) Running applications and managing hardware resources

C) Providing physical protection to the computer

D) Generating reports and documents.

6. What is the role of a web browser on a computer?

   A) Playing music and videos

   B) Managing emails

   C) Accessing and displaying web pages on the internet.

   D) Creating spreadsheets

7. What is cyberspace?

   A) A Physical location where internet servers are stored.

   B) The collective environment of digital communication and information.

   C) A type of computer virus

   D) An online gaming platform.

8. What is the purpose of a web browser in web technology?

   A) To create websites.

   B) To manage emails

   C) To access and display web pages on the internet.

   D) To store data securely

9. What is HTML(Hypertext Markup Language) used for in web development?

   A) Creating dynamic animations.

   B) Storing databases

   C) Defining the structure and content of web pages

   D) Securing websites from cyber attacks.

10. What is the basic unit of data transmission over the internet?

    A) Packet

    B) Byte

    C) Megabyte

    D) Gigabyte

(4)

11. What is the function of an Internet Protocol(IP) address in internet architecture?

    A) To identify the physical location of a website server

    B) To encrypt data during transmission

    C) To uniquely identify devices connected to the internet.

    D) To manage email communications.

12. Which of the following is a fundamental component of the TCP/IP protocol suite used for communication over the internet?

    A) HTTP(Hypertext Transfer Protocol)

    B) DNS(Domain Name System)

    C) SSL(Secure Sockets Layer)

    D) TCP(Transmission Control Protocol)

13. What is the primary mission of the Internet Society?

    A) To develop and market internet-related technologies.

    B) To advocate for an open, globally-connected, and secure internet for everyone

    C) To regulate internet traffic and content

    D) To promote online advertising and e-commerce

14. Who is responsible for regulating cyberspace and internet-related activities in most countries?

    A) Internet Service Providers (ISPs)

    B) Government agencies and regulatory bodies

    C) Social media platforms

    D) Non-Governmental Organizations (NGOs)

15. What is the primary goal of cybersecurity?

    A) To prevent physical theft of computers.

    B) To protect digital assets, data,and information from unauthorized access, attacks and damage.

    C) To ensure fast internet speed

    D) To promote social media usage.

16. What is a common issue faced in cybersecurity?

   A)   Lack of cybersecurity awareness and training.

   B)   Excessive use of antivirus software

   C)   Over-reliance on outdated technologies

   D)   Lack of internet connectivity.

17. Which of the following is a challenge in cybersecurity management?

   A)   Increasing collaboration and information sharing between organizations

   B)   Implementing strong encryption methods for data protection.

   C)   Dealing with evolving cyber threats and sophisticated attack techniques

   D)   Having unlimited financial resources for cybersecurity measures.

18. Which of the following is an example of a cybercrime against individuals?

   A)   Cyber espionage

   B)   Phishing

   C)   Distributed Denial of Service (DDoS) attacks

   D)   Insider threats

19. What category does identity theft fall under in the classification of cybercrimes?

   A)   Cyber terrorism

   B)   Financial crimes

   C)   Cyber harassment

   D)   Intellectual property theft.

20. What is a common form of cybercrime targeting children?

   A)   Cyberbullying

   B)   Identity theft

   C)   Corporate espionage

   D)   Hacking into government databases.

NA6S-6109-B-24   (6)

21. Which of the following is a cybercrime that specifically targets women?

A) Phishing attacks

B) Unauthorized access to financial accounts

C) Online harassment and stalking

D) Software piracy

22. Which of the following is a characteristic of a zero-day attack?

A) It relies on outdated security measures

B) It requires physical access to the target device.

C) It can bypass known security patches and updates.

D) It only affects a single user at a time.

23. What is a zero-click attack?

A) An attack that requires the user to click on a malicious link or attachment

B) An attack that automatically executes without any user interaction

C) An attack that targets zero-day vulnerabilities exclusively.

D) An attack that occurs at exactly midnight (zero hour)

24. What is a social network?

A) A physical gathering of people in a specific location.

B) An online platform that connects individuals or organizations based on common interests or relationships.

C) A network of roads and transportation systems.

D) A financial network for investment and trading.

25. Which of the following is an example of a professional social network?

A) Facebook

B) Instagram

C) Linkedin

D) Snapchat

26. What is a microblogging social network?

A) A network that focuses on sharing short updates or posts.

B) A network for sharing photos and videos

C) A network for professional networking and job searching

D) A network for sharing long-form articles and blog posts.

27. Which type of social network is Characterized by visual content sharing and discovery?

A) Microblogging

B) Professional networking

C) Social media management

D) Visual content sharing

28. What is social media security?

A) Ensuring that social media platforms are free of advertisements

B) Protecting user data, privacy, and accounts from unauthorized access and cyber threats.

C) Preventing the sharing of viral content on social media

D) Enforcing strict posting guidelines on social media platforms.

29. What is the purpose of flagging content on social media platforms?

A) To increase the visibility of the content

B) To mark content as inappropriate or violating community guidelines

C) To automatically delete the content

D) To reward the creator of the content

30. Who typically handles the reports of inappropriate content on social media platforms?

    A) Automated bots

    B) Customer support representatives

    C) Content creators

    D) Community moderators

31. What is a common security measure to enhance social media account security?

    A) Sharing passwords openly on social media platforms

    B) Enabling two-factor authentication (2FA)

    C) Using the same password for multiple social media accounts.

    D) Accepting friend requests from unknown users

32. What is a recommended best practice for maintaining a professional image on social media platforms?

    A) Sharing personal opinions on controversial topics

    B) Using appropriate language and tone in posts and comments

    C) Posting updates without considering privacy settings

    D) Ignoring messages and comments from followers

33. Which of the following is a key aspect of successful social media marketing strategies?

    A) Posting sporadically without a content plan

    B) Ignoring customer feedback and comments

    C) Consistently creating valuable and engaging content

    D) Relying solely on paid advertising without organic efforts

34. What is a key advantage of e-commerce for businesses?

    A) Limited customer reach

    B) Higher operating costs

    C) Global market reach and expanded customer base

    D) Manual order processing only

35. Which of the following is a popular e-commerce website for buying and selling hand made or vintage items.

A) Amazon

B) eBay

C) Etsy

D) Walmart

36. What is an advantage of e-commerce for consumers?

A) Limited product variety

B) Inconvenient payment options

C) 24/7 accessibility and convenience of shopping.

D) Lack of customer reviews and ratings

37. What is a key component of digital payments infrastructure?

A) Cash

B) Cheques

C) Payment gateways

D) In-person transactions

38. Which of the following is a mode of digital payment?

A) Writing a check

B) Swiping a credit card

C) Using a mobile wallet app

D) Exchanging physical currency

39. What is a benefit of using digital wallets for payments?

A) Limited acceptance at merchants

B) Slow transaction processing times

C) Convenient and quick payments using smartphones

D) Higher risk of fraud

NA6S-6109-B-24   (10)

40. What is UPI (Unified Payments Interface)?

   A) A type of physical payment card

   B) An electronic fund transfer system in India

   C) A mobile operating system

   D) A social media platform

41. What is a benefit of using UPI for payments?

   A) Limited compatibility with banks

   B) Higher transaction fees

   C) Instant and seamless fund transfers between bank accounts

   D) Longer processing times

42. What are e-wallets?

   A) Physical wallets used for storing cash

   B) Mobile applications that store digital cash for making payments

   C) Prepaid credit cards

   D) Bank account statements

43. What is Aadhaar Card-enabled payment?

   A) Using Aadhaar Card for identification only

   B) Making payments directly from Aadhaar-linked bank accounts without needing cards or PINs.

   C) Making cash payments at government offices

   D) A type of credit card payment

44. How does biometric authentication enhance security in digital payments?

   A) It makes payments slower and less convenient

   B) It allows for payments without any authentication

   C) It verifies users based on unique physical traits like fingerprints or iris scans

   D) It increases the risk of fraud

45. What is the primary purpose of the Consumer Protection Act?

A) To regulate banking operations in India.

B) To protect consumers from unfair trade practices and ensure their rights.

C) To promote digital payments

D) To regulate stock market transactions.

46. Which regulatory body in India is responsible for implementing guidelines related to digital payments and financial transactions?

A) Securities and Exchange Board of India (SEBI)

B) Reserve Bank of India (RBI)

C) Insurance Regulatory and Development Authority of India (IRDAI)

D) Ministry of Finance

47. What is a recommended practice to enhance mobile phone security?

A) Sharing passwords with friends and family

B) Disabling screen lock and biometric authentication

C) Installing antivirus software from unknown sources

D) Keeping the operating system and apps updated

48. What is the purpose of a strong password policy?

A) To use easily guessable passwords

B) To enforce complex and unique passwords for better security

C) To share passwords openly with colleagues

D) To change passwords only once a year

49. What is a security patch?

A) A type of malware

B) An update that fixes vulnerabilities and improves security

C) A physical security device for phones

D) A software tool for data recovery

NA6S-6109-B-24   (12)

50. How often should security patches be applied to mobile devices?

    A) Once every few years

    B) Only when experiencing security breaches

    C) Regularly and promptly as updates are released by manufacturers.

    D) Only during major software upgrades

51. What is a common risk of not implementing security patch management?

    A) Improved device performance.

    B) Enhanced Security against cyber threats

    C) Increased vulnerability to cyber attacks and exploits

    D) Reduced battery consumption

52. What is the primary function of antivirus software?

    A) Protecting physical devices from theft

    B) Detecting and removing malware and viruses from computers and devices

    C) Improving internet speed

    D) Managing email accounts

53. What is a firewall in the context of computer security?

    A) A physical barrier used to block intruders from entering a building

    B) A software or hardware security system that monitors and controls incoming and outgoing network traffic.

    C) A type of antivirus software

    D) A device used for data encryption

54. Which of the following is a common Wi-Fi security protocol that encrypts data transmitted over wireless networks?

    A) WEP (Wired Equivalent Privacy)

    B) WPS (Wi-Fi Protected Setup)

    C) WPA2 (Wi-Fi Protected Access 2)

    D) SSID (Service Set Identifier)

55. What is a benefit of using a strong Wi-Fi password?

   A) Faster internet speed

   B) Improved device performance

   C) Enhanced protection against unauthorized access and hackers

   D) Lower electricity consumption

56. What is a potential risk of using public Wi-Fi networks without proper security measures?

   A) Increased device battery life

   B) Exposure of sensitive data to hackers anb cybercriminals

   C) Improved network performance

   D) Automatic installation of security patches

57. What is the purpose of configuring basic security policies on a computer network?

   A) To limit access to network resources based on user roles and permissions

   B) To increase internet speed

   C) To disable all security measures for easy access

   D) To install unauthorized software

58. Which of the following is an example of a basic security policy?

   A) Allowing guest users full administrative access to the network

   B) Requiring strong passwords and regular password changes

   C) Sharing sensitive data publicly on social media platforms

   D) Ignoring software updates and security patches

59. What is the purpose of permissions in computer security?

A) To grant access to all users without restrictions

B) To control access to files, folders, and resources based on user roles and privileges.

C) To disable network connectivity

D) To delete all data and files

60. What is a common best practice for configuring permissions on shared folders?

A) Granting read, write, and execute permissions to all users

B) Denying all users access to shared folders

C) Assigning permissions based on the principle of least privilege

D) Automatically sharing all folders without restrictions.

———————