Public Library · FBISE / NBF

Computer Science Grade 12 — Chapter 6

Impacts of Computing

by Public Library

Independent practice MCQs from the supplied Class 12 Computer Science notes pack. Total: 50 questions.

A. Important / Main Topics

1. Security protocols are best defined as:

(A) Rules and procedures to protect data and communication on networks
(B) Types of databases
(C) Programming languages
(D) Types of networks

Correct Answer: A

Explanation: Security protocols are rules and procedures to protect data and communication on networks.

2. What does confidentiality ensure?

(A) Data is accessible to everyone
(B) Data is accessible only to authorized parties
(C) Data is deleted
(D) Data is ignored

Correct Answer: B

Explanation: Confidentiality ensures that data is accessible only to authorized parties.

3. What does data integrity ensure?

(A) Information is changed frequently
(B) Information is deleted
(C) Information remains accurate, consistent, and unaltered
(D) Information is ignored

Correct Answer: C

Explanation: Data integrity ensures that information remains accurate, consistent, and unaltered.

4. What is authentication?

(A) Deleting data
(B) Encrypting data
(C) Storing data
(D) Verifying user or device identities

Correct Answer: D

Explanation: Verifying user or device identities — this correctly answers the question.

5. What is access control?

(A) Deciding who can access, change, or send data
(B) Deleting data
(C) Encrypting data
(D) Storing data

Correct Answer: A

Explanation: Access control decides who can access, change, or send data.

6. What is secure transmission?

(A) Deleting data
(B) Protecting data during transmission
(C) Storing data
(D) Ignoring data

Correct Answer: B

Explanation: Protecting data during transmission — this correctly answers the question.

7. What is data backup and recovery?

(A) Deleting data
(B) Ignoring data
(C) Ensuring data can be restored after loss
(D) Encrypting data

Correct Answer: C

Explanation: Data backup and recovery ensures that data can be brought back if it's lost.

8. What is identity theft?

(A) Sharing personal information with friends
(B) Using someone's personal details with permission
(C) Deleting personal information
(D) Using someone's personal details without permission for fraud

Correct Answer: D

Explanation: Identity theft happens when someone uses your personal details without permission for fraud.

9. Which of the following is a risk of sharing private information?

(A) All of the above
(B) Phishing
(C) Data breaches
(D) Lost or stolen items

Correct Answer: A

Explanation: Phishing, data breaches, and lost or stolen items are all risks of sharing private information.

10. What is phishing?

(A) A type of data breach
(B) Sending fraudulent emails or messages to steal personal information
(C) A type of online scam
(D) A type of lost item

Correct Answer: B

Explanation: Sending fraudulent emails or messages to steal personal information — this correctly answers the question.

11. What is a data breach?

(A) When individuals share data with friends
(B) When data is encrypted
(C) When organizations lose customer data due to cyber attacks
(D) When data is deleted

Correct Answer: C

Explanation: A data breach occurs when organizations or websites are attacked online and lose customer data.

12. Which of the following is a best practice to prevent identity theft?

(A) Share passwords with friends
(B) Ignore financial statements
(C) Use the same password for all accounts
(D) Be careful about sharing personal information

Correct Answer: D

Explanation: Being careful about sharing personal information is a best practice to prevent identity theft.

13. What is a DDoS attack?

(A) Flooding a system with too much traffic
(B) Encrypting files
(C) Stealing information
(D) Deceiving people

Correct Answer: A

Explanation: A DDoS attack floods a system with too much traffic, making it slow or unavailable.

14. What is ransomware?

(A) A type of virus
(B) Malicious software that locks or encrypts files and demands money
(C) A type of spyware
(D) A type of phishing

Correct Answer: B

Explanation: Ransomware is malicious software that locks or encrypts files and demands money to unlock them.

15. What are security methods?

(A) Types of databases
(B) Programming languages
(C) Techniques to protect systems and data from unauthorized access
(D) Types of networks

Correct Answer: C

Explanation: Security methods are techniques and technologies used to protect systems and data from unauthorized access.

16. Why is employee training important for cybersecurity?

(A) It deletes data
(B) It stores data
(C) It ignores security
(D) It helps employees spot phishing attempts

Correct Answer: D

Explanation: It helps employees spot phishing attempts — this correctly answers the question.

17. What does email filtering do?

(A) Catches and blocks phishing emails
(B) Deletes all emails
(C) Stores emails permanently
(D) Ignores emails

Correct Answer: A

Explanation: Catches and blocks phishing emails — this correctly answers the question.

18. What is the purpose of secure communication protocols?

(A) To delete data
(B) To keep communication secure
(C) To store data
(D) To ignore security

Correct Answer: B

Explanation: To keep communication secure — this correctly answers the question.

19. What is web content filtering?

(A) Allowing access to all websites
(B) Deleting websites
(C) Blocking access to known phishing sites
(D) Ignoring websites

Correct Answer: C

Explanation: Blocking access to known phishing sites — this correctly answers the question.

20. Why are security updates important?

(A) They delete data
(B) They store data
(C) They ignore security

(D) They close known vulnerabilities

Correct Answer: D

Explanation: Security updates close known vulnerabilities that attackers could exploit.

21. What is troubleshooting security problems?

(A) Finding and fixing security issues
(B) Deleting data
(C) Storing data
(D) Ignoring security

Correct Answer: A

Explanation: Troubleshooting security problems is the process of finding and fixing security issues to protect systems and apps.

22. What is the first step in troubleshooting security problems?

(A) User education
(B) Identify the issue
(C) Regular backups
(D) Document and learn

Correct Answer: B

Explanation: The first step is to identify the issue.

23. Why is user education important?

(A) It deletes data
(B) It stores data
(C) It prevents human error
(D) It ignores security

Correct Answer: C

Explanation: User education is important because human error is a major cause of security breaches.

24. Why are regular backups important?

(A) They delete data
(B) They ignore security
(C) They store data permanently
(D) They ensure data can be recovered after security incidents

Correct Answer: D

Explanation: Regular backups ensure that data can be recovered if lost due to security problems.

25. Why is security considered an ongoing process?

(A) Because threats evolve constantly
(B) Because security is a one-time task
(C) Because security is not important
(D) Because security is easy

Correct Answer: A

Explanation: Security is an ongoing process because threats evolve constantly, requiring continuous assessment and adjustment.

B. Less Important / Secondary Topics

26. What is a cybersecurity threat?

(A) Any potential danger that could compromise security
(B) A type of database
(C) A programming language
(D) A type of network

Correct Answer: A

Explanation: A cybersecurity threat is any potential danger that could compromise the security of a computer system.

27. Which of the following is a strategy for identifying cybersecurity threats?

(A) Employee training and awareness
(B) All of the above
(C) Email filtering
(D) Web content filtering

Correct Answer: B

Explanation: Employee training, email filtering, and web content filtering are all strategies for identifying cybersecurity threats.

28. What are computational perspectives?

(A) A type of database
(B) A programming language
(C) Using computers to solve problems by breaking down complex tasks
(D) A type of network

Correct Answer: C

Explanation: Using computers to solve problems by breaking down complex tasks — this correctly answers the question.

29. Why are computational perspectives important?

(A) They delete data
(B) They store data
(C) They ignore security
(D) They enhance problem-solving and critical thinking

Correct Answer: D

Explanation: They enhance problem-solving and critical thinking — this correctly answers the question.

30. Which of the following is a key skill in computational perspectives?

(A) All of the above
(B) Decomposition
(C) Pattern recognition
(D) Abstraction

Correct Answer: A

Explanation: Decomposition, pattern recognition, and abstraction are all key skills in computational perspectives.

31. What are computing applications?

(A) Types of databases
(B) Software programs and systems designed to perform specific tasks
(C) Programming languages
(D) Types of networks

Correct Answer: B

Explanation: Computing applications are software programs and systems designed to perform specific tasks.

32. Why is collaboration important in computing application design?

(A) It deletes data
(B) It stores data
(C) It brings together diverse skills and perspectives
(D) It ignores security

Correct Answer: C

Explanation: It brings together diverse skills and perspectives — this correctly answers the question.

33. What are resources for equal information accessibility?

(A) Types of databases
(B) Programming languages
(C) Types of networks
(D) Tools and projects to give everyone equal access to information

Correct Answer: D

Explanation: Resources for equal information accessibility are tools, projects, and initiatives designed to ensure that everyone has equal access to information.

34. What are digital libraries?

(A) Online libraries with free access to educational materials
(B) Physical libraries
(C) Types of databases
(D) Programming languages

Correct Answer: A

Explanation: Digital libraries are online libraries that offer free access to educational materials.

35. What are collaborative tools?

(A) Types of databases
(B) Software applications designed to facilitate teamwork and communication
(C) Programming languages
(D) Types of networks

Correct Answer: B

Explanation: Collaborative tools are software applications designed to facilitate teamwork and communication among individuals.

36. A company wants to protect data during transmission over the internet. Which protocol is most appropriate?

(A) HTTP
(B) FTP
(C) HTTPS
(D) SMTP

Correct Answer: C

Explanation: HTTPS uses TLS/SSL to secure data during transmission over the internet.

37. A company wants to secure communication between remote offices using a VPN. Which protocol is most appropriate?

(A) HTTP
(B) FTP
(C) SMTP
(D) IPsec

Correct Answer: D

Explanation: IPsec is a set of protocols that secure IP communication and is often used for VPNs.

38. A company wants to ensure that data remains unchanged during transmission. Which security objective is most relevant?

(A) Integrity
(B) Confidentiality
(C) Availability
(D) Usability

Correct Answer: A

Explanation: Integrity ensures that data remains unchanged during transmission, storage, and processing.

39. A company wants to prevent unauthorized access to its systems. Which security objective is most relevant?

(A) Integrity
(B) Confidentiality
(C) Availability
(D) Usability

Correct Answer: B

Explanation: Confidentiality ensures that data is accessible only to authorized parties, preventing unauthorized access.

40. A company wants to ensure that its systems are available when needed. Which security objective is most relevant?

(A) Integrity
(B) Confidentiality
(C) Availability
(D) Usability

Correct Answer: C

Explanation: Availability ensures that systems and data are accessible and usable when needed.

41. A user wants to protect their account with two forms of identification. Which security method is most appropriate?

(A) Single-factor authentication
(B) Password only
(C) PIN only
(D) Two-factor authentication (2FA)

Correct Answer: D

Explanation: Two-factor authentication (2FA) — this correctly answers the question.

42. A company wants to use unique physical traits for identification. Which security method is most appropriate?

(A) Biometric verification
(B) Password authentication
(C) PIN authentication
(D) Token authentication

Correct Answer: A

Explanation: Biometric verification uses unique physical traits like fingerprints or face scans for identification.

43. A company wants to ensure that data remains private during transmission. Which technique is most appropriate?

(A) Decryption
(B) Encryption
(C) Compression
(D) Duplication

Correct Answer: B

Explanation: Encryption converts plaintext to ciphertext, ensuring that data remains private during transmission.

44. A company uses symmetric cryptography for bulk data encryption. What is the main advantage?

(A) It uses two keys
(B) It is slower than asymmetric cryptography
(C) It is fast and efficient for large data volumes
(D) It requires no key

Correct Answer: C

Explanation: Symmetric cryptography is fast and efficient for large data volumes because it uses the same key for encryption and decryption.

45. A company uses asymmetric cryptography for key exchange. What is the main advantage?

(A) It is faster than symmetric cryptography
(B) It uses the same key for encryption and decryption
(C) It requires no key
(D) It solves the key distribution problem

Correct Answer: D

Explanation: Asymmetric cryptography uses a public key for encryption and a private key for decryption, solving the key distribution problem.

46. A company wants to protect against DDoS attacks. Which measure is most appropriate?

(A) Traffic filtering and load balancing
(B) Ignoring the attack
(C) Sharing passwords
(D) Disabling security

Correct Answer: A

Explanation: Traffic filtering and load balancing — this correctly answers the question.

47. A company wants to protect against ransomware. Which measure is most appropriate?

(A) Ignoring the attack
(B) Regular backups
(C) Sharing passwords
(D) Disabling security

Correct Answer: B

Explanation: Regular backups ensure that data can be recovered if a ransomware attack occurs.

48. A company wants to protect against spyware. Which measure is most appropriate?

(A) Ignoring the attack
(B) Sharing passwords
(C) Anti-spyware tools and cautious downloading
(D) Disabling security

Correct Answer: C

Explanation: Anti-spyware tools and cautious downloading help prevent spyware from infecting systems.

49. A company wants to protect against phishing. Which measure is most appropriate?

(A) Ignoring the attack
(B) Sharing passwords
(C) Disabling security
(D) Awareness training and email filtering

Correct Answer: D

Explanation: Awareness training and email filtering — this correctly answers the question.

50. A company wants to protect against viruses. Which measure is most appropriate?

(A) Antivirus software and safe browsing
(B) Ignoring the attack
(C) Sharing passwords
(D) Disabling security

Correct Answer: A

Explanation: Antivirus software and safe browsing help prevent viruses from infecting systems.