1. What is the main purpose of information security?

   a) To increase computer speed

   b) To protect information from theft, corruption, or disaster while keeping it accessible

   c) To reduce hardware costs

   d) To improve software design

2. Which of the following is NOT an objective of information security?

   a) Confidentiality

   b) Integrity

   c) Availability

   d) Duplication

3. What is a "threat" in computer security?

   a) A security mechanism

   b) A potential violation of security

   c) A type of antivirus

   d) A backup procedure

4. Which term refers to a vulnerability that has been exploited to cause harm?

   a) Risk

   b) Attack

   c) Threat

   d) Ethics

5. What does "non-repudiation" ensure?

   a) Data is encrypted

   b) Messages are from the claimed sender and unaltered

   c) Data is always available

   d) Passwords are strong

6. Which of these is a common source of security breaches?

   a) Firewall

   b) Encryption

   c) Employee misconduct

   d) Antivirus software

7. What is a "hacker" in the context of security?

   a) Only someone who breaks into systems illegally

   b) Only someone skilled in programming

   c) Someone who gains unauthorized access to a system

   d) Someone who designs security software

8. What is the purpose of a firewall?

   a) To encrypt data

   b) To back up files

   c) To filter and block unauthorized network traffic

   d) To create audit logs

9. Which of the following is a method to protect against data loss?

   a) Using strong passwords

   b) Regular data backups

   c) Installing antivirus software

   d) Using encryption

10. What does "integrity" in information security ensure?

   a) Data is kept secret

   b) Data is accurate and unaltered

   c) Data is always available

   d) Data is encrypted

11. Which security objective ensures data is accessible to authorized users?

    a) Confidentiality

    b) Integrity

    c) Availability

    d) Non-repudiation

12. What is "cyber terrorism"?

    a) Stealing personal data

    b) Politically motivated attacks on computer systems

    c) Creating computer viruses

    d) Unauthorized access to emails

13. Which of the following is a result of a security breach?

    a) Improved system performance

    b) Denial of services

    c) Increased data availability

    d) Enhanced user privacy

14. What is the primary function of antivirus software?

    a) To block network intruders

    b) To encrypt files

    c) To detect and remove malicious software

    d) To create secure passwords

15. Which of the following is a rule for creating secure passwords?

    a) Use your name

    b) Use a mix of letters and numbers

    c) Keep it short

    d) Use your phone number

16. What is the purpose of an audit log?

    a) To encrypt data transmissions

    b) To back up system files

    c) To record system events and user activities

    d) To block unauthorized access

17. Which of the following is a reliability measure for IT systems?

    a) Strong passwords

    b) Uninterruptible Power Supply (UPS)

    c) Firewalls

    d) Data encryption

18. What is a "fault-tolerant computer"?

    a) A computer that never fails

    b) A computer with duplicate components to ensure reliability

    c) A computer with strong encryption

    d) A computer used only for backups

19. Which of the following is a quality-of-life issue related to IT?

    a) Increased productivity

    b) Social isolation

    c) Faster internet speeds

    d) Better job opportunities

20. What is digital piracy?

    a) Creating original software

    b) Illegal copying of digital products

    c) Protecting software with copyright

    d) Licensing software legally

21. Which of the following is a method to prevent software piracy?

   a) Using strong passwords

   b) Software site licensing

   c) Installing firewalls

   d) Data encryption

22. What is the ethical question to ask before developing an IT system?

   a) "Can IT do this?"

   b) "Should IT do this?"

   c) "How fast can IT do this?"

   d) "Who will use IT?"

23. Which of the following is an economic issue related to IT?

   a) Improved communication

   b) Widening gap between rich and poor

   c) Faster data processing

   d) Better entertainment options

24. What is "information overload"?

   a) Lack of information

   b) Too much information to process effectively

   c) Encrypted information

   d) Stolen information

25. Which of the following is an environmental issue related to IT?

   a) Social isolation

   b) Toxic waste from computer disposal

   c) Software piracy

   d) Unauthorized access

26. What is the purpose of hardening an IT resource?

   a) To make it run faster

   b) To make it more secure against attacks

   c) To reduce its cost

   d) To make it easier to use

27. Which security measure helps protect against data interception?

   a) Strong passwords

   b) Data encryption

   c) Antivirus software

   d) Audit logs

28. What is a "security program"?

   a) A type of antivirus software

   b) Policies and measures to protect IT assets

   c) A backup procedure

   d) A type of encryption

29. What does "ethics" refer to in IT?

   a) Technical skills

   b) Moral principles and behavior

   c) System performance

   d) Security measures

30. Which of the following is a principle area of security?

   a) User training

   b) Network security

   c) Data entry

   d) Software development