⍰ EASY (Q1–Q10)

Q1. Protecting information system security primarily aims to:
A. Increase system speed
B. Protect data and services
C. Reduce hardware cost
D. Improve UI design

Q2. Which security control prevents attacks before they occur?
A. Detective
B. Corrective
C. Preventive
D. Administrative

Q3. Firewalls are mainly used to:
A. Encrypt data
B. Control network traffic
C. Detect malware
D. Manage users

Q4. IDS stands for:
A. Internet Defense System
B. Intrusion Detection System
C. Information Data Security
D. Internal Defense Software

Q5. Mobile security primarily focuses on protecting:
A. Mobile towers
B. Mobile devices and data
C. SIM cards only
D. Network cables

Q6. Wireless communication is more vulnerable because it uses:
A. Wired media
B. Optical fiber
C. Radio waves
D. Copper cables

Q7. WPA is related to:
A. Web security
B. Wireless security
C. Database security
D. Physical security

Q8. Credit card fraud involves:
A. Network slowdown
B. Unauthorized financial transactions
C. Hardware theft
D. Data backup

Q9. Information Security Management focuses on:
A. Malware development
B. Governance and risk management
C. Programming
D. System upgrades

Q10. AAA in security stands for:
A. Access, Authorization, Availability
B. Authentication, Authorization, Accounting
C. Audit, Access, Authentication
D. Availability, Access, Accountability

□ MEDIUM (Q11–Q25)

Q11. Detective controls are used to:
A. Prevent attacks
B. Detect security incidents
C. Recover systems
D. Encrypt data

Q12. Which device filters traffic based on predefined rules?
A. IDS
B. Firewall
C. Antivirus
D. Proxy

Q13. Mobile devices are at higher risk because they are:
A. Less powerful
B. Always connected
C. Hard to use
D. Expensive

Q14. Wireless attacks often exploit:
A. Encryption protocols
B. Broadcast nature of wireless media
C. Physical security
D. Hardware limitations

Q15. VPNs are used in mobile security to:
A. Increase speed
B. Secure data transmission
C. Detect malware
D. Manage users

Q16. Credit card skimming involves:
A. Encrypting card data
B. Capturing card details illegally
C. Blocking transactions
D. Verifying identity

Q17. Which fraud uses fake websites or apps?
A. Skimming
B. Phishing
C. Shoulder surfing
D. Physical theft

Q18. ISMS helps organizations to:
A. Write programs
B. Manage security risks
C. Increase bandwidth
D. Install antivirus

Q19. Risk management lifecycle includes:
A. Risk identification
B. Risk analysis
C. Risk treatment
D. All of the above

Q20. Which protocol secures wireless networks?
A. FTP
B. WPA3
C. HTTP
D. Telnet

Q21. Mobile malware often spreads through:
A. BIOS updates
B. App installations
C. CPU registers
D. Hardware faults

Q22. Encryption ensures which security objective?
A. Availability
B. Integrity
C. Confidentiality
D. Accountability

Q23. Which attack targets wireless networks by impersonation?
A. DoS
B. Spoofing
C. SQL Injection
D. Buffer Overflow

Q24. Information security audits help to:
A. Detect malware
B. Ensure policy compliance
C. Improve UI
D. Increase speed

Q25. Which wireless feature allows device management?
A. WPA
B. MDM
C. IDS
D. IPS

🔴 HARD (Q26–Q40)

Q26. Preventive controls reduce risk by:
A. Detecting incidents
B. Limiting attack surface
C. Recovering systems
D. Logging events

Q27. Wireless security protocols evolved to address:
A. Physical theft
B. Eavesdropping and spoofing
C. Hardware failure
D. User interface issues

Q28. Credit card fraud in mobile environments often exploits:
A. Weak encryption and user trust
B. Hardware damage
C. Power failure
D. Network congestion

Q29. IDS differs from IPS because IDS:
A. Blocks traffic
B. Detects and alerts only
C. Encrypts packets
D. Controls access

Q30. Information Security Management aligns security with:
A. Hardware capability
B. Business objectives
C. Software versions
D. User preferences

Q31. Mobile Device Management (MDM) enables:
A. Malware creation
B. Centralized device control
C. Network routing
D. Packet sniffing

Q32. Wireless attacks are harder to trace because:
A. They use malware
B. Attackers remain anonymous
C. Traffic is encrypted
D. They crash systems

Q33. Corrective controls focus on:
A. Prevention
B. Detection
C. Recovery
D. Authorization

Q34. Credit card fraud detection relies heavily on:
A. User training
B. Transaction monitoring
C. Encryption only
D. Firewalls

Q35. Strong authentication reduces risk of:
A. DoS attacks
B. Unauthorized access
C. Hardware failure
D. Data backup

Q36. Which security principle limits damage from compromised accounts?
A. Least privilege
B. Defense-in-depth
C. Encryption
D. Availability

Q37. Mobile security policies define:
A. Programming standards
B. Acceptable device usage
C. Hardware configuration
D. Network topology

Q38. Wireless intrusion detection monitors:
A. Wired traffic
B. Radio frequency traffic
C. CPU usage
D. Disk space

Q39. Credit card fraud has high impact due to:
A. Physical damage
B. Financial loss and trust erosion
C. System downtime
D. Performance issues

Q40. ISMS effectiveness is measured through:
A. Number of tools
B. Compliance and audits
C. Hardware upgrades
D. Network speed