Biyani's Think Tank

Concept based notes

INTRODUCTION TO CYBER SECURITY

(BCOM 4th Semester (P+H), BBA 4th Semester, BVA 4th Semester and BA 4th Semester)

Ms. Giti Vatsa

Department of Commerce & Management

Biyani Girls College, Jaipur

Published by:

Think Tanks

Biyani Group of Colleges

Concept & Copyright:

BiyaniShikshanSamitiSector-3, Vidhyadhar Nagar, Jaipur-302023(Rajasthan)

Ph : 0141-2338371,2338591-95 Fax:0141-2338007

E-mail:acad@biyanicolleges.org

Website:www.gurukpo.com;www.biyanicolleges.org

ISBN:-978–93–83343–11–9

Edition: 2025

While every effort is taken to avoid errors or omissions in this Publication, any mistake or omission that may have crept is not intentional. It may be taken note of that neither the publisher nor the author will be responsible for any damage or loss of any kind arising to anyone in any manner on account of such errors and omissions.

Leaser Type Setted by:

Biyani College Printing Department

Preface

I am glad to present this book, especially designed to serve the need soft he students. The book has been written keeping in mind the general weakness in understanding the fundamental concepts of the topics. The book is self- explanatory and adopts the "Teach Yourself" style. It is based on question- answer pattern. The language of book is quite easy and understandable based on scientific approach.

Any further improvement in the contents of the book by making corrections, omission and inclusion is keen to be achieved based on suggestions from the readers for which the author shall be obliged.

I acknowledge special thanks to Mr. Rajeev Biyani, *Chairman* & Dr. Sanjay Biyani, *Director*(*Acad.*) Biyani Group of Colleges, who are the backbones and main concept provider and also have been constant source of motivation throughout this Endeavour. They played an active role in coordinating the various stages of this Endeavour and spearheaded the publishing work.

I look forward to receiving valuable suggestions from professors of various educational institutions, other faculty members and students for improvement of the quality of the book. The reader may feel free to send in their comments and suggestions to the under mentioned address.

Author

□□□

Syllabus

UNIT 1:

Introduction to Cyber Space, History of Internet, Cyber Crime, Information Security, Computer Ethics and Security Policies, email security, securing web browser, Antivirus, Guidelines for secure password and Wi-Fi security, Guidelines for setting up a Secure password, Two-steps authentication, Password Manager

UNIT II:

Guidelines for basic Windows security, Guidelines for social media security, Tips and best practices for safer Social Networking, User Account Password, Smartphone security guidelines, Online Banking, Credit Card and UPI Security, Online Banking Security, Mobile Banking Security, Security of Debit and Credit Card, POS Security, Security of Micro ATMs, e-wallet Security Guidelines

UNIT III:

Social Engineering, Types of Social Engineering, How Cyber Criminal Works, how to prevent for being a victim of Cybercrime, Cyber Security Threat Landscape and Techniques, Emerging Cyber Security Threats, Cyber Security Techniques, Firewall

UNIT IV:

Cyber Security Initiatives in India, Cyber Security Incident Handling, Cyber Security Assurance, IT Security Act, Hackers-Attacker-Countermeasures, Web Application Security, Digital Infrastructure Security, Defensive Programming, Information Destroying and Recovery Tools, Destroying Sensitive Information

UNIT I:

Multiple Type questions:

1. What is the term 'cyberspace' commonly used to refer to?
A. Virtual computer world
B. A type of hardware
C. A local server
D. None of the above
Answer: Virtual computer world

2. Which of the following is not part of cyberspace?
A. Social media
B. Physical computers
C. Websites
D. Online databases
Answer: Physical computers

3. Which organization is credited with the invention of the internet?
A. NASA
B. DARPA
C. IBM
D. Google
Answer: DARPA

4. In which decade was the internet first developed?
A. 1950s
B. 1960s
C. 1970s
D. 1980s
Answer: 1960s

5. Which of the following is an example of cyber crime?
A. Phishing
B. Robbery
C. Burglary
D. Kidnapping
Answer: Phishing

6. Identity theft is a type of:
A. Physical crime

B. Cyber crime
C. Property crime
D. Natural disaster
Answer: Cyber crime

7. The main goal of information security is to protect:
A. Software only
B. Hardware only
C. Data and systems
D. Network cables
Answer: Data and systems

8. Which of these is not a component of information security?
A. Confidentiality
B. Integrity
C. Availability
D. Profitability
Answer: Profitability

9. Computer ethics deal with:
A. Legal use of software
B. Computer games
C. Hardware repair
D. Typing speed
Answer: Legal use of software

10. Which of the following is considered unethical in computing?
A. Creating backups
B. Hacking
C. Using antivirus
D. Installing updates
Answer: Hacking

11. Security policies help organizations to:
A. Reduce internet speed
B. Enhance data protection
C. Build computers
D. Train animals
Answer: Enhance data protection

12. A good security policy should be:
A. Vague
B. Difficult
C. Clear and enforceable
D. None of the above
Answer: Clear and enforceable

13. Which of the following helps protect email accounts?
A. Strong password
B. Public Wi-Fi
C. Open ports
D. Cookies
Answer: Strong password

14. Phishing emails typically try to:
A. Provide offers
B. Steal personal information
C. Improve productivity
D. Clean your inbox
Answer: Steal personal information

15. Which one is a secure web browser setting?
A. Disabling pop-up blocker
B. Allowing all cookies
C. Using HTTPS
D. Saving all passwords
Answer: Using HTTPS

16. Cookies can sometimes be a threat to:
A. Your internet connection
B. Web design
C. Online privacy
D. Wi-Fi signal
Answer: Online privacy

17. The purpose of antivirus software is to:
A. Play music
B. Scan for viruses
C. Create backups
D. Increase brightness

Answer: Scan for viruses

18. Which of these is not a function of antivirus software?
A. Virus detection
B. Virus removal
C. Gaming
D. Real-time protection
Answer: Gaming

19. A secure password should include:
A. Your name
B. Common words
C. Letters, numbers, symbols
D. Only numbers
Answer: Letters, numbers, symbols

20. Changing passwords regularly helps in:
A. Wasting time
B. Increasing risk
C. Improving security
D. Slowing performance
Answer: Improving security

21. Which encryption method is most secure for Wi-Fi?
A. WEP
B. WPA
C. WPA2
D. Open
Answer: WPA2

22. Default router passwords should be:
A. Kept
B. Changed
C. Shared
D. Ignored
Answer: Changed

23. Two-step authentication increases security by requiring:
A. One password
B. A captcha

C. Two different verifications
D. Nothing extra
Answer: Two different verifications

24. Which is an example of two-step authentication?
A. Password only
B. Fingerprint and password
C. Username only
D. Secret question only
Answer: Fingerprint and password

25. A password manager helps to:
A. Forget passwords
B. Remember and store passwords securely
C. Hack passwords
D. Avoid passwords
Answer: Remember and store passwords securely

26. Which of these is a benefit of using a password manager?
A. Weaker passwords
B. One password for all
C. Secure storage of many passwords
D. Sharing passwords with friends
Answer: Secure storage of many passwords

27. Which of the following is NOT a type of cyber crime?
A. Identity theft
B. Phishing
C. Firewall installation
D. Ransomware attack
Answer: C

28. The first version of the internet, known as ARPANET, was developed in:
A. 1969
B. 1983
C. 1995
D. 2001
Answer: A

29. Which of the following is an example of a strong password?
A. 12345678
B. password123
C. G@rb!Tx7L

D. Qwerty
Answer: C

30. What is the primary function of a password manager?
A. Encrypt emails
B. Create and store secure passwords
C. Monitor web traffic
D. Update antivirus software
Answer: B

31. Which of these protocols is considered secure for websites?
A. HTTP
B. FTP
C. HTTPS
D. IPX
Answer: C

32. Which of the following is a common technique used in cyber crime?
A. Data encryption
B. Social engineering
C. Software patching
D. Network segmentation
Answer: B

33. Which of the following is NOT a recommended method to secure your email?
A. Enabling spam filters
B. Using two-factor authentication
C. Sharing your email password with trusted friends
D. Avoiding clicking on suspicious links
Answer: C

34. The process of converting data into a coded format to prevent unauthorized access is called:
A. Hacking
B. Decryption
C. Encryption
D. Spamming
Answer: C

35. Which of the following is a characteristic of ethical computer use?
A. Spamming users with advertisements
B. Accessing someone else's computer without permission

C. Respecting privacy and intellectual property
D. Installing malicious software
Answer: C

36. What is the purpose of security policies in an organization?
A. To restrict internet usage
B. To define rules for secure operations and protect assets
C. To train hackers
D. To reduce software performance
Answer: B

37. Which of the following is a correct example of a secure Wi-Fi setup?
A. Open network with no password
B. WEP encryption with a short password
C. WPA3 encryption with a strong password
D. Default SSID with factory settings
Answer: C

38. What is one major benefit of using Two-Factor Authentication (2FA)?
A. Increases login time
B. Reduces need for passwords
C. Adds an extra layer of security
D. Makes systems more expensive
Answer: C

39. A secure password should be all of the following EXCEPT:
A. Easy to guess
B. Long
C. Complex
D. Unique
Answer: A

40. Which of the following is considered a *preventive* information security measure?
A. Investigating a data breach
B. Installing antivirus software
C. Recovering deleted files
D. Reporting phishing emails after clicking
Answer: B

41. A firewall primarily helps in:
A. Generating secure passwords

B. Preventing unauthorized access to or from a private network

C. Encrypting email messages

D. Detecting hardware issues

Answer: B

42. What does 'cyberspace' primarily refer to?
A) Physical location of computer servers
B) The tangible hardware of the internet
C) A virtual environment created by interconnected digital devices
D) An online shopping platform
Answer: C

43. Which of the following is considered the beginning of the modern internet?
A) The invention of the World Wide Web in 1991
B) The launch of Facebook
C) The development of ARPANET in the late 1960s
D) The release of Windows 95
Answer: C

44. Which of the following is not a type of cybercrime?
A) Phishing
B) Identity theft
C) ATM withdrawal
D) Ransomware attack
Answer: C

45. Information security focuses primarily on:
A) Speed of internet
B) Protecting data and systems from unauthorized access
C) Increasing software features
D) Designing websites
Answer: B

46. Which of the following is not part of computer ethics?
A) Respecting intellectual property
B) Promoting privacy rights
C) Hacking for fun
D) Avoiding plagiarism
Answer: C

47. A security policy typically outlines:
A) Software usage guidelines
B) Steps for creating websites
C) Rules and procedures to protect an organization’s information assets
D) Marketing strategies for security products
Answer: C

48. What is the most common method for ensuring email security?
A) Sending email in plain text
B) Using CAPTCHA
C) Using end-to-end encryption
D) Forwarding emails to multiple users
Answer: C

49. Which of the following can secure your web browser?
A) Installing browser toolbars
B) Disabling pop-up blockers
C) Keeping your browser and plugins updated
D) Avoiding ad blockers
Answer: C

50. The primary function of antivirus software is to:
A) Improve internet speed
B) Block email spam
C) Detect and remove malicious software
D) Design web applications
Answer: C

51. Which of the following is a good practice for creating a secure password?
A) Use your birth date
B) Use “password123”
C) Use a mix of uppercase, lowercase, numbers, and symbols
D) Repeat the same password across all accounts
Answer: C

52. Which of the following enhances Wi-Fi security?
A) Disabling WPA encryption
B) Changing the default router password
C) Leaving the network name unchanged
D) Using WEP instead of WPA2
Answer: B

53. Two-step authentication adds:
A) A duplicate password
B) An additional layer of security using a second factor (like OTP)
C) An extra username
D) Email verification only
Answer: B

54. A password manager helps users by:
A) Storing usernames only
B) Creating and managing complex passwords
C) Hacking into systems

D) Sharing passwords publicly
Answer: B

55. Which of the following is a benefit of using a password manager?
A) It sends your passwords to friends
B) It allows easy reuse of passwords
C) It helps generate and store strong, unique passwords
D) It reduces browser performance
Answer: C

56. What does HTTPS in a web address indicate?
A) The website is under maintenance
B) The website is optimized for speed
C) The connection is secured using SSL/TLS encryption
D) The site uses cookies
Answer: C

57. Which of the following is least secure for online authentication?
A) Biometric verification
B) Two-factor authentication
C) Password-only login
D) OTP-based login
Answer: C

58. A phishing attack aims to:
A) Improve email marketing
B) Secure web browsers
C) Trick users into giving up confidential information
D) Speed up system performance
Answer: C

59. Which of the following is not an example of malware?
A) Trojan horse
B) Worm
C) Firewall
D) Ransomware
Answer: C

60. The act of monitoring and analyzing network traffic for malicious activity is called:
A) Data mining
B) Intrusion Detection
C) Cloud computing
D) Web scraping
Answer: B

61. What is the most secure type of Wi-Fi encryption currently available for home networks?
A) WEP
B) WPA
C) WPA2
D) WPA3
Answer: D

62. A strong password should ideally be:
A) Short and easy to remember
B) Reused across multiple accounts
C) A mix of letters, numbers, and special characters
D) Based on your pet's name
Answer: C

63. Why is using the same password across multiple sites risky?
A) It improves system speed
B) It helps remember passwords easily
C) If one site is compromised, all accounts can be accessed
D) It requires no maintenance
Answer: C

64. What is a brute-force attack?
A) Sending spam emails repeatedly
B) Guessing passwords by trying all combinations
C) Physically damaging a server
D) Deleting system files
Answer: B

65. Which of the following best describes two-factor authentication (2FA)?
A) Login with a username and PIN only
B) Using fingerprint or retina scan alone
C) A combination of something you know and something you have
D) Using two passwords
Answer: C

66. Which of the following is a recommended way to protect sensitive information while using public Wi-Fi?
A) Disable firewall
B) Use a Virtual Private Network (VPN)
C) Share login details
D) Keep all apps running
Answer: B

67. Which of these statements about antivirus software is false?
A) It can help detect and remove spyware

B) It guarantees 100% protection against all cyber threats
C) It should be updated regularly
D) It can scan for malware in email attachments
Answer: B

68. A secure password reset process should include:
A) Simple questions like "What is your name?"
B) Sending the password to any email
C) Identity verification through secondary means (e.g., OTP, email link)
D) Immediate access without verification
Answer: C

70. What is the role of security patches in software?
A) Decrease performance
B) Add new features only
C) Fix vulnerabilities and improve protection
D) Slow down virus scanning
Answer: C

UNIT II:

Q1. Which of the following is a basic Windows security best practice?
A. Disabling automatic updates
B. Avoiding use of antivirus
C. Keeping Windows and software up to date
D. Using the same password for all accounts
Answer: C

Q2. Which of the following is recommended for securing your social media accounts?
A. Using public Wi-Fi to post updates
B. Sharing login credentials with friends
C. Enabling two-factor authentication
D. Keeping your profile public
Answer: C

Q3. What is a *safe* social networking tip?
A. Accepting friend requests from unknown people
B. Clicking on suspicious links
C. Avoiding oversharing personal information
D. Posting travel plans publicly
Answer: C

Q4. Which of the following is a **strong user account password** practice on Windows?
A. Using "admin123" as your password
B. Leaving the password blank
C. Using a long, complex password with numbers and symbols
D. Using your birthdate
Answer: C

Q5. What is a **smartphone security** best practice?
A. Disabling screen lock
B. Installing apps from unknown sources
C. Regularly updating the operating system
D. Ignoring software updates
Answer: C

Q6. Which of the following is the most secure way to access your online bank account?
A. Using public Wi-Fi at a coffee shop
B. Saving passwords on shared computers
C. Using a private device with up-to-date antivirus
D. Sharing OTPs with friends
Answer: C

Q7. What should you avoid to protect your **credit/debit card information**?
A. Monitoring statements regularly
B. Entering card details on suspicious websites
C. Reporting lost/stolen cards promptly
D. Using secure ATMs
Answer: B

Q8. Which of the following actions helps ensure **POS (Point of Sale) security**?
A. Letting the cashier take your card out of sight
B. Covering the keypad while entering your PIN
C. Leaving your receipt at the counter
D. Using cards with magnetic stripes only
Answer: B

Q9. Which of the following ensures **e-wallet security**?
A. Using same password across all wallets
B. Not setting a screen lock on your phone
C. Linking wallet to an expired credit card
D. Enabling transaction alerts and using secure PIN
Answer: D

Q10. A key recommendation for **UPI security** is:
A. Sharing your UPI PIN with the merchant
B. Using UPI only on rooted/jailbroken devices
C. Verifying UPI apps from official sources
D. Allowing access to all device permissions
Answer: C

Q11. Which of the following is **NOT** a recommended **mobile banking** practice?
A. Logging out after transactions
B. Installing apps from third-party app stores
C. Using official banking apps
D. Keeping apps updated
Answer: B

Q12. What helps in protecting **Micro ATM transactions**?
A. Using the same PIN for all cards
B. Allowing unverified agents to operate it
C. Ensuring biometric authentication is securely handled
D. Ignoring transaction receipts
Answer: C

Q13. Which of the following is the most secure way to keep your Windows operating system safe?
A. Disable Windows Firewall
B. Avoid installing updates
C. Regularly update Windows and install security patches
D. Use an outdated antivirus software
Answer: C

Q14. What is the purpose of User Account Control (UAC) in Windows?
A. To monitor system performance
B. To block internet access
C. To alert when a program tries to make system changes
D. To enhance gaming performance
Answer: C

Q15. Which of the following is a good practice for social media security?
A. Accepting friend requests from strangers
B. Sharing your password with friends
C. Regularly updating privacy settings

D. Posting real-time location frequently
Answer: C

Q16. Which is the safest way to handle suspicious links on social networking sites?
A. Click to see what it is
B. Forward it to friends
C. Ignore or report the link
D. Bookmark it for later
Answer: C

Q17. Which of the following passwords is the most secure?
A. 123456
B. John1985
C. Pa$$w0rd!2025
D. mypassword
Answer: C

Q18. How often should you change your passwords for critical accounts?
A. Every 5 years
B. Only when hacked
C. Every 3–6 months
D. Never
Answer: C

Q19. Which of these practices enhances smartphone security?
A. Installing apps from unknown sources
B. Disabling automatic updates
C. Using strong screen lock and enabling device encryption
D. Keeping Bluetooth always on
Answer: C

Q20. Why should you avoid using public Wi-Fi for financial transactions?
A. It drains your battery
B. It’s slower
C. It can be insecure and lead to data theft
D. It’s too expensive
Answer: C

Q21. What is the best practice for secure online banking?
A. Save passwords in browser
B. Use incognito mode without logging out

C. Use two-factor authentication
D. Share OTP with bank executive
Answer: C

Q22. Which of these actions ensures UPI security?
A. Sharing UPI PIN over the phone
B. Using UPI apps from trusted sources only
C. Clicking on links in SMS to make payments
D. Keeping screen lock disabled
Answer: B

Q23. What should you do if your debit/credit card is lost or stolen?
A. Wait and search for it later
B. Ignore it if you don't use it often
C. Report and block the card immediately
D. Post about it on social media
Answer: C

Q24. While using POS machines, which of the following should be practiced?
A. Allow cashier to swipe card out of sight
B. Always use chip-based cards and shield PIN entry
C. Sign blank slips
D. Share your card details with the attendant
Answer: B

Q25. How can you secure transactions at Micro ATMs?
A. Disclose PIN to the operator
B. Demand printed receipt and verify transaction
C. Swipe multiple times for speed
D. Use any card lying around
Answer: B

Q26. Which is a safe e-wallet practice?
A. Using the same PIN for all apps
B. Clicking on wallet links in unknown messages
C. Downloading apps from official stores only
D. Storing PIN in notes app
Answer: C

Q27. What is the most common method fraudsters use to trick e-wallet users?
A. Offering legitimate cash-back
B. Calling from official numbers
C. Phishing through links and fake support calls
D. Sending receipts only
Answer: C

Q28. Which of the following is a basic Windows security measure?
A. Turning off Windows Firewall
B. Disabling automatic updates
C. Installing antivirus software and keeping it updated
D. Using the same password for all accounts
Answer: C

Q29. What is the best practice for keeping your social media accounts secure?
A. Accepting all friend requests
B. Sharing personal details publicly
C. Enabling two-factor authentication
D. Using the same password across platforms
Answer: C

Q30. Which of the following is NOT a safe social networking tip?
A. Reviewing privacy settings
B. Posting vacation plans in real-time
C. Using strong passwords
D. Avoiding clicking unknown links
Answer: B

Q31. Which of the following is a strong password?
A. 12345678
B. MyName123
C. !Q2w#E4r%T6y
D. Password123
Answer: C

Q32. To secure your smartphone, you should:
A. Download apps from unknown sources
B. Disable screen lock
C. Keep the OS and apps updated
D. Share your phone password with friends
Answer: C

Q33. Which is a safe online banking practice?
A. Logging in from public Wi-Fi
B. Saving passwords in browser

C. Using bank’s official app or website
D. Sharing OTP with customer care
Answer: C

Q34. How can you protect your UPI transactions?
A. Share UPI PIN with trusted people
B. Use secure apps from verified sources
C. Keep your UPI app open all the time
D. Disable phone lock for easy access
Answer: B

Q35. Which of the following actions enhances mobile banking security?
A. Ignoring app updates
B. Using biometric authentication
C. Sharing banking details via SMS
D. Using rooted/jailbroken devices
Answer: B

Q36. To prevent unauthorized card transactions, you should:
A. Share card CVV with close friends
B. Write PIN on the back of the card
C. Enable transaction alerts
D. Use the card on untrusted websites
Answer: C

Q37. When using a POS terminal, which practice is safest?
A. Allowing the cashier to swipe the card privately
B. Covering the keypad when entering your PIN
C. Using outdated cards
D. Entering card details loudly
Answer: B

Q38. What should you do when using a Micro ATM?
A. Ignore transaction receipt
B. Share your Aadhaar OTP with the agent
C. Confirm the device is authentic and secure
D. Use someone else’s fingerprint
Answer: C

Q39. How can you improve the security of your e-wallet?
A. Use weak passwords
B. Disable screen lock
C. Link it to public 5WI-Fi
D. Set transaction limits and enable app lock
Answer: D

Q40. Which of the following is essential for keeping a Windows system secure?

A. Disabling user account control

B. Using an outdated antivirus

C. Creating standard user accounts for regular use

D. Turning off automatic updates

Answer: C

UNIT III:

Q1. What is social engineering in cybersecurity?

A. Designing computer systems

B. Manipulating people to gain confidential information

C. Encrypting sensitive data

D. Programming ethical hacking tools

Answer: B

Q2. Which of the following is NOT a type of social engineering attack?

A. Phishing

B. Pretexting

C. Baiting

D. SQL Injection

Answer: D

Q3. In which social engineering attack does an attacker leave a malware-infected USB drive for someone to find?

A. Pretexting

B. Baiting

C. Tailgating

D. Phishing

Answer: B

Q4. Tailgating refers to:

A. Following someone on social media

B. Gaining access by entering a restricted area behind someone without permission

C. Sending fraudulent emails

D. Leaving a fake website for users to click

Answer: B

Q5. What is the first phase in a typical cyber-attack?

A. Exfiltration

B. Exploitation

C. Reconnaissance

D. Encryption
Answer: C

Q6. Which of the following is commonly used by cybercriminals to trick users into revealing passwords?
A. Brute-force attack
B. Phishing
C. DDoS attack
D. Ransomware
Answer: B

Q7. Which practice helps prevent being a victim of phishing?
A. Clicking on all email links
B. Opening attachments from unknown senders
C. Verifying the email source before responding
D. Using the same password everywhere
Answer: C

Q8. A strong password should include:
A. Your date of birth
B. Only letters
C. A mix of letters, numbers, and special characters
D. Simple words from the dictionary
Answer: C

Q9. Which of the following best describes the cybersecurity threat landscape?
A. A list of antivirus tools
B. A collection of global cyber laws
C. The evolving set of cyber threats and vulnerabilities organizations face
D. Cybersecurity careers
Answer: C

Q10. Which of the following is a technique used to protect against malware?
A. Using outdated software
B. Disabling firewalls
C. Regular software updates
D. Ignoring security warnings
Answer: C

Q11. Which of the following is an example of an emerging cybersecurity threat?
A. Email spam
B. AI-powered phishing attacks
C. Simple viruses
D. Manual hacking
Answer: B

Q12. Deepfake technology poses a threat because it:
A. Boosts productivity
B. Enhances video quality
C. Can be used for impersonation and misinformation
D. Blocks spam
Answer: C

Q13. What is multi-factor authentication (MFA)?
A. Using one strong password
B. Verifying identity with multiple credentials (e.g., password + OTP)
C. Logging in via social media
D. None of the above
Answer: B

Q14. Encryption is used to:
A. Speed up internet
B. Protect data by converting it into unreadable format
C. Slow down hackers
D. Open firewalls
Answer: B

Q15. What is the primary function of a firewall?
A. To enhance display resolution
B. To block unauthorized access to a network
C. To provide Wi-Fi signals
D. To store data
Answer: B

Q16. Which type of firewall filters traffic based on application-level rules?
A. Packet-filtering firewall
B. Stateful inspection firewall
C. Application-layer firewall
D. Network firewall
Answer: C

Q17. Which of the following best defines "pretexting" in social engineering?
A. Gaining access via physical intrusion
B. Creating a fabricated scenario to trick the victim into sharing information
C. Following someone into a restricted area
D. Infecting systems with malware
Answer: B

Q18. What is the goal of "quid pro quo" attacks in social engineering?
A. Destroy data
B. Offer something in exchange for information
C. Redirect network traffic

D. Monitor CCTV footage
Answer: B

Q19. What is a botnet?
A. A single powerful virus
B. A network of infected computers controlled remotely
C. A software update tool
D. A type of firewall
Answer: B

Q20. Which of the following is NOT a way cybercriminals distribute ransomware?
A. Email attachments
B. Fake software updates
C. Physical theft
D. Exploit kits on malicious websites
Answer: C

Q21. The principle of "least privilege" in cybersecurity refers to:
A. Giving users maximum access
B. Giving users only the access they need
C. Allowing admin access by default
D. Sharing passwords among team members
Answer: B

Q22. Which of these is a behavioral indicator of a phishing attack?
A. Slow computer performance
B. Email with a mismatched domain name
C. Loud fan noise from CPU
D. Printer not working
Answer: B

Q23. Which of the following threats can result in denial of service (DoS)?
A. Brute-force attack
B. Man-in-the-middle attack
C. Distributed denial-of-service (DDoS)
D. Ransomware
Answer: C

Q24. A zero-day vulnerability is:
A. Already patched by the developer
B. Known to attackers but not yet known to the software vendor
C. A phishing email
D. A type of firewall
Answer: B

Q25. Which technology increases the risk of automated identity theft?
A. Blockchain
B. IoT
C. Artificial Intelligence (AI)
D. USB drives
Answer: C

Q26. What makes IoT devices vulnerable to cyberattacks?
A. High cost
B. Use of blockchain
C. Lack of regular updates and weak security configurations
D. They are not connected to the internet
Answer: C

Q27. What does VPN stand for?
A. Virtual Private Network
B. Verified Password Number
C. Virtual Protocol Node
D. Variable Port Network
Answer: A

Q28. What is penetration testing used for?
A. Installing software
B. Testing system performance
C. Simulating attacks to find vulnerabilities
D. Scanning barcodes
Answer: C

Q29. Which of the following firewalls uses both packet filtering and stateful inspection?
A. Stateless firewall
B. Proxy firewall
C. Hybrid firewall
D. Network-layer firewall
Answer: C

Q30. A proxy firewall works at which layer of the OSI model?
A. Network Layer
B. Transport Layer
C. Application Layer
D. Data Link Layer
Answer: C

Q31. Which of the following is a limitation of traditional firewalls?
A. Cannot inspect email content
B. Cannot filter incoming packets
C. Cannot block IP addresses

D. Cannot perform logging
Answer: A

Q32. What is the purpose of regular software updates in cybersecurity?
A. Improve aesthetics
B. Add more advertisements
C. Patch known vulnerabilities
D. Reduce RAM usage
Answer: C

Q33. A digital certificate is used to:
A. Certify programming skills
B. Verify the identity of websites
C. Speed up downloads
D. Format USB drives
Answer: B

Q34. What does the “https” in a URL indicate?
A. Website is government owned
B. Server is in India
C. Connection is secured with SSL/TLS encryption
D. Website is hosted on the cloud
Answer: C

Q35. What does a “logic bomb” refer to in cybersecurity?
A. Explosive virus sent by email
B. Code triggered by a specific event
C. Computer's power surge
D. Overloaded memory cache
Answer: B

Q36. Which technique is used to capture encrypted credentials via a fake Wi-Fi access point?
A. Evil Twin Attack
B. Brute-force Attack
C. Watering Hole Attack
D. Buffer Overflow
Answer: A

Q37. Which of the following is an example of an insider threat?
A. Hacker exploiting a website vulnerability
B. Employee stealing confidential data
C. User downloading malware from a spam email
D. Attacker performing a brute-force attack
Answer: B

Q38. An attacker posing as IT support to extract a user's password is an example of:
A. Malware
B. Pre-texting
C. Phishing
D. Shoulder surfing
Answer: B

Q39. Which cybercrime involves unlawfully accessing and altering sensitive government data?
A. Cyber-terrorism
B. Cyberbullying
C. Identity Theft
D. Spamming
Answer: A

Q40. What is "credential stuffing"?
A. Sending spam messages
B. Trying known username-password combinations on multiple sites
C. Encrypting files for ransom
D. Phishing using text messages
Answer: B

Q41. Which attack method floods a network with traffic to make services unavailable?
A. Ransomware
B. Botnet
C. Denial of Service (DoS)
D. Phishing
Answer: C

Q42. The main function of antivirus software is to:
A. Encrypt data
B. Protect against unauthorized physical access
C. Detect and remove malicious software
D. Filter spam emails
Answer: C

Q43. What does the "sandboxing" technique help with in cybersecurity?
A. Blocking malicious IP addresses
B. Isolating suspicious code in a secure environment for analysis
C. Encrypting email communication
D. Increasing download speed
Answer: B

Q44. What is the use of a "honeypot" in cybersecurity?
A. To attract hackers and study their behavior
B. To store secure credentials

C. To backup encrypted files
D. To test bandwidth
Answer: A

Q45. What kind of firewall can block traffic based on user identity and device?
A. Packet-filtering firewall
B. Application-level gateway
C. Next-generation firewall (NGFW)
D. Proxy server
Answer: C

Q46. Which device sits between a trusted internal network and untrusted external networks like the internet?
A. Router
B. Modem
C. Switch
D. Firewall
Answer: D

Q47. Which of the following is a physical form of network security?
A. Software firewall
B. Intrusion Detection System (IDS)
C. Biometric access controls
D. VPN
Answer: C

Q48. What does a cybersecurity risk assessment primarily evaluate?
A. Employee satisfaction
B. Software interface design
C. Threats, vulnerabilities, and potential impact
D. Server storage limits
Answer: C

Q49. The term "CIA triad" in cybersecurity stands for:
A. Code, Interface, Algorithm
B. Confidentiality, Integrity, Availability
C. Control, Intelligence, Access
D. Cybercrime, Intrusion, Authentication
Answer: B

Q50. In risk management, a vulnerability is defined as:
A. A method of attacking systems
B. An outdated software
C. A weakness that can be exploited
D. A type of firewall
Answer: C

Q51. What is “smishing”?
A. Phishing via SMS
B. Social media hacking
C. Sniffing wireless networks
D. Spoofing emails
Answer: A

Q52. Which of the following can be used to intercept data on unsecured Wi-Fi networks?
A. Firewall
B. Packet sniffer
C. VPN
D. Encryption
Answer: B

Q53. Quantum computing poses future risks to cybersecurity primarily because it could:
A. Run without electricity
B. Decrypt traditional encryption methods quickly
C. Eliminate malware
D. Reduce phishing attacks
Answer: B

Q54. What is the best practice for managing passwords in an organization?
A. Share strong passwords with team
B. Use default passwords for ease
C. Use a password manager
D. Write passwords on paper
Answer: C

Q55. Which policy helps ensure employees don’t reuse personal passwords for company systems?
A. Acceptable Use Policy (AUP)
B. Bring Your Own Device (BYOD) Policy
C. Password Policy
D. Disaster Recovery Policy
Answer: C

Q56. Which of the following is a common type of social engineering attack?
A. SQL Injection
B. Phishing
C. DDoS
D. Man-in-the-Middle
Answer: B

Q57. What does a baiting social engineering attack typically involve?
A. Offering fake job opportunities
B. Leaving infected devices like USB drives to lure victims

C. Sending spam emails
D. Using malware over a network
Answer: B

Q58. Which form of social engineering uses voice communication to deceive victims?
A. Vishing
B. Smishing
C. Phishing
D. Baiting
Answer: A

Q59. The main objective of social engineering is to:
A. Destroy systems
B. Steal money directly
C. Manipulate people to disclose confidential data
D. Speed up computers
Answer: C

Q60. Which of these can prevent social engineering attacks?
A. Anti-virus software only
B. Strong passwords
C. User awareness and training
D. Spam filters
Answer: C

Q61. A zero-day attack exploits vulnerabilities that:
A. Have been patched
B. Are well-known and documented
C. Are unknown to the software vendor
D. Only affect mobile devices
Answer: C

Q62. Which of the following is considered an insider threat?
A. An external hacker
B. A former employee misusing access
C. A ransomware attack
D. A SQL Injection
Answer: B

Q63. The increasing use of IoT devices has led to:
A. Improved network security
B. Fewer vulnerabilities
C. New types of cyber threats
D. Increased CPU performance
Answer: C

Q64. Ransomware typically demands:
A. A job offer
B. Access credentials
C. Payment to restore encrypted data
D. Email verification
Answer: C

Q65. A botnet refers to:
A. A tool for software development
B. A set of infected computers under a hacker's control
C. A safe computer environment
D. A VPN service
Answer: B

Q66. Which of the following is a preventive security control?
A. Antivirus software
B. Incident log
C. Disaster recovery plan
D. Data breach report
Answer: A

Q67. Which of the following does NOT protect against malware?
A. Antivirus
B. Backup system
C. Firewalls
D. Sandboxing
Answer: B

Q68. A stateful firewall can:
A. Track the state of network connections
B. Only allow HTTP traffic
C. Automatically update user software
D. Store passwords
Answer: A

Q69. Deep Packet Inspection (DPI) is a feature of:
A. Traditional firewalls
B. Proxy servers
C. Next-Generation Firewalls (NGFW)
D. Load balancers
Answer: C

Q70. Which is not a feature of a firewall?
A. Packet filtering
B. Virus removal
C. Network traffic monitoring

D. Port blocking
Answer: B

Q71. A polymorphic virus is dangerous because:
A. It cannot be encrypted
B. It changes its code to avoid detection
C. It only affects Linux
D. It targets firewalls
Answer: B

Q72. The best way to defend against emerging cyber threats is:
A. Avoid using the internet
B. Rely on default device settings
C. Stay updated with patches and awareness
D. Use outdated software
Answer: C

Q73. AI in cybersecurity is being used for:
A. Writing malware
B. Automating phishing
C. Threat detection and response
D. Slowing down networks
Answer: C

Q74. Threat intelligence is:
A. A way to attack systems
B. Real-time analysis of incoming traffic only
C. Information to understand and mitigate threats
D. Information given to hackers
Answer: C

Q75. Cyber hygiene refers to:
A. Regular virus scanning only
B. Physical cleaning of devices
C. Routine practices for maintaining system health and safety
D. Disk fragmentation
Answer: C

Q76. What is the primary weakness exploited in social engineering attacks?
A. Firewalls
B. Human behavior
C. Encryption
D. Operating systems
Answer: B

Q77. A common way cybercriminals gather personal data is through:
A. Antivirus software
B. Social engineering techniques
C. Application logs
D. Code obfuscation
Answer: B

Q78. Smishing is a form of phishing carried out through:
A. Voice call
B. Email
C. SMS messages
D. Instant messaging apps
Answer: C

Q79. Which of the following is an example of a technical control to prevent cybercrime?
A. Employee training
B. Company policies
C. Firewall
D. Incident response plan
Answer: C

Q80. Pharming redirects users to:
A. Their email inbox
B. A legitimate banking website
C. A fake website to steal credentials
D. The deep web
Answer: C

Q81. Which of the following is a preventive technique against ransomware?
A. Paying the ransom quickly
B. Keeping offline backups
C. Opening unknown attachments
D. Ignoring software updates
Answer: B

Q82. Cybercriminals use spoofing to:
A. Authenticate users
B. Log activity
C. Disguise malicious communication as legitimate
D. Track users
Answer: C

Q83. Which of the following is NOT a part of the cyber threat landscape?
A. Malware
B. Natural disasters
C. Insider threats

D. Phishing
Answer: B

Q84. An attack that floods a system with traffic to make it unavailable is called:
A. Phishing
B. DoS
C. Spoofing
D. Brute force
Answer: B

Q85. Which term describes an attack that exploits previously unknown software vulnerabilities?
A. Trojan horse
B. Zero-day attack
C. Brute-force attack
D. Logic bomb
Answer: B

Q86. Which type of firewall filters traffic based on application layer data?
A. Packet-filtering firewall
B. Circuit-level gateway
C. Stateful firewall
D. Application-layer firewall
Answer: D

Q87. Multi-factor authentication (MFA) enhances:
A. Malware detection
B. Encryption
C. Identity verification
D. Internet speed
Answer: C

Q88. Which of the following is not a purpose of a firewall?
A. Blocking unauthorized access
B. Scanning for viruses
C. Controlling traffic flow
D. Enforcing network policies
Answer: B

Q89. A firewall that analyzes the full context of a packet including its state and application is known as:
A. Proxy firewall
B. Next-generation firewall (NGFW)
C. Hardware firewall
D. Static firewall
Answer: B

Q90. Which technique is commonly used to reduce the attack surface of a system?
A. Enabling all services
B. Installing outdated software
C. Disabling unnecessary ports/services
D. Avoiding user authentication
Answer: C

Q91. Which of these is NOT a common method of data loss prevention (DLP)?
A. Email encryption
B. Access control
C. Cloud backup
D. Phishing attacks
Answer: D

Q92. An example of endpoint security software is:
A. Browser
B. MS Excel
C. Antivirus
D. Discord
Answer: C

Q93. Which of the following best describes encryption?
A. Erasing files
B. Converting data into unreadable format
C. Compressing data
D. Formatting a hard drive
Answer: B

Q94. Two-factor authentication requires:
A. Two usernames
B. A username and two passwords
C. Two different types of credentials
D. A single password
Answer: C

Q95. Which of the following ensures confidentiality of sensitive data?
A. Data compression
B. Data deletion
C. Encryption
D. Authentication
Answer: C

UNIT IV:

Q1. What is social engineering in cybersecurity?
A. Using encryption for data safety
B. Manipulating people to give confidential information
C. Coding malicious software
D. Breaking firewalls
Answer: B

Q2. Phishing is a type of attack where the attacker:
A. Physically accesses a device
B. Sends malicious software on pen drives
C. Tricks users into providing confidential info via fake websites
D. Hacks CCTV systems
Answer: C

Q3. What is the goal of baiting in social engineering?
A. Launch DDoS attacks
B. Entice users to download malicious content
C. Encrypt communication
D. Block a firewall
Answer: B

Q4. Which is an example of a preventive step against social engineering?
A. Leaving passwords on sticky notes
B. Clicking unknown links
C. Using strong authentication and awareness training
D. Ignoring software updates
Answer: C

Q5. Which of the following is NOT a type of cybercrime?
A. Hacking
B. Identity Theft
C. Cyber bullying
D. File Compression
Answer: D

Q6. What is the primary motive of ransomware?
A. Destroying files
B. Asking for money to unlock encrypted data
C. Hacking government servers
D. Redirecting search results
Answer: B

Q7. Which practice reduces your risk of cybercrime?
A. Using the same password for all accounts

B. Installing antivirus software
C. Turning off system updates
D. Sharing credentials
Answer: B

Q8. What is a brute-force attack?
A. Flooding a system with traffic
B. Guessing passwords using trial-and-error
C. Encrypting files
D. Accessing CCTV
Answer: B

Q9. What is spoofing?
A. Destroying data intentionally
B. Monitoring internet usage
C. Pretending to be a trusted source
D. Encrypting backups
Answer: C

Q10. Shoulder surfing refers to:
A. Monitoring network traffic
B. Watching someone enter their password
C. Attacking server-side code
D. Looking over source code
Answer: B

Q11. A common example of phishing is:
A. Pop-up ads
B. Fake emails pretending to be from banks
C. USB malware
D. Server downtime
Answer: B

Q12. Which is a form of technical social engineering?
A. Dumpster diving
B. Malware-injected emails
C. Bribing an employee
D. Eavesdropping
Answer: B

Q13. What is vishing?
A. Video-based phishing
B. Phishing via phone calls
C. Verifying passwords
D. Using fake QR codes
Answer: B

Q14. What is smishing?
A. Phishing via SMS
B. Malware from ads
C. Phishing via WhatsApp
D. Voice cloning
Answer: A

Q15. Which of the following is the safest way to verify a suspicious email?
A. Click the link to see where it leads
B. Reply to the email
C. Contact the sender through a trusted source
D. Forward to all colleagues
Answer: C

Q16. Which method is used to secure personal information online?
A. Sharing it on social media
B. Using public Wi-Fi
C. Two-factor authentication
D. Using outdated software
Answer: C

Q17. Which of the following is an example of a passive attack?
A. Phishing
B. Data interception
C. DDoS attack
D. Ransomware
Answer: B

Q18. A Trojan horse attack is best described as:
A. A self-replicating program
B. A hidden malicious code within legitimate software
C. An attempt to guess passwords
D. A type of firewall
Answer: B

Q19. Which tool is commonly used for network packet analysis?
A. Wireshark
B. Nmap
C. Burp Suite
D. Metasploit
Answer: A

Q20. What does “zero-day vulnerability” refer to?
A. A flaw already patched
B. A known virus
C. A software flaw unknown to the vendor

D. A public vulnerability
Answer: C

Q21. Which one is a preventive control in cybersecurity?
A. Firewall
B. Incident log
C. Audit trail
D. Recovery plan
Answer: A

Q22. Which of the following is not a cybersecurity technique?
A. Encryption
B. Intrusion detection
C. Packet sniffing
D. Authentication
Answer: C

Q23. What does a firewall primarily do?
A. Backs up data
B. Encrypts files
C. Filters network traffic
D. Generates passwords
Answer: C

Q24. Which type of firewall filters traffic based on IP addresses and ports?
A. Application gateway
B. Packet-filtering firewall
C. Proxy firewall
D. Stateful firewall
Answer: B

Q25. A Next-Generation Firewall (NGFW) offers which additional feature?
A. Only packet filtering
B. Deep packet inspection
C. Antivirus update
D. Database encryption
Answer: B

Q26. Which device is used to hide internal IP addresses from the external world?
A. Switch
B. Router
C. NAT device
D. Modem
Answer: C

Q27. Which of the following is an example of physical digital infrastructure security?
A. Firewalls
B. Antivirus
C. Biometric access controls
D. IP blocking
Answer: C

Q28. The IT Act 2000 was mainly enacted to:
A. Promote digital marketing
B. Regulate telecom operations
C. Provide legal recognition to electronic commerce and data security
D. Promote social media
Answer: C

Q29. Which organization handles critical information infrastructure protection in India?
A. UIDAI
B. NCIIPC
C. TRAI
D. NIC
Answer: B

Q30. The CERT-In was set up under which act?
A. Indian Penal Code
B. Information Technology Act
C. Data Protection Act
D. Digital India Act
Answer: B

Q31. The IT (Amendment) Act, 2008 added which new offence?
A. Online shopping fraud
B. Cyber terrorism
C. Domain squatting
D. Phishing
Answer: B

Q32. The first step in the Incident Response Lifecycle is:
A. Recovery
B. Containment
C. Detection
D. Preparation
Answer: D

Q33. A cybersecurity assurance process mainly helps in:
A. Writing secure code
B. Managing employee attendance
C. Establishing stakeholder trust in IT systems

D. Automating HR functions
Answer: C

Q34. Containment in incident response helps to:
A. Clean infected systems
B. Prevent damage from spreading
C. Increase memory speed
D. Improve file storage
Answer: B

Q35. Which type of vulnerability allows hackers to execute scripts in a user's browser?
A. CSRF
B. XSS
C. Ransomware
D. SQL Injection
Answer: B

Q36. Defensive programming mainly involves:
A. Creating long code
B. Ignoring error messages
C. Writing code that anticipates misuse and errors
D. Hiding the UI
Answer: C

Q37. Which of the following is a defensive programming technique?
A. Hard coding passwords
B. Input validation
C. Disabling logs
D. Ignoring exceptions
Answer: B

Q38. Which tool is used for secure deletion of sensitive files in Windows?
A. MS Word
B. SDelete
C. Paint
D. Disk Defragmenter
Answer: B

Q39. What is data remanence?
A. Backed-up data
B. Residual data after deletion
C. Data stored on CDs
D. Lost data
Answer: B

Q40. Which of the following tools can help recover accidentally deleted files?
A. Notepad++
B. Recuva
C. SDelete
D. Git
Answer: B

Q41. Which of the following is considered an ethical hacker?
A. Black Hat
B. White Hat
C. Grey Hat
D. Red Hat
Answer: B

Q42. A Denial of Service (DoS) attack primarily targets:
A. Confidentiality
B. Integrity
C. Availability
D. Authentication
Answer: C

Q43. Keylogging is used to:
A. Encrypt passwords
B. Log user activity
C. Capture keystrokes to steal credentials
D. Clean malware
Answer: C

Q44. Which technique protects against SQL injection?
A. Packet filtering
B. Parameterized queries
C. Firewall
D. IP Whitelisting
Answer: B

Q45. Which is NOT a valid countermeasure for phishing attacks?
A. Email filtering
B. User education
C. Regular password reset
D. Ignoring software updates
Answer: D

Q46. Which HTTP header helps prevent Cross-Site Scripting (XSS)?
A. Content-Security-Policy
B. GET
C. POST

D. Accept-Encoding
Answer: A

Q47. CAPTCHA is mainly used to:
A. Encrypt passwords
B. Improve webpage speed
C. Distinguish between humans and bots
D. Scan viruses
Answer: C

Q48. Which web app attack involves unauthorized commands from a trusted user's browser?
A. SQL Injection
B. XSS
C. CSRF
D. Brute force
Answer: C

Q49. Which tool is primarily used for web vulnerability scanning?
A. Nikto
B. Recuva
C. Wireshark
D. Metasploit
Answer: A

Q50. Secure coding practices include all EXCEPT:
A. Input validation
B. Error handling
C. Hardcoding credentials
D. Code reviews
Answer: C

Q51. The Digital India Programme primarily aims to:
A. Build hospitals
B. Increase digital infrastructure and services
C. Promote agriculture
D. Fund startups
Answer: B

Q52. Under IT Act, who is authorized to investigate cybercrime in India?
A. Sub Inspector
B. Any civilian
C. Inspector rank or above
D. Private company
Answer: C

Q53. Who heads the Cyber Swachhta Kendra (Botnet Cleaning Center) in India?
A. NIC
B. NCIIPC
C. MeitY and CERT-In
D. UIDAI
Answer: C

Q54. Information Security Education and Awareness (ISEA) project is launched by:
A. DRDO
B. ISRO
C. MeitY
D. ICERT
Answer: C

Q55. Which is not a key sector protected under India's Critical Information Infrastructure (CII)?
A. Power
B. Banking
C. Tourism
D. Telecom
Answer: C

Q56. What is digital forensics?
A. Writing security software
B. Developing digital apps
C. Investigation of digital data for legal purposes
D. Recovering hard drives
Answer: C

Q57. The main aim of data sanitization is to:
A. Backup data
B. Store personal files
C. Permanently remove sensitive data
D. Compress files
Answer: C

Q58. Which tool is most useful for creating disk images during forensics?
A. FTK Imager
B. Paint
C. Wireshark
D. WordPad
Answer: A

Q59. In defensive programming, which of the following is NOT recommended?
A. Using input validation
B. Writing clear error messages

C. Avoiding exception handling
D. Logging security events
Answer: C

Q60. The command-line tool used for secure deletion on Linux is:
A. shred
B. mv
C. rm
D. cat
Answer: A

Q61. Which international standard focuses on Information Security Management Systems (ISMS)?
A. ISO 9001
B. ISO 14001
C. ISO/IEC 27001
D. ISO 50001
Answer: C

Q62. Which of the following is NOT a core function of the NIST Cybersecurity Framework?
A. Identify
B. Protect
C. Attack
D. Respond
Answer: C

Q63. What is the main benefit of using a cybersecurity framework?
A. Reduce taxes
B. Standardize security practices
C. Increase internet speed
D. Reduce hardware cost
Answer: B

Q64. Which tool is widely used for penetration testing?
A. Putty
B. Kali Linux
C. CCleaner
D. Zoom
Answer: B

Q65. Which tool is used for detecting vulnerabilities in web applications?
A. Nmap
B. Burp Suite
C. Angry IP Scanner

D. Wireshark
Answer: B

Q66. The primary goal of a honeypot is to:
A. Prevent phishing
B. Attract and analyze attackers
C. Scan for malware
D. Encrypt sensitive files
Answer: B

Q67. Which of the following is NOT a purpose of cyber forensics?
A. Identify cyber attackers
B. Track deleted files
C. Create user interfaces
D. Provide evidence in court
Answer: C

Q68. A buffer overflow occurs when:
A. Code is not compiled properly
B. Program exceeds its memory boundary
C. A virus infects a file
D. Input is restricted
Answer: B

Q69. Which language is more prone to buffer overflows due to lack of built-in protections?
A. Python
B. Java
C. C
D. Ruby
Answer: C

Q70. Which is the best defense against SQL Injection?
A. Firewall
B. Antivirus
C. Input sanitization and parameterized queries
D. Using GET requests
Answer: C

Q71. Code obfuscation is used to:
A. Increase speed
B. Hide source code logic
C. Translate code
D. Generate test data
Answer: B

Q72. Section 66F of the IT Act, 2008 deals with:
A. Data breach
B. Identity theft
C. Cyber terrorism
D. Data protection
Answer: C

Q73. Which body handles cybersecurity incidents in India?
A. NIC
B. CERT-In
C. DoT
D. RBI
Answer: B

Q74. Which project provides cyber hygiene and awareness for citizens in India?
A. Smart India Hackathon
B. Digital India Portal
C. Cyber Swachhta Kendra
D. DigiLocker
Answer: C

Q75. Who can issue orders for blocking of websites in India under IT Act?
A. CBI
B. State Police
C. Secretary, MeitY
D. RBI
Answer: C

Q76. Which of the following is a secure data erasure method?
A. Formatting
B. Disk partitioning
C. DoD 5220.22-M
D. File renaming
Answer: C

Q77. Which tool helps in recovering accidentally deleted partitions?
A. TestDisk
B. SDelete
C. Notepad
D. Paint
Answer: A

Q78. Which of the following is a non-recoverable method of destroying data?
A. File deletion
B. Formatting
C. Physical destruction

D. Disk cleanup
Answer: C

Q79. What is the purpose of Wipe software?
A. Enhance storage speed
B. Remove malware
C. Securely erase data beyond recovery
D. Backup files
Answer: C

Q80. Data encryption ensures:
A. Compression
B. Data is visible in plain text
C. Confidentiality
D. Advertisement blocking
Answer: C