1. What is cybercrime?
a. Legal computer activities
b. Any legal act committed using a computer
c. Illegal act committed using a computer
d. Computer programming
Answer: c. Illegal act committed using a computer

2. Who are cyber criminals?
a. Ethical hackers
b. Individuals or organizations committing illegal acts using a computer
c. Regular computer users
d. Computer manufacturers
Answer: b. Individuals or organizations committing illegal acts using a computer

3. What is the major reason for cybercrime related to financial gain?
a. Personal motives
b. Opportunism
c. Espionage
d. Stealing financial information
Answer: d. Stealing financial information

4. What type of hackers focus on fixing identified weaknesses in systems?
a. Black hat hackers
b. White hat hackers
c. Organized hackers
d. Internet stalkers
Answer: b. White hat hackers

5. What is the classification of cybercrimes based on the groups they target?
a. Three categories
b. Four categories
c. Five categories
d. Six categories
Answer: b. Four categories

6. Which cybercrime is an illegal modification of data?
a. Cyber stalking
b. Phishing
c. Data Diddling
d. Denial of Service Attack Answer: c. Data Diddling

7. What does cyber terrorism aim to affect adversely?
a. Financial institutions
b. Harmony between different groups
c. Individual privacy
d. Social media platforms
Answer: b. Harmony

between different groups

8. What is the purpose of a Salami attack?
a. Financial crimes
b. Identity theft
c. Espionage
d. Online harassment
Answer: a. Financial crimes

9. What is the main motive of cyber theft?
a. Identity theft
b. Gathering confidential data
c. Defamation
d. Personal gain
Answer: b.
Gathering
confidential data

10. What is the term for crimes committed against property in cyberspace?
a. Cyber espionage
b. Cyber terrorism
c. Intellectual property crimes
d. Cyber thefts
Answer: c.
Intellectual
property crimes

11. What is cyber grooming?
a. Improving cybersecurity
b. Building online relationships with minors
c. Ethical hacking
d. Selling stolen data online
Answer: b. Building online relationships with minors

12. Which type of cybercrime involves sending a large number of emails to crash a victim's email account?
a. Cyber stalking
b. Phishing
c. Email bombing
d. Cyber defamation Answer: c. Email bombing

13. What is the purpose of forgery in cybercrime?
a. Identity theft
b. Creating fake documents
c. Intellectual property theft
d. Financial gain
Answer: b.
creating fake
documents

14. What is the primary objective of a Denial of Service (DoS) attack?
a. Financial gain

b. Identity theft
c. Preventing access to computer systems
d. Gathering confidential data
Answer: c. Preventing access to computer systems

15. What is the main focus of cyber terrorism?
a. Financial institutions
b. Threatening governments
c. Social media platforms
d. Intellectual property theft
Answer: b.
Threatening
governments

16. What is the primary target of web jacking?
a. Intellectual property
b. Financial institutions
c. Government systems
d. Websites
Answer: d. Websites

17. What is the term for the unauthorized taking of another's credit card information? a. Identity theft

b. Credit card fraud
c. Cyber theft
d. Forgery
Answer: b. Credit card fraud

18. What is the main focus of cybercrime against women and children?
a. Intellectual property theft
b. Cyber terrorism
c. Exploiting women through online platforms
d. Identity theft
Answer: c. Exploiting women through online platforms

19. What is the term for the illegal deal or trade in children in cybercrime? a. Identity theft

b. Cyber terrorism
c. Trafficking
d. Cyber grooming
Answer: c. Trafficking

20. What does morphing involve in cybercrime?
a. Changing smoothly from one image to another
b. Hacking social media accounts
c. Creating fake documents
d. Gathering confidential data
Answer: a. Changing smoothly from one image to another

21. How can victims report cybercrimes in India according to the content?

a. Contacting the nearest cyber cell or police station

b. Filing a complaint through the National Cyber Crime Reporting Portal c. Both a and b

d. None of the above

Answer: c. Both a and b

22. What is the primary purpose of a Salami attack in cybercrime?

a. Financial crimes

b. Identity theft

c. Espionage

d. Online harassment

Answer: a. Financial crimes

23. What is the primary objective of web jacking?

a. Intellectual property theft

b. Financial gain

c. Gaining control of a website fraudulently

d. Identity theft

Answer: c. Gaining control of a website fraudulently

24. Which type of hackers intentionally attempt to crack a system with permission to identify weak points?

a. Black hat hackers

b. White hat hackers

c. Organized hackers

d. Internet stalkers

Answer: b. White hat hackers

25. What is the missing vital feature in internet-enabled mobile cell phones according to the content? a. Security

b. Portability

c. Flexibility

d. Data storage

Answer: a. Security

26. What type of attacks involve intrusion into computer systems and mobile operating systems to gain unauthorized access? a. Phishing

b. Ransomware

c. Hacking

d. Identity theft

Answer: c. Hacking

27. What is the primary goal of mobile malware?

a. Encrypting data

b. Gaining access to private data and financial fraud

c. Locking and rendering devices unusable

d. Disrupting operations

Answer: b. Gaining access to private data and financial fraud

28. What does ransomware do in both computer and mobile contexts?

a. Encrypts victim's data and demands payment

b. Steals sensitive data and permanently locks the device
c. Locks and encrypts data, demanding payment for release
d. Disables wireless connections in devices
Answer: c. Locks and encrypts data, demanding payment for release

29. What is the outcome of identity theft in cybercrime?
a. Unauthorized access to computers
b. Gaining access to private data
c. Criminal acts committed using victim's identity
d. Rendering devices inaccessible and unusable
Answer: c. Criminal acts committed using victim's identity

30. What is Bluebugging in the context of cybercrime?
a. Accessing calendar and address book
b. Listening to mobile phone conversations
c. Sending malicious text messages
d. Locking mobile devices remotely
Answer: b. Listening to mobile phone conversations

31. What is phishing in cybercrime?
a. Locking and encrypting data
b. Unauthorized access to computers
c. Gaining access to private data through deception
d. Mobile malware attacks
Answer: c. Gaining access to private data through deception
32. What is vishing in the context of phishing?
a. Email phishing
b. Phone phishing
c. SMS phishing
d. Social media phishing
Answer: b. Phone phishing

33. What is smishing in the context of phishing?
a. Email phishing
b. Phone phishing
c. SMS phishing
d. Social media phishing
Answer: c. SMS phishing

34. What are the tips for securing cell phones mentioned in the content?
a. Turn off wireless connections when not needed
b. Install outdated antivirus software
c. Share personal information with strangers
d. Store personal banking details in cell phones
Answer: a. Turn off wireless connections when not needed

35. What is the primary goal of malware in cybercrime?
a. Gaining unauthorized access
b. Disabling wireless connections
c. Causing harm to devices through various means
d. Extracting confidential information from users
Answer: c. Causing harm to devices through various means

36. What is the primary demand made by ransomware attackers?

a. Payment in cash

b. Payment in cryptocurrency

c. Providing access to more devices

d. Deleting victim's data

Answer: b. Payment in cryptocurrency

37. How does a computer virus spread according to the content?

a. Through physical contact

b. Through social media links

c. Through email and text message attachments

d. Through Wi-Fi connections

Answer: c. Through email and text message attachments

38. What is the impact of ransomware on a computer?

a. Locks and renders the computer unusable

b. Steals sensitive data permanently

c. Deletes all files on the computer

d. Disables wireless connections

Answer: a. Locks and renders the computer unusable

39. What is the primary focus of online banking fraud in financial frauds?

a. Gaining unauthorized access to accounts

b. Exploiting weaknesses in mobile systems

c. Stealing credit card information

d. Accessing private data for financial gain

Answer: a. Gaining unauthorized access to accounts

40. What is mobile payment fraud primarily exploiting?

a. Weaknesses in mobile systems

b. Unauthorized access to online banking accounts

c. Credit card information

d. Social media links

Answer: a. Weaknesses in mobile systems

41. What is the first category of credit card fraud mentioned in the content? a. Lost or stolen cards

b. Account takeover

c. Counterfeit cards

d. Email order/telephone order fraud

Answer: a. Lost or stolen cards

42. What is the second category of credit card fraud mentioned in the content? a. Lost or stolen cards

b. Account takeover

c. Counterfeit cards

d. Email order/telephone order fraud

Answer: b. Account takeover

43. What is the primary recommendation for handling malware attacks according to the content?

a. Reset credentials and restore from backup

b. Disconnect infected devices and monitor network traffic
c. Pay the ransom to guarantee access to files
d. Continue using infected devices with caution
Answer: b. Disconnect infected devices and monitor network traffic

44. How does a computer virus infect other computers on the same network?
a. By stealing credit card information
b. By disabling wireless connections
c. By running infected programs on other devices
d. By connecting to public Wi-Fi networks
Answer: c. By running infected programs on other devices

45. What is the primary characteristic of social engineering attacks?
a) Exploiting software vulnerabilities
b) Relying on human error
c) Targeting specific operating systems
d) Using advanced encryption techniques Answer: b) Relying on human error

46. Which classification of social engineering involves person-to-person interaction?
a) Human-Based Social Engineering
b) Computer-Based Social Engineering
c) Hardware-Based Social Engineering
d) Network-Based Social Engineering
Answer: a) Human-Based Social Engineering

47. What is "Impersonation" in the context of social engineering?
a) Acting as an important user
b) Using a third person for deception
c) Pretending to be a legitimate employee or user
d) Calling technical support for assistance
Answer: c) Pretending to be a legitimate employee or user

48. How does "Shoulder Surfing" work in social engineering?
a) Manipulating emails for deception
b) Looking for information in discarded materials
c) Observing someone's sensitive information directly
d) Using a third person for impersonation
Answer: c) Observing someone's sensitive information directly

49. What does "Dumpster Diving" involve in social engineering?
a) Calling technical support for assistance
b) Spreading malware through emails
c) Looking for information in discarded materials
d) Impersonating an employee to obtain information
Answer: c) Looking for information in discarded materials

50. Which of the following is an example of computer-based social engineering?
a) Impersonating an employee
b) Dumpster diving for information

c) Sending fake emails (Phishing)
d) Acting as an important user
Answer: c) Sending fake emails (Phishing)

51. What is a "Zero-Day Attack"?
a) An attack that occurs on the same day it is planned
b) An attack that exploits a vulnerability before a patch is available
c) An attack that requires zero clicks from the user
d) An attack that involves zero social engineering techniques
Answer: b) An attack that exploits a vulnerability before a patch is available

52. Which system is NOT mentioned as a common target for Zero-Day Attacks?
a) Operating systems
b) Web browsers
c) Mobile applications
d) Certified shops Answer: d) Certified shops
53. What is the purpose of a web application firewall (WAF)?
a) Spreading malware through emails
b) Monitoring and regulating network traffic
c) Preventing social engineering attacks
d) Investigating cybercrimes
Answer: b) Monitoring and regulating network traffic

54. What is a characteristic of a Zero Click Attack?
a) Requires human action to start
b) Rely on phishing emails
c) Doesn't require human action to start
d) Involves physical intrusion
Answer: c) Doesn't require human action to start

55. How was the WhatsApp Zero-Click Attack initiated?
a) Through a fake email
b) By clicking on a link
c) Via a missed call
d) Opening an infected attachment
Answer: c) Via a missed call

56. What is the modus operandi of cybercrime?
a) The legal process followed in cybercrime investigations
b) The organization responsible for cybercrime prevention
c) The method used by criminals for successful commission of a crime
d) The software used by cybercriminals
Answer: c) The method used by criminals for successful commission of a crime

57. What elements are recorded in the modus operandi files of cybercrime?
a) Software vulnerabilities
b) Social engineering techniques
c) Details like entry point, means, object, time, style, tale, transport, and trademark

d) Cybersecurity best practices
Answer: c) Details like entry point, means, object, time, style, tale, transport, and trademark

58. How should evidence be preserved in reporting cybercrimes?
a) Delete all evidence to avoid further damage
b) Share evidence on social media platforms
c) Document and preserve relevant information
d) Preserve evidence only if it's related to financial fraud
Answer: c) Document and preserve relevant information

59. What is CERT-In?
a) A computer security software
b) A cybersecurity incident response team
c) A social engineering technique
d) An online consumer complaints platform Answer: b) A cybersecurity incident response team

60. What is the purpose of the National Cyber Crime Reporting Portal (NCCRP)?
a) To spread awareness about cybersecurity
b) To facilitate online reporting of cybercrimes in India
c) To provide cybersecurity training
d) To conduct cybercrime investigations
Answer: b) To facilitate online reporting of cybercrimes in India

61. What should you do in case of financial fraud or unauthorized transactions?
a) Report it to social media platforms
b) Share details on online consumer complaints platforms
c) Inform your bank immediately
d) Preserve evidence on your devices
Answer: c) Inform your bank immediately

62. What is the role of Cyber Crime Cells in reporting cybercrimes?
a) Investigate cybercrimes
b) Coordinate responses to cybersecurity incidents
c) Provide legal assistance
d) Develop cybersecurity software
Answer: a) Investigate cybercrimes

63. What is the significance of local cybercrime helpline numbers?
a) Provide cybersecurity training
b) Offer legal assistance
c) Coordinate responses to significant cybersecurity incidents
d) Assist individuals seeking help with cybercrime issues
Answer: d) Assist individuals seeking help with cybercrime issues

64. How can you prevent a Zero-Click Attack?
a) Uninstall programs you don't use
b) Jailbreak your phone
c) Avoid updating your operating system
d) Share your personal information online
Answer: a) Uninstall programs you don't use

65. What is the role of an inbound firewall?
a) Monitor and regulate network traffic
b) Spread malware through pop-up windows
c) Conduct phishing attacks
d) Investigate cybercrimes
Answer: a) Monitor and regulate network traffic

66. What is the primary purpose of a web application firewall (WAF)?
a) To spread malware through emails
b) To monitor and regulate network traffic
c) To prevent social engineering attacks
d) To protect against web-based attacks Answer: d) To protect against web-based attacks
67. What is the principle of least privilege in cybersecurity?
a) Giving excessive privileges to every user
b) Limiting privileges based on identity, not function
c) Providing maximum access rights to every subject
d) Allowing users to choose their own privileges
Answer: b) Limiting privileges based on identity, not function

68. How do Zero Day Attacks differ from other cyber threats?
a) They require human action to start
b) They exploit vulnerabilities before patches are available
c) They are always initiated through phishing emails
d) They only target hardware vulnerabilities
Answer: b) They exploit vulnerabilities before patches are available

69. In the context of social engineering, what is phishing?
a) Impersonating an employee
b) Dumpster diving for information
c) Sending fake emails to deceive users
d) Using shoulder surfing techniques
Answer: c) Sending fake emails to deceive users

70. What is a common target for Zero-Day Attacks?
a) Certified shops
b) Mobile applications
c) Social media platforms
d) Food delivery services
Answer: b) Mobile applications

71. What is the primary characteristic of a Zero Click Attack?
a) Requires multiple clicks from the user
b) Needs manual execution by the user
c) Doesn't need human action to start
d) Exploits vulnerabilities before patches are available
Answer: c) Doesn't need human action to start

72. What is the primary method used in a WhatsApp Zero-Click Attack?
a) Fake emails

b) Phishing
c) Missed call manipulation
d) Malicious attachments
Answer: c) Missed call manipulation

73. What should you avoid to enhance digital security?
a) Regularly updating your operating system
b) Disabling pop-ups on online browsers
c) Jail breaking your phone
d) Creating strong passwords Answer: c) Jail breaking your phone
74. How does the principle of least privilege contribute to cybersecurity?
a) Gives maximum access rights to every subject
b) Limits the potential damage a bad actor might cause
c) Encourages users to choose their own privileges
d) Requires users to authenticate multiple times
Answer: b) Limits the potential damage a bad actor might cause

75. What is the primary purpose of an Incident Response Plan in cybersecurity?
a) To develop software applications
b) To outline steps in case of a cybersecurity incident
c) To create secure passwords for users
d) To conduct regular security audits
Answer: b) To outline steps in case of a cybersecurity incident

76. Why is regular data backup important in cybersecurity?
a) To increase internet speed
b) To recover from data loss incidents
c) To prevent phishing attacks
d) To deploy endpoint protection solutions
Answer: b) To recover from data loss incidents

77. What does Patch Management involve in cybersecurity?
a) Creating secure passwords
b) Monitoring network traffic
c) Keeping software up to date with security patches
d) Conducting phishing attacks
Answer: c) Keeping software up to date with security patches

78. What is the purpose of Network Segmentation in cybersecurity?
a) Sending fake emails
b) Protecting web applications
c) Monitoring system activities
d) Enhancing data backup processes
Answer: c) Monitoring system activities

79. What is the role of Endpoint Protection in cybersecurity?
a) Implementing multi-factor authentication
b) Conducting regular security audits
c) Monitoring network traffic
d) Detecting and blocking malicious activities on devices
Answer: d) Detecting and blocking malicious activities on devices

80. What does Multi-Factor Authentication (MFA) add to cybersecurity?
a) An extra layer of security
b) Regular security audits
c) Monitoring system activities
d) Conducting phishing attacks Answer: a) An extra layer of security
81. What is the primary purpose of Security Awareness Training?
a) To implement network segmentation
b) To educate employees about cybersecurity threats
c) To develop secure software applications
d) To conduct regular security audits
Answer: b) To educate employees about cybersecurity threats

82. How does encryption contribute to cybersecurity?
a) Monitoring network traffic
b) Protecting sensitive data during transmission and storage
c) Conducting phishing attacks
d) Implementing multi-factor authentication
Answer: b) Protecting sensitive data during transmission and storage

83. What is the role of Intrusion Detection and Prevention Systems (IDPS) in cybersecurity?
a) Spreading malware through emails
b) Protecting web applications
c) Monitoring system activities and responding to potential incidents
d) Conducting regular security audits
Answer: c) Monitoring system activities and responding to potential incidents

84. What is the primary purpose of a Web Application Firewall (WAF)?
a) Monitoring and regulating network traffic
b) Protecting against web-based attacks on applications
c) Spreading malware through emails
d) Conducting phishing attacks
Answer: b) Protecting against web-based attacks on applications

85. Why is regular security audit essential in cybersecurity?
a) To create secure passwords
b) To educate employees about cybersecurity threats
c) To identify weaknesses in systems and networks
d) To develop secure software applications
Answer: c) To identify weaknesses in systems and networks

86. How does Cyber Insurance contribute to cybersecurity?
a) Conducting regular security audits
b) Mitigating financial losses in case of a cybersecurity incident
c) Implementing multi-factor authentication
d) Monitoring network traffic
Answer: b) Mitigating financial losses in case of a cybersecurity incident

87. What does Vendor Security Assessment involve in cybersecurity?
a) Creating secure passwords for users
b) Protecting web applications
c) Assessing the security practices of third-party vendors
d) Conducting phishing attacks
Answer: c) Assessing the security practices of third-party vendors

88. What is the purpose of Access Controls in cybersecurity?
a) Monitoring network traffic
b) Creating secure passwords for users
c) Limiting user privileges based on job responsibilities
d) Protecting web applications
Answer: c) Limiting user privileges based on job responsibilities

89. Why is Continuous Monitoring important in cybersecurity?
a) To develop secure software applications
b) To conduct regular security audits
c) To detect and respond to suspicious or malicious behavior in real-time
d) To implement network segmentation
Answer: c) To detect and respond to suspicious or malicious behavior in real-time

90. What is Threat Intelligence Sharing in cybersecurity?
a) Creating secure passwords for users
b) Engaging in collaboration and open communication
c) Conducting regular security audits
d) Sharing information about emerging threats and vulnerabilities
Answer: d) Sharing information about emerging threats and vulnerabilities

91. Why is Legal Compliance important in cybersecurity?
a) To develop secure software applications
b) To foster a culture of collaboration
c) To ensure compliance with relevant cybersecurity laws and regulations
d) To implement multi-factor authentication
Answer: c) To ensure compliance with relevant cybersecurity laws and regulations

92. What is the purpose of DDoS Protection in cybersecurity?
a) To implement network segmentation
b) To conduct regular security audits
c) To mitigate the impact of distributed denial-of-service attacks
d) To protect against web-based attacks
Answer: c) To mitigate the impact of distributed denial-of-service attacks

93. How does Cloud Security Measures contribute to cybersecurity?
a) To educate employees about cybersecurity threats
b) To develop secure software applications

c) To implement security measures provided by the cloud service provider
d) To conduct regular security audits
Answer: c) To implement security measures provided by the cloud service provider

94. What is the significance of Collaboration and Communication in cybersecurity?
a) To implement network segmentation
b) To foster a culture of collaboration and open communication
c) To protect against web-based attacks
d) To conduct regular security audits

Answer: b) To foster a culture of collaboration and open communication

UNIT-IV

1. What is the definition of E-Commerce?

A) The exchange of goods only

B) Buying and selling of goods, products, or services over the internet

C) Traditional commerce

D) Physical store transactions

Answer: B) Buying and selling of goods, products, or services over the internet

2. Which of the following is another term for E-Commerce?

A) M-Commerce

B) Digital Commerce

C) Traditional Commerce

D) A and B

Answer: D) A and B

3. What types of transactions are considered part of E-Commerce?

A) Only transactions involving goods

B) Only transactions involving services

C) Transactions of money, funds, and data

D) All of the above

Answer: C) Transactions of money, funds, and data

4. Which of the following is NOT a way in which E-Commerce transactions can occur?

A) Business to Business (B2B)

B) Business to Customer (B2C)

C) Company to Company (C2C)

D) Customer to Government (C2G)

Answer: D) Customer to Government (C2G)

5. Who are the main components of E-Commerce?

A) Sellers and buyers

B) Users and vendors

C) Marketers and consumers

D) Suppliers and manufacturers

Answer: B) Users and vendors

6. Which of the following is NOT a responsibility of e-commerce vendors? A) Supply Chain Management

B) Shipping and returns

C) Warehouse operations

D) Product manufacturing

Answer: D) Product manufacturing

7. Which of the following is NOT a function of e-commerce vendors' responsibilities?

A) Marketing and loyalty programs

B) Customer support

C) Product display

D) Invoice management

Answer: D) Invoice management

8. What is the function of the technology infrastructure in e-commerce?

A) Providing internet connectivity

B) Storing data/programs essential for operations

C) Managing payment gateways

D) Handling shipping and logistics

Answer: B) Storing data/programs essential for operations

9. Which of the following is crucial for the success of e-commerce transactions?

A) Efficient shipping services

B) Advanced payment gateways

C) Internet/network connectivity

D) Marketing strategies

Answer: C) Internet/network connectivity

10. What is the purpose of a web portal in e-commerce?

A) Providing internet connectivity

B) Storing data/programs

C) Facilitating e-commerce transactions

D) Managing inventory

Answer: C) Facilitating e-commerce transactions

11. Which of the following is NOT an example of a payment gateway?

A) Credit/Debit Card Payments

B) Online bank payments

C) Social media platforms

D) Unified Payments Interface (UPI)

Answer: C) Social media platforms

12. What role does the payment gateway play in e-commerce transactions? A) Managing inventory

B) Providing internet connectivity

C) Facilitating secure payment transactions

D) Handling customer support

Answer: C) Facilitating secure payment transactions

13. What is the primary purpose of encryption in e-commerce security?

A) Protecting against malware

B) Securing physical servers

C) Encoding sensitive information during transmission

D) Preventing unauthorized access to networks

Answer: C) Encoding sensitive information during transmission

14. Which technology is commonly used for encrypting data in e-commerce transactions?

A) Virtual Private Network (VPN)

B) Secure Sockets Layer (SSL) or Transport Layer Security (TLS)

C) Antivirus software

D) Firewall

Answer: B) Secure Sockets Layer (SSL) or Transport Layer Security (TLS)

15. What is the purpose of secure payment gateways in e-commerce?

A) Protecting physical servers

B) Securing customer passwords

C) Ensuring secure transmission of financial information

D) Preventing unauthorized access to networks

Answer: C) Ensuring secure transmission of financial information

16. How do firewalls and security software contribute to e-commerce security?

A) By encrypting data

B) By verifying user identity

C) By preventing unauthorized access to the network

D) By conducting security audits

Answer: C) By preventing unauthorized access to the network

17. What is the role of authentication and authorization in e-commerce security?

A) Protecting against malware

B) Verifying user identity

C) Encrypting data

D) Conducting security audits

Answer: B) Verifying user identity

18. What is the importance of regular updates and patch management in e-commerce security?

A) Protecting physical servers

B) Preventing unauthorized access to networks

C) Ensuring data privacy compliance

D) Mitigating vulnerabilities

Answer: D) Mitigating vulnerabilities

19. Which aspect of e-commerce security involves adhering to regulations like GDPR and CCPA?

A) Risk assessment and monitoring

B) Data privacy and compliance

C) Customer education

D) Physical security measures

Answer: B) Data privacy and compliance

20. What is the purpose of conducting risk assessment and monitoring in e-commerce security?

A) Securing physical servers

B) Preventing unauthorized access to networks

C) Identifying potential vulnerabilities and threats

D) Educating customers

Answer: C) Identifying potential vulnerabilities and threats

21. How does customer education contribute to e-commerce security? A) By securing physical servers

B) By preventing unauthorized access to networks

C) By verifying user identity

D) By promoting safe online practices

Answer: D) By promoting safe online practices

22. Why is physical security important in e-commerce?

A) To prevent data breaches

B) To secure customer passwords

C) To ensure secure transmission of financial information

D) To prevent unauthorized access to hardware and infrastructure

Answer: D) To prevent unauthorized access to hardware and infrastructure

23. Which of the following is a common threat to e-commerce platforms?

A) Weather disruptions

B) Data Breaches

C) Employee strikes

D) Office supply shortages

Answer: B) Data Breaches

24. What is a common method used by cybercriminals in phishing attacks?

A) Sending physical letters

B) Making phone calls

C) Sending deceptive emails or messages

D) Distributing flyers

Answer: C) Sending deceptive emails or messages

25. What is the purpose of malware and viruses in e-commerce threats?

A) Enhancing website performance

B) Disrupting operations and compromising user data

C) Improving customer experience

D) Strengthening network security

Answer: B) Disrupting operations and compromising user data

26. What is the goal of a DDoS attack on an e-commerce website?

A) Stealing customer information

B) Causing financial losses

C) Overwhelming the website's servers with excessive traffic

D) Encrypting sensitive data

Answer: C) Overwhelming the website's servers with excessive traffic

27. How do attackers exploit vulnerabilities in SQL Injection attacks?

A) By intercepting communication between users and the website

B) By inserting malicious SQL queries to access or manipulate the database

C) By tricking users into revealing sensitive information

D) By distributing malware through infected files

Answer: B) By inserting malicious SQL queries to access or manipulate the database

28. What is the objective of a Man-in-the-Middle (MITM) attack?

A) Overwhelming the website's servers with excessive traffic

B) Intercepting communication to steal information or manipulate data

C) Accessing the supply chain network

D) Executing payment frauds

Answer: B) Intercepting communication to steal information or manipulate data

29. What is the risk associated with identity theft in e-commerce? A) Loss of inventory

B) Legal disputes with suppliers

C) Unauthorized access to customer accounts and financial fraud D) Shipping delays

Answer: C) Unauthorized access to customer accounts and financial fraud

30. What aspect of e-commerce does a supply chain attack target?

A) Customer education

B) Payment gateways

C) Physical security measures

D) Weaknesses in the supply chain

Answer: D) Weaknesses in the supply chain

31. What is a common type of payment fraud in e-commerce?

A) Sending counterfeit products

B) Charging excessive shipping fees

C) Stolen credit card information or unauthorized transactions

D) Delaying order fulfillment

Answer: C) Stolen credit card information or unauthorized transactions

32. What is the primary purpose of using Secure Sockets Layer (SSL) encryption in ecommerce?

A) Protecting against phishing attacks

B) Enhancing website performance

C) Encrypting data transmitted between website and users' browsers

D) Securing physical servers

Answer: C) Encrypting data transmitted between website and users' browsers

33. How can strong password policies contribute to e-commerce security?

A) Protecting against malware

B) Preventing unauthorized access to networks

C) Encrypting data

D) Enhancing user authentication

Answer: D) Enhancing user authentication

34. What is the purpose of regularly updating software and security patches in e-commerce?

A) Enhancing website design

B) Ensuring compliance with regulations

C) Patching vulnerabilities that attackers could exploit

D) Preventing server downtime

Answer: C) Patching vulnerabilities that attackers could exploit

35. What is the significance of using reputable payment gateways in e-commerce?

A) Preventing data breaches

B) Ensuring compliance with GDPR

C) Complying with PCI DSS and securely handling payment information

D) Securing physical servers

Answer: C) Complying with PCI DSS and securely handling payment information

36. How does data encryption contribute to e-commerce security?
A) Preventing phishing attacks
B) Securing physical servers
C) Encrypting sensitive data when stored or transmitted
D) Enhancing customer support

Answer: C) Encrypting sensitive data when stored or transmitted

37. What is the purpose of conducting regular security audits and testing in e-commerce?
A) Enhancing website aesthetics
B) Identifying vulnerabilities and weaknesses in the system
C) Preventing employee strikes
D) Improving customer service

Answer: B) Identifying vulnerabilities and weaknesses in the system

38. What is the function of firewalls in e-commerce security?
A) Monitoring and controlling incoming and outgoing traffic
B) Encrypting sensitive data
C) Conducting security audits
D) Enhancing user authentication

Answer: A) Monitoring and controlling incoming and outgoing traffic

39. Why is employee training important in e-commerce security?
A) To prevent natural disasters
B) To enhance website performance
C) To educate employees about security best practices and prevent internal breaches
D) To improve supply chain management

Answer: C) To educate employees about security best practices and prevent internal breaches

40. How does compliance with privacy policies and regulations contribute to e-commerce security?
A) Preventing data breaches
B) Enhancing website design
C) Improving customer support
D) Complying with legal requirements and protecting customer data

Answer: D) Complying with legal requirements and protecting customer data

41. What is the importance of monitoring and responding to suspicious activity in ecommerce?
A) Enhancing user experience
B) Improving website aesthetics
C) Detecting potential security breaches and responding promptly
D) Preventing phishing attacks

Answer: C) Detecting potential security breaches and responding promptly

42. How does regular data backup contribute to e-commerce security?

A) Enhancing website performance

B) Preventing server downtime

C) Protecting against malware

D) Ensuring data can be recovered in case of a security breach or data loss

Answer: D) Ensuring data can be recovered in case of a security breach or data loss

43. Which e-commerce platform is known for its auction-style selling?

A) Amazon

B) eBay

C) Alibaba

D) Walmart

Answer: B) eBay

44. Which e-commerce site specializes in wholesale trading between businesses and consumers?

A) Amazon

B) eBay

C) Alibaba

D) Walmart

Answer: C) Alibaba

45. Which platform is popular for its focus on handmade, vintage, and unique goods?

A) Amazon

B) eBay

C) Etsy

D) Walmart

Answer: C) Etsy

46. Which e-commerce site is renowned for its specialization in electronics?

A) Amazon

B) eBay

C) Best Buy

D) Walmart

Answer: C) Best Buy

47. Which platform targets a younger audience with trendy fashion and beauty products?

A) Amazon

B) ASOS

C) Etsy

D) Walmart

Answer: B) ASOS

48. Which e-commerce site is known for its cashback rewards for purchases?

A) Amazon

B) eBay

C) Rakuten

D) Walmart

Answer: C) Rakuten

49. Which platform is popular for its customer service and wide selection of shoes and clothing? A) Amazon
B) eBay
C) Zappos
D) Walmart
Answer: C) Zappos

49. Which e-commerce platform is similar to Walmart and offers a diverse range of products? A) Amazon
B) Target
C) Alibaba
D) Walmart
Answer: B) Target

50. Which e-commerce site is one of the largest online retailers offering a wide range of products? A) Amazon
B) eBay
C) Alibaba
D) Walmart
Answer: A) Amazon

51. Which platform is primarily focused on handmade, vintage, and unique goods?
A) Alibaba
B) Etsy
C) ASOS
D) Target
Answer: B) Etsy

52. What is the primary characteristic of digital payments?
A) Involves exchange of hard cash
B) Requires physical presence at a bank
C) Transactions occur through digital or online modes
D) Relies on bartering goods instead of currency
Answer: C) Transactions occur through digital or online modes

53. What is the function of a payment gateway in digital payments?
A) Stores payment information on smartphones
B) Facilitates transactions by connecting merchants, banks, and customers
C) Transmits data between the merchant's bank and the customer's bank
D) Enables contactless payments through NFC technology
Answer: B) Facilitates transactions by connecting merchants, banks, and customers

54. Which component of digital payments enables contactless payments?
A) Payment Processor
B) Mobile Wallets
C) Near Field Communication (NFC)
D) QR Codes
Answer: C) Near Field Communication (NFC)

55. What is the role of a payment processor in digital payments?
A) Stores payment information on smartphones
B) Facilitates transactions by connecting merchants, banks, and customers
C) Transmits data between the merchant's bank and the customer's bank
D) Enables contactless payments through NFC technology
Answer: C) Transmits data between the merchant's bank and the customer's bank

56. Which stakeholder in digital payments provides the infrastructure and accounts necessary for transactions?
A) Financial Institutions
B) Payment Service Providers (PSPs)
C) Regulatory Bodies/Government Agencies
D) Security Firms
Answer: A) Financial Institutions

57. What are mobile wallets in the context of digital payments?
A) Scannable codes that store payment information
B) Decentralized forms of currency like Bitcoin
C) Apps or platforms that store payment information for transactions through smartphones D) Technology enabling contactless payments
Answer: C) Apps or platforms that store payment information for transactions through smartphones

58. What technology enables easy transactions through scannable codes?
A) Payment Gateway
B) Payment Processor
C) QR Codes
D) NFC Technology
Answer: C) QR Codes

59. Who are the primary users making payments or transactions in digital payment systems?
A) Financial Institutions
B) Customers/Users
C) Merchants/Retailers
D) Payment Service Providers (PSPs)
Answer: B) Customers/Users

60. Which stakeholder ensures the security of digital payment systems by providing encryption and cybersecurity services?
A) Financial Institutions
B) Security Firms
C) Merchants/Retailers
D) Payment Service Providers (PSPs)
Answer: B) Security Firms

61. What is the function of regulatory bodies/government agencies in digital payments? A) Providing encryption and cybersecurity services
B) Developing and maintaining technology for digital payment systems

C) Creating and enforcing rules, regulations, and standards to ensure security and fairness D) Facilitating transactions between merchants and customers

Answer: C) Creating and enforcing rules, regulations, and standards to ensure security and fairness

62. Which of the following is a widely used payment method that allows users to make cashless transactions online, in digital payment apps, and through PoS machines?

A) Unified Payment Interface (UPI)
B) Electronic Wallets (e-Wallets)
C) Banking Cards
D) Unstructured Supplementary Service Data (USSD)

Answer: C) Banking Cards

63. What is the main advantage of using Unified Payment Interface (UPI) for digital payments?

A) Allows users to store financial information and make quick transactions
B) Culminates numerous bank accounts into a single application for easy money transfer
C) Enables mobile banking services through basic phones without internet connectivity
D) Facilitates digital payments using Aadhar-linked accounts

Answer: B) Culminates numerous bank accounts into a single application for easy money transfer

64. Which digital payment mode allows users to store money for future online transactions and is protected with a password?

A) Unified Payment Interface (UPI)
B) Banking Cards
C) Electronic Wallets (e-Wallets)
D) Unstructured Supplementary Service Data (USSD)

Answer: C) Electronic Wallets (e-Wallets)

65. What technology enables mobile banking services through basic phones without the need for internet connectivity?

A) Unified Payment Interface (UPI)
B) Unstructured Supplementary Service Data (USSD)
C) Electronic Wallets (e-Wallets)
D) Aadhar-enabled Payments System (AEPS)

Answer: B) Unstructured Supplementary Service Data (USSD)

66. Which digital payment system leverages Aadhar-linked accounts for transferring money between two Aadhar-linked Bank Accounts?

A) Unified Payment Interface (UPI)
B) Electronic Wallets (e-Wallets)
C) Aadhar-enabled Payments System (AEPS)
D) Banking Cards

Answer: C) Aadhar-enabled Payments System (AEPS)

67. What is the primary characteristic of USSD technology in digital payments? A) Requires internet connectivity

B) Allows users to store financial information

C) Facilitates mobile banking services through basic phones

D) Utilizes scannable codes for transactions

Answer: C) Facilitates mobile banking services through basic phones

68. Which digital payment mode enables users to make transactions without the need to type in card or bank details?

A) Unified Payment Interface (UPI)

B) Banking Cards

C) Electronic Wallets (e-Wallets)

D) Unstructured Supplementary Service Data (USSD)

Answer: A) Unified Payment Interface (UPI)

69. Which component of digital payments facilitates transactions by connecting merchants, banks, and customers, and ensures secure transfer of sensitive information?

A) Banking Cards

B) Payment Gateway

C) Payment Processor

D) Mobile Wallets

Answer: B) Payment Gateway

70. What distinguishes AEPS from other digital payment systems? A) It requires internet connectivity for transactions.

B) It facilitates transactions without Aadhar authentication.

C) It leverages Aadhar-linked accounts for transactions.

D) It primarily uses scannable codes for transactions.

Answer: C) It leverages Aadhar-linked accounts for transactions.

71. Which digital payment mode witnessed over 2 billion transactions in October, making it one of the most popular modes in 2020?

A) Unified Payment Interface (UPI)

B) Electronic Wallets (e-Wallets)

C) Aadhar-enabled Payments System (AEPS) D) Banking Cards

Answer: A) Unified Payment Interface (UPI)

72. What is the primary characteristic of phishing scams in digital payments? A) Direct bank transfers

B) Fake messages, emails, or websites

C) Contactless payment methods

D) Biometric authentication

Answer: B) Fake messages, emails, or websites

73. How do fraudsters typically use stolen personal information in identity theft?

A) To make unauthorized transactions

B) To enable biometric authentication

C) To download antivirus software

D) To install malware on devices

Answer: A) To make unauthorized transactions

74. What is the objective of an account takeover in digital payments?

A) To enable biometric authentication

B) To make unauthorized transactions

C) To regularly monitor credit reports

D) To install antivirus software

Answer: B) To make unauthorized transactions

75. What is card skimming in digital payments?

A) Using strong, unique passwords

B) Making contactless payments

C) Illegally copying credit or debit card information

D) Installing antivirus software

Answer: C) Illegally copying credit or debit card information

76. What preventive measure is recommended for combating malware and spyware attacks?

A) Making contactless payments

B) Regularly updating antivirus and anti-malware software

C) Using strong, unique passwords

D) Enabling two-factor authentication

Answer: B) Regularly updating antivirus and anti-malware software

77. What are unauthorized transactions in digital payments?

A) Transactions made with the account holder's consent

B) Transactions made without the account holder's knowledge or consent

C) Transactions using biometric authentication

D) Transactions monitored by antivirus software

Answer: B) Transactions made without the account holder's knowledge or consent

78. How can individuals protect themselves from social engineering attacks?

A) Enabling transaction notifications

B) Regularly updating operating systems and apps

C) Being cautious of unsolicited calls or messages asking for personal information

D) Checking account statements for unfamiliar transactions

Answer: C) Being cautious of unsolicited calls or messages asking for personal information

79. What security measures are mandated by the Reserve Bank of India (RBI) for digital transactions?

A) Regular monitoring of transactions

B) Customer education about safe practices

C) Implementation of robust security measures like two-factor authentication

D) Dispute resolution process

Answer: C) Implementation of robust security measures like two-factor authentication

80. How does the RBI encourage customer awareness regarding digital payments?

A) By providing prompt redressal for unauthorized transactions

B) Through educational campaigns and notifications

C) By limiting customer liability in case of unauthorized transactions

D) By establishing a Payment System Board

Answer: B) Through educational campaigns and notifications

81. What is the liability of customers in cases of unauthorized transactions, as per RBI guidelines?
A) Unlimited liability
B) No liability
C) Limited liability, subject to certain conditions and timeline for reporting D) Liability transferred to the bank
Answer: C) Limited liability, subject to certain conditions and timeline for reporting

82. Which legislation establishes the regulatory framework for payment systems in India?
A) RBI Act, 1934
B) Companies Act, 2013
C) Payment and Settlement Systems Act, 2007
D) Indian Contract Act, 1872
Answer: C) Payment and Settlement Systems Act, 2007

83. What is the role of the Reserve Bank of India (RBI) under the Payment and Settlement Systems Act, 2007?
A) Licensing of payment system operators
B) Regulation of payment systems
C) Designation of payment systems
D) All of the above
Answer: D) All of the above

84. What does the concept of "settlement finality" entail?
A) Settlements are reversible under certain circumstances
B) Settlements are irrevocable and final once deemed so
C) Settlements are subject to ongoing monitoring by the RBI D) Settlements are regulated by the Payment System Board
Answer: B) Settlements are irrevocable and final once deemed so

85. What is the objective of the Payment System Board established within the RBI?
A) Oversight and monitoring of payment systems
B) Enforcement of penalties
C) Licensing of payment system operators
D) Regulation of payment systems
Answer: A) Oversight and monitoring of payment systems

UNIT-V

1. What is one of the essential practices for securing endpoint devices?
A) Avoiding software updates
B) Disabling firewalls
C) Implementing strong authentication
D) Sharing passwords openly
Answer: C) Implementing strong authentication

2. Which practice is recommended for securing mobile phones?
A) Using untrusted sources for app downloads
B) Enabling encryption for stored data
C) Avoiding regular software updates
D) Disabling lock screen security
Answer: B) Enabling encryption for stored data

3. What is a key aspect of a robust password policy?
A) Allowing common passwords
B) Requiring infrequent password changes
C) Implementing multi-factor authentication (MFA)
D) Encouraging password sharing
Answer: C) Implementing multi-factor authentication (MFA)

4. Why is it essential to keep software updated on endpoint devices?
A) To maintain vulnerabilities and security flaws
B) To prevent unauthorized access to the device
C) To ensure compatibility with outdated applications D) To reduce the need for strong authentication
Answer: A) To maintain vulnerabilities and security flaws

5. What is the purpose of encrypting sensitive data on endpoint devices?
A) To simplify data access
B) To prevent unauthorized access if the device is lost or stolen
C) To increase the risk of data breaches
D) To allow easy data sharing with others
Answer: B) To prevent unauthorized access if the device is lost or stolen

6. Which action is NOT recommended for mobile phone security?
A) Using VPNs on public networks
B) Regularly updating the operating system and apps
C) Jailbreaking or rooting the device
D) Enabling remote wipe/locate features
Answer: C) Jailbreaking or rooting the device

7. What is the purpose of implementing multi-factor authentication (MFA)?
A) To simplify the login process
B) To add an extra layer of security
C) To encourage password sharing
D) To reduce the need for strong passwords
Answer: B) To add an extra layer of security

8. Why is it essential to avoid jailbreaking or rooting mobile phones?
A) To increase the risk of data breaches
B) To simplify device customization
C) To avoid exposing the device to more risks
D) To enable encryption for stored data
Answer: C) To avoid exposing the device to more risks

9. What is the primary purpose of a password policy?
A) To encourage password sharing
B) To provide guidelines for creating strong passwords
C) To discourage regular password changes
D) To allow unrestricted access to accounts
Answer: B) To provide guidelines for creating strong passwords

10. What is one of the key elements of a robust password policy?
A) Allowing common passwords
B) Prohibiting multi-factor authentication (MFA)
C) Requiring periodic password changes

D) Encouraging password sharing

Answer: C) Requiring periodic password changes

11. Why is it important to review and manage app permissions on mobile phones?

A) To limit what data apps can access

B) To encourage app downloads from untrusted sources

C) To simplify the app installation process D) To increase the risk of data breaches

Answer: A) To limit what data apps can access

12. What is one of the key practices for securing endpoint devices?

A) Sharing passwords openly

B) Disabling firewalls

C) Regularly backing up important data

D) Allowing unrestricted access to accounts

Answer: C) Regularly backing up important data

13. What is the purpose of enabling encryption for mobile data?

A) To simplify data access

B) To prevent unauthorized access if the device is lost or stolen

C) To increase the risk of data breaches

D) To allow easy data sharing with others

Answer: B) To prevent unauthorized access if the device is lost or stolen

14. What is the primary purpose of using strong authentication methods?

A) To simplify the login process

B) To add an extra layer of security

C) To encourage password sharing

D) To reduce the need for regular software updates

Answer: B) To add an extra layer of security

15. Why is it important to avoid installing apps from untrusted sources on mobile phones?

A) To simplify the app installation process

B) To increase the risk of data breaches

C) To encourage customization of the device

D) To reduce the risk of installing malicious software

Answer: D) To reduce the risk of installing malicious software

16. What is the first step in security patch management? A) Testing

B) Acquisition

C) Assessment

D) Identification

Answer: D) Identification

17. What is the purpose of the assessment phase in patch management? A) Testing the patches

B) Evaluating the severity and impact of vulnerabilities

C) Applying patches to the production environment

D) Monitoring for new vulnerabilities

Answer: B) Evaluating the severity and impact of vulnerabilities

18. Where should patches be obtained from during the acquisition

phase?

A) Unverified sources

B) Official sources

C) Social media

D) Online forums

Answer: B) Official sources

19. Why is testing patches necessary before deployment?

A) To delay the patching process

B) To ensure they work as intended and don't create conflicts

C) To avoid monitoring and maintenance

D) To minimize documentation requirements

Answer: B) To ensure they work as intended and don't create conflicts

20. What should be done after deploying patches to the production environment?

A) Stop monitoring

B) Start testing again

C) Verification

D) Acquisition

Answer: C) Verification

21. What is the purpose of monitoring and maintenance in patch management? A) To avoid patching systems

B) To ensure all systems are up to date with the latest security patches

C) To avoid documentation

D) To skip the identification phase

Answer: B) To ensure all systems are up to date with the latest security patches

22. Why is documentation essential in patch management? A) To avoid audits

B) To maintain records of applied patches and any issues encountered

C) To reduce the need for testing

D) To speed up the deployment process

Answer: B) To maintain records of applied patches and any issues encountered

23. Which of the following is NOT a phase in security patch management?

A) Assessment

B) Deployment

C) Ignoring

D) Verification

Answer: C) Ignoring

24. What is the primary goal of effective patch management?

A) To increase the likelihood of security breaches

B) To mitigate the risks associated with security vulnerabilities

C) To delay the deployment of patches

D) To avoid acquiring patches from official sources

Answer: B) To mitigate the risks associated with security vulnerabilities

25. Which phase involves confirming that patches have been successfully applied?
A) Testing
B) Acquisition
C) Verification
D) Documentation
Answer: C) Verification

26. Why is data backup important?
A) To increase system performance
B) To prevent downloading third-party software
C) To safeguard against data loss
D) To automate system updates
Answer: C) To safeguard against data loss

27. What is a recommended practice for effective data backup?
A) Storing backups in a single location
B) Verifying backups only once a year
C) Using encryption for sensitive data
D) Testing backups only during system crashes
Answer: C) Using encryption for sensitive data

28. Which factor determines the frequency of data backups?
A) The amount of available storage space
B) The importance of the data and its rate of change
C) The speed of the internet connection
D) The number of third-party software installed
Answer: B) The importance of the data and its rate of change

29. What is the purpose of testing the restoration process for backups?
A) To automate the backup process
B) To ensure backups are encrypted
C) To verify that backups are usable
D) To increase system performance
Answer: C) To verify that backups are usable

30. Why should users prioritize important data for backup?
A) To reduce system performance
B) To simplify the backup process
C) To increase the risk of data loss
D) To ensure critical data is protected
Answer: D) To ensure critical data is protected

31. Where should users obtain software from to ensure safety?
A) Unverified third-party websites
B) Reputable sources such as official websites or trusted app stores
C) Random online forums
D) Social media platforms
Answer: B) Reputable sources such as official websites or trusted app stores

32. What should users check to gauge the reliability of third-party software?
A) The color scheme of the software website
B) The number of advertisements on the website
C) Reviews, ratings, and user feedback

D) The font size used on the software's download page

Answer: C) Reviews, ratings, and user feedback

33. What should users do when installing third-party software?

A) Ignore the permissions requested by the software

B) Install software from any available source

C) Review and consider the permissions requested

D) Install software without reading the license agreement

Answer: C) Review and consider the permissions requested

34. Why is it important to keep all software updated?

A) To increase system vulnerabilities

B) To prevent downloading third-party software

C) To automate the data backup process D) To patch security vulnerabilities

Answer: D) To patch security vulnerabilities

35. What should users do with unused software?

A) Keep it installed for future use

B) Uninstall it to reduce potential vulnerabilities

C) Share it with friends and family

D) Ignore its presence on the system

Answer: B) Uninstall it to reduce potential vulnerabilities

36. What should users do before downloading third-party software from a website?

A) Verify the authenticity of the website and software

B) Install the software immediately without hesitation

C) Skip reading the license agreement

D) Disable antivirus software

Answer: A) Verify the authenticity of the website and software

37. Why is it important to read the license agreement before installing third-party software?

A) To increase system performance

B) To understand the terms and conditions of using the software

C) To avoid encryption of data backups

D) To simplify the software installation process

Answer: B) To understand the terms and conditions of using the software

38. What is a recommended practice for managing third-party software?

A) Avoid regular updates to maintain system stability

B) Share downloaded software with others

C) Back up data regularly to mitigate potential issues

D) Download software from unverified sources for variety

Answer: C) Back up data regularly to mitigate potential issues

39. What should users consider using to test potentially risky software?

A) Virtual environments or sandboxes

B) Sharing software with colleagues

C) Ignoring reviews and ratings

D) Installing it directly on the main system

Answer: A) Virtual environments or sandboxes

40. Which action enhances security when managing third-party software?

A) Disabling antivirus software

B) Sharing passwords openly

C) Regularly updating all software

D) Avoiding backups of critical data

Answer: C) Regularly updating all software

41. What is the purpose of establishing device usage guidelines in a device security policy?

A) To restrict all device usage within the organization

B) To specify who can use company devices and for what purposes

C) To encourage unlimited device usage

D) To enforce strict penalties for device misuse

Answer: B) To specify who can use company devices and for what purposes

42. What does an acceptable use policy typically cover in a device security policy? A) Employee salaries and benefits

B) Browsing certain websites and downloading software

C) Company mission and vision statements

D) Personal hobbies and interests

Answer: B) Browsing certain websites and downloading software

43. What is recommended for password and authentication in a device security policy?

A) Weak, easily guessable passwords

B) Sharing passwords among colleagues

C) Strong, unique passwords for each device and multi-factor authentication

D) Passwords written on sticky notes attached to devices

Answer: C) Strong, unique passwords for each device and multi-factor authentication

44. Why is data encryption mandated in a device security policy?

A) To make data easier to access

B) To increase the risk of data breaches

C) To prevent unauthorized access to sensitive data

D) To slow down device performance

Answer: C) To prevent unauthorized access to sensitive data

45. What is the purpose of regular updates and patching in a device security policy?

A) To keep devices outdated and vulnerable

B) To reduce device performance

C) To protect against vulnerabilities by installing the latest security updates

D) To increase the risk of security breaches

Answer: C) To protect against vulnerabilities by installing the latest security updates

46. What does access control entail in a device security policy?

A) Allowing unlimited access to all data and systems

B) Limiting access to data and systems based on job roles and responsibilities

C) Providing access to external parties without restrictions

D) Sharing access credentials openly

Answer: B) Limiting access to data and systems based on job roles and responsibilities

47. What protocols are typically defined for secure remote access in a device security policy?

A) Use of outdated and insecure connections

B) Avoiding virtual private networks (VPNs)

C) Secure remote access using VPNs and other secure connections

D) Sharing login credentials openly

Answer: C) Secure remote access using VPNs and other secure connections

48. Why are procedures for handling lost or stolen devices established in a device security policy?

A) To encourage device theft

B) To avoid reporting lost or stolen devices

C) To mitigate potential data breaches

D) To increase the risk of unauthorized access

Answer: C) To mitigate potential data breaches

49. What is the purpose of software and application management guidelines in a device security policy?

A) To install outdated and insecure software

B) To prevent employees from installing any software

C) To specify guidelines for installing, updating, and removing software and applications

D) To encourage employees to install unauthorized software

Answer: C) To specify guidelines for installing, updating, and removing software and applications

50. Why is employee training included in a device security policy?

A) To increase the risk of security incidents

B) To reduce employee awareness of potential threats

C) To educate employees about security best practices and potential threats

D) To encourage employees to share sensitive information

Answer: C) To educate employees about security best practices and potential threats

51. What is the primary function of a host firewall?

A) Scanning for viruses

B) Filtering network traffic

C) Encrypting data in transit

D) Managing user permissions

Answer: B) Filtering network traffic

52. What does antivirus software primarily protect against?

A) Unauthorized network access

B) Phishing attacks

C) Malicious software (malware)

D) Hardware failures

Answer: C) Malicious software (malware)

53. Which best practice involves using complex passwords and multi-factor authentication?

A) Regular backups

B) Secure Wi-Fi networks

C) Host firewall configuration

D) User authentication

Answer: D) User authentication

54. What is the significance of regular software updates in cybersecurity?

A) They prevent hardware failures

B) They minimize the need for backups

C) They patch security vulnerabilities

D) They improve Wi-Fi network speed

Answer: C) They patch security vulnerabilities

55. How does a host firewall contribute to computer security?

A) By encrypting sensitive data

B) By detecting phishing emails

C) By controlling network traffic

D) By managing user permissions

Answer: C) By controlling network traffic

56. Which measure involves restricting user access to only necessary data and systems?

A) Regular backups

B) Least privilege

C) Encryption of sensitive data D) Multi-factor authentication

Answer: B) Least privilege

57. What is the primary purpose of antivirus software?

A) Filtering network traffic

B) Encrypting sensitive data

C) Detecting and removing malware

D) Managing user authentication

Answer: C) Detecting and removing malware

58. What is the significance of implementing both host firewalls and antivirus software?

A) They increase Wi-Fi network speed

B) They prevent hardware failures

C) They provide complementary protection

D) They eliminate the need for regular backups

Answer: C) They provide complementary protection

59. What does a host firewall help prevent?

A) Unauthorized network access

B) Malware infections

C) Data breaches

D) Phishing attacks

Answer: A) Unauthorized network access

60. Which practice involves creating duplicate copies of important data?

A) Multi-factor authentication

B) Regular backups

C) Secure Wi-Fi networks

D) Host firewall configuration

Answer: B) Regular backups

61. What is the primary role of a host firewall in cybersecurity?
A) Scanning for viruses
B) Monitoring system activities
C) Filtering network traffic
D) Managing user permissions
Answer: C) Filtering network traffic

62. Why are regular security audits important in cybersecurity?
A) To increase Wi-Fi network speed
B) To identify and address vulnerabilities
C) To manage user authentication
D) To encrypt sensitive data
Answer: B) To identify and address vulnerabilities

63. How does antivirus software protect against malware?
A) By encrypting sensitive data
B) By filtering network traffic
C) By detecting and removing malicious software
D) By managing user permissions
Answer: C) By detecting and removing malicious software

64. What is the significance of multi-factor authentication in cybersecurity? A) It improves Wi-Fi network speed
B) It prevents hardware failures
C) It adds an extra layer of security
D) It eliminates the need for regular backups
Answer: C) It adds an extra layer of security

65. What is the primary purpose of encrypting sensitive data?
A) To prevent unauthorized network access
B) To detect phishing attacks
C) To minimize the impact of hardware failures
D) To protect data confidentiality
Answer: D) To protect data confidentiality

66. What is the primary purpose of configuring firewall rules based on the principle of least privilege?
A) To maximize network speed
B) To block all inbound traffic
C) To allow only necessary traffic
D) To disable firewall logging
Answer: C) To allow only necessary traffic

67. Why is it important to regularly update firewall software?
A) To enhance Wi-Fi security
B) To improve network speed
C) To ensure the latest security patches
D) To enable default deny policy
Answer: C) To ensure the latest security patches

68. What is the purpose of enabling logging and monitoring in firewall management?
A) To block all outbound traffic
B) To track firewall activities
C) To disable real-time protection
D) To hide the network name (SSID)

Answer: B) To track firewall activities

69. What does a default deny policy aim to achieve in firewall management?
A) To allow all traffic by default
B) To block all inbound traffic
C) To minimize the attack surface
D) To enable real-time scanning
Answer: C) To minimize the attack surface

70. What is a key benefit of enabling real-time protection in antivirus management? A) It speeds up system scans
B) It reduces the need for scheduled scans
C) It monitors files and processes for suspicious behavior
D) It automatically updates virus definitions
Answer: C) It monitors files and processes for suspicious behavior

71. Why is user education an important aspect of antivirus management? A) To configure firewall settings
B) To ensure router compatibility
C) To prevent malware infections
D) To enable WPA3 encryption
Answer: C) To prevent malware infections

72. Which encryption standard is recommended for Wi-Fi security?
A) WPA2
B) WEP
C) WPA3
D) None of the above
Answer: C) WPA3

73. What is the purpose of hiding the network name (SSID) in Wi-Fi security?
A) To increase network speed
B) To prevent unauthorized access
C) To enable MAC address filtering
D) To minimize router firmware updates
Answer: B) To prevent unauthorized access

74. How does MAC address filtering contribute to Wi-Fi security?
A) By hiding the network name (SSID)
B) By encrypting network traffic
C) By restricting access to specific devices
D) By enabling guest networks
Answer: C) By restricting access to specific devices

75. What is the purpose of using a VPN in Wi-Fi security?
A) To disable firewall settings
B) To enable WPS
C) To encrypt internet traffic on public networks
D) To monitor network logs
Answer: C) To encrypt internet traffic on public networks

76. What is the first step in creating a basic security policy?
A) Implement Permissions

B) Define Security Policies

C) Conduct a Risk Assessment

D) Employee Training

Answer: C) Conduct a Risk Assessment

77. Which principle advocates giving users only the necessary permissions to perform their tasks?

A) Least Privilege

B) Separation of Duties

C) Role-Based Access Control

D) Access Control Policies

Answer: A) Least Privilege

78. What is the purpose of defining data encryption policies in a security policy?

A) To enforce password guidelines

B) To specify roles and permissions

C) To determine how often systems should be updated

D) To specify when and where encryption should be applied to sensitive data

Answer: D) To specify when and where encryption should be applied to sensitive data

79. How can access controls be enforced in a security policy?

A) Through regular audits and updates

B) By implementing user roles

C) Through employee training

D) Using tools like access control lists (ACLs) or Role-Based Access Control (RBAC)

Answer: D) Using tools like access control lists (ACLs) or Role-Based Access Control (RBAC)

80. Why is it important to periodically review and update security policies and permissions?

A) To educate employees about security policies

B) To align security policies with relevant regulations and standards

C) To implement data encryption policies

D) To conduct a risk assessment

Answer: B) To align security policies with relevant regulations and standards