

Chapter 8: Cyber Security

Q1. Which of the following are the three basic pillars of cyber security often abbreviated as CIA?

- A) Cost, Investment, Analysis
- B) Control, Identity, Access
- C) Coding, Installation, Automation
- D) Confidentiality, Integrity, Availability

Answer: D) Confidentiality, Integrity, Availability

Q2. Which of the following describes 'Confidentiality' in cyber security?

- A) Ensuring hardware is expensive
- B) Ensuring data speed is fast
- C) Ensuring information is available to everyone
- D) Ensuring information is accessible only to authorized users

Answer: D) Ensuring information is accessible only to authorized users

Q3. Which of the following describes 'Integrity' in cyber security?

- A) Ensuring data is accurate and has not been tampered with
- B) Ensuring data is deleted
- C) Ensuring data is always public
- D) Ensuring data access is slow

Answer: A) Ensuring data is accurate and has not been tampered with

Q4. Which of the following describes 'Availability' in cyber security?

- A) Ensuring authorized users can access data/systems when needed
- B) Ensuring only hackers can access data
- C) Ensuring data is deleted regularly
- D) Ensuring data is hidden permanently

Answer: A) Ensuring authorized users can access data/systems when needed

Q5. Which of the following describes a 'Threat' in cyber security?

- A) A method used to fix a vulnerability
- B) A type of firewall hardware
- C) A potential danger that could exploit a vulnerability to cause harm
- D) A type of antivirus software

Answer: C) A potential danger that could exploit a vulnerability to cause harm

Q6. Which of the following describes a 'Vulnerability' in cyber security?

- A) A type of encryption key
- B) A fully secure system with no weaknesses
- C) A weakness in a system that could be exploited by a threat
- D) A type of antivirus software

Answer: C) A weakness in a system that could be exploited by a threat

Q7. Which of the following describes 'Risk' in the context of cyber security?

- A) A guaranteed security breach with no possibility of prevention
- B) The potential for loss or damage when a threat exploits a vulnerability
- C) A type of firewall hardware
- D) A type of antivirus software

Answer: B) The potential for loss or damage when a threat exploits a vulnerability

Q8. Which of the following describes 'Security Policies'?

- A) A type of network cable
- B) A type of malware
- C) A type of hardware component
- D) Documented rules and guidelines governing how an organization protects its information assets

Answer: D) Documented rules and guidelines governing how an organization protects its information assets

Q9. Which of the following describes 'Security Mechanisms'?

- A) A type of malware
- B) Technical and procedural measures implemented to protect systems and data
- C) A type of cyber threat
- D) A type of vulnerability

Answer: B) Technical and procedural measures implemented to protect systems and data

Q10. Which of the following is a recommended practice for creating a strong password?

- A) Using a mix of letters, numbers and special characters, avoiding easily guessable information
- B) Using the same simple password everywhere
- C) Using '123456' for all accounts
- D) Using your name and date of birth

Answer: A) Using a mix of letters, numbers and special characters, avoiding easily guessable information

Q11. Which of the following browser feature allows browsing without saving history, cookies, or form data?

- A) In Private/Incognito Browsing
- B) Bookmarks save favorite websites
- C) Extensions add browser features
- D) Downloads folder stores downloaded files

Answer: A) In Private/Incognito Browsing

Q12. Which of the following is used to identify a secure website while browsing?

- A) A colorful website design
- B) A website with many advertisements
- C) HTTP without 'S' and no padlock symbol
- D) HTTPS and the padlock symbol in the address bar

Answer: D) HTTPS and the padlock symbol in the address bar

Q13. Which of the following describes clearing 'Cookies' as a safe browsing practice?

- A) Uninstalling the web browser permanently
- B) Disconnecting from the internet permanently
- C) Removing small stored data files that websites use to track browsing/preferences
- D) Deleting the entire operating system

Answer: C) Removing small stored data files that websites use to track browsing/preferences

Q14. Which of the following describes a computer 'Virus' as a security threat?

- A) A type of antivirus software
- B) A type of legitimate software update
- C) A self-replicating malicious program that attaches to files and spreads to other systems
- D) A type of firewall hardware

Answer: C) A self-replicating malicious program that attaches to files and spreads to other systems

Q15. Which of the following describes a computer 'Worm' as a security threat?

- A) A type of legitimate software update
- B) A self-replicating malware that spreads across networks without needing to attach to a host file
- C) A type of antivirus software
- D) A type of firewall hardware

Answer: B) A self-replicating malware that spreads across networks without needing to attach to a host file

Q16. Which of the following describes a 'Trojan Horse' as a security threat?

- A) Malicious software disguised as legitimate software to trick users into installing it
- B) A type of firewall hardware
- C) A type of antivirus software
- D) A type of legitimate software update

Answer: A) Malicious software disguised as legitimate software to trick users into installing it

Q17. Which of the following describes 'Spyware' as a security threat?

- A) A type of antivirus software
- B) Software that secretly monitors user activity and sends data to a third party
- C) A type of legitimate software update
- D) A type of firewall hardware

Answer: B) Software that secretly monitors user activity and sends data to a third party

Q18. Which of the following describes the umbrella term for malicious software including viruses, worms, and trojans?

- A) Malware

- B) Firmware is permanent device software, not necessarily malicious
- C) Shareware is trial legitimate software
- D) Freeware is free legitimate software

Answer: A) Malware

Q19. Which of the following describes 'Netiquettes'?

- A) A type of firewall hardware
- B) A type of network cable
- C) Rules of etiquette to be followed while communicating on the internet
- D) A type of malware

Answer: C) Rules of etiquette to be followed while communicating on the internet

Q20. Which of the following is the correct full form of DOS as a type of cyber attack?

- A) Data Output Service is not a standard cyber attack term
- B) Denial of Service
- C) Disk Operating System is unrelated to this cyber attack context
- D) Digital Operating Standard is not a standard cyber attack term

Answer: B) Denial of Service

Q21. Which of the following describes a DOS (Denial of Service) attack?

- A) An attack that overwhelms a system with traffic to make it unavailable to legitimate users
- B) A type of antivirus scan
- C) A type of legitimate software update
- D) A type of encrypted communication

Answer: A) An attack that overwhelms a system with traffic to make it unavailable to legitimate users

Q22. Which of the following describes a DDOS (Distributed Denial of Service) attack?

- A) A type of legitimate network monitoring tool
- B) A single-source attack only
- C) A type of antivirus software
- D) A DOS attack launched simultaneously from multiple distributed sources/systems

Answer: D) A DOS attack launched simultaneously from multiple distributed sources/systems

Q23. Which of the following describes 'Phishing' as a cyber security threat?

- A) A legitimate marketing email
- B) A fraudulent attempt to obtain sensitive information by pretending to be a trustworthy source
- C) A type of firewall setting
- D) A type of antivirus feature

Answer: B) A fraudulent attempt to obtain sensitive information by pretending to be a trustworthy source

Q24. Which of the following is a recommended action upon recognizing an attempted phishing email?

- A) Forwarding it to all your contacts
- B) Clicking every link to verify its authenticity
- C) Not clicking any links/attachments and reporting or deleting the email
- D) Replying with your personal/banking details

Answer: C) Not clicking any links/attachments and reporting or deleting the email

Q25. Which of the following describes 'Basics of Software Licensing'?

- A) Legal terms and conditions governing the use, distribution, and modification of software
- B) A type of firewall hardware
- C) A type of network cable
- D) A type of malware

Answer: A) Legal terms and conditions governing the use, distribution, and modification of software

Q26. Which of the following Act governs electronic transactions, digital signatures, and cyber crimes in India?

- A) IT Act 2000
- B) Companies Act
- C) Right to Information Act
- D) Consumer Protection Act

Answer: A) IT Act 2000

Q27. Which of the following describes the objective of the Cyber Security module as stated in the syllabus?

- A) To learn only presentation design
- B) To learn only spreadsheet formulas
- C) To know about security features and vulnerabilities and secure a network from attacks
- D) To learn only word processing skills

Answer: C) To know about security features and vulnerabilities and secure a network from attacks

Q28. Which of the following describes 'unsolicited e-mail' commonly known as spam?

- A) Unwanted, bulk emails sent without the recipient's consent
- B) Emails from known, trusted contacts only
- C) Official government emails only
- D) Emails saved in the Drafts folder

Answer: A) Unwanted, bulk emails sent without the recipient's consent

Q29. Which of the following is a recommended practice regarding fraudulent and unsolicited emails?

- A) Opening every attachment regardless of sender
- B) Forwarding suspicious emails to all contacts
- C) Replying with personal information to verify legitimacy
- D) Being cautious, not opening suspicious attachments, and verifying senders

Answer: D) Being cautious, not opening suspicious attachments, and verifying senders

Q30. Which of the following describes 'Data Security and protection' as a broad concept?

- A) Measures taken to make data publicly available to everyone
- B) Measures taken to slow down data processing
- C) Measures taken to delete all data permanently
- D) Measures taken to protect data from unauthorized access, corruption, or loss

Answer: D) Measures taken to protect data from unauthorized access, corruption, or loss

Q31. Which of the following describes a Trojan Horse in cyber security?

- A) A type of firewall
- B) A type of encryption
- C) Malicious software disguised as legitimate software to trick users into installing it
- D) A type of antivirus

Answer: C) Malicious software disguised as legitimate software to trick users into installing it

Q32. Which of the following describes Adware?

- A) A type of antivirus
- B) A type of firewall

- C) Software that automatically displays or downloads unwanted advertisements
- D) A type of operating system

Answer: C) Software that automatically displays or downloads unwanted advertisements

Q33. Which of the following describes a Keylogger?

- A) A type of firewall
- B) A type of antivirus
- C) Malicious software/hardware that records keystrokes to steal sensitive information like passwords
- D) A type of legitimate typing tool

Answer: C) Malicious software/hardware that records keystrokes to steal sensitive information like passwords

Q34. Which of the following describes a Zero-day vulnerability?

- A) A type of antivirus feature
- B) A type of firewall setting
- C) A vulnerability that has existed for zero days and poses no risk
- D) A security flaw that is exploited by attackers before the vendor releases a fix/patch

Answer: D) A security flaw that is exploited by attackers before the vendor releases a fix/patch

Q35. Which of the following is a Password Manager software used for?

- A) A type of virus
- B) Securely storing and managing complex, unique passwords for different accounts
- C) Sharing your passwords with others
- D) A type of firewall

Answer: B) Securely storing and managing complex, unique passwords for different accounts

Q36. Which of the following describes Biometric Authentication?

- A) Using unique physical characteristics like fingerprints or facial recognition to verify identity
- B) Using only a text password
- C) Using only a security question
- D) Using only an email address

Answer: A) Using unique physical characteristics like fingerprints or facial recognition to verify identity

Q37. Which of the following describes a Data Breach?

- A) A password change
- B) A software update
- C) A routine data backup
- D) An incident where sensitive/confidential data is accessed or disclosed without authorization

Answer: D) An incident where sensitive/confidential data is accessed or disclosed without authorization

Q38. Which of the following describes a Privacy Policy on a website?

- A) A type of virus warning
- B) A type of software license only for developers
- C) A type of advertisement
- D) Explains how the website collects, uses, and protects user data

Answer: D) Explains how the website collects, uses, and protects user data

Q39. Which of the following describes Two-Factor Authentication (2FA)?

- A) A type of virus
- B) Using the same password twice
- C) A type of antivirus only
- D) A security process requiring two different forms of verification to access an account

Answer: D) A security process requiring two different forms of verification to access an account

Q40. Which of the following is a recommended practice for creating passwords?

- A) Using '123456' for all accounts
- B) Using a unique, complex password for each account
- C) Writing passwords on a sticky note on your monitor
- D) Using your date of birth as a password

Answer: B) Using a unique, complex password for each account

Q41. Which of the following should you do before clicking a link in an unexpected email?

- A) Forward it to friends
- B) Click immediately
- C) Reply with personal information
- D) Verify the sender and hover over the link to check its authenticity

Answer: D) Verify the sender and hover over the link to check its authenticity

Q42. Which of the following is a benefit of regularly backing up important data?

- A) Deletes original files
- B) Slows down the computer permanently
- C) Increases risk of virus attack
- D) Protection against data loss due to malware, hardware failure or accidental deletion

Answer: D) Protection against data loss due to malware, hardware failure or accidental deletion

Q43. Which of the following describes Social Engineering in cyber security?

- A) A type of antivirus
- B) A type of firewall
- C) Manipulating people into revealing confidential information
- D) Designing social media websites

Answer: C) Manipulating people into revealing confidential information

Q44. Which of the following is a good practice for securing home Wi-Fi routers?

- A) Changing the default admin password and using strong Wi-Fi encryption
- B) Sharing the Wi-Fi password publicly
- C) Keeping the default password 'admin'
- D) Disabling all security features

Answer: A) Changing the default admin password and using strong Wi-Fi encryption

Q45. Which of the following file type is commonly used to spread viruses via email attachments?

- A) JPEG images only
- B) Executable/macro-enabled documents
- C) Plain text files only
- D) None, files cannot carry viruses

Answer: B) Executable/macro-enabled documents

Q46. Which of the following practice helps prevent unauthorized access if your device is left unattended?

- A) Enabling auto screen lock with a password/PIN
- B) Sharing your PIN with colleagues
- C) Disabling password protection
- D) Leaving the device unlocked

Answer: A) Enabling auto screen lock with a password/PIN

Q47. Which of the following describes 'Encryption'?

- A) Compressing files
- B) Deleting data permanently
- C) Printing files
- D) Converting data into a coded form to prevent unauthorized access

Answer: D) Converting data into a coded form to prevent unauthorized access

Q48. Which of the following should you check on a website before entering payment details?

- A) The website has many advertisements
- B) The website uses HTTPS (secure padlock symbol)
- C) The website loads quickly
- D) The website has a colorful design

Answer: B) The website uses HTTPS (secure padlock symbol)

Q49. Which of the following is a risk of clicking on pop-up advertisements from unknown sources?

- A) It has no risk at all
- B) It always gives free prizes
- C) It improves computer speed
- D) It may lead to malware infection or phishing sites

Answer: D) It may lead to malware infection or phishing sites

Q50. Which of the following is the safest way to dispose of an old computer/mobile with personal data?

- A) Securely wiping/formatting the data before disposal
- B) Giving it away without deleting any data
- C) Selling it with all personal data intact
- D) Throwing it away without any precaution

Answer: A) Securely wiping/formatting the data before disposal

Q51. Which of the following is a common cyber threat where attackers overload a server to make it unavailable, related to DOS/DDOS?

- A) Antivirus Scan
- B) Firewall Setup
- C) Denial of Service (DoS) Attack
- D) Software Update

Answer: C) Denial of Service (DoS) Attack

Q52. Which of the following is the correct action if your email account shows suspicious login activity?

- A) Share your password with support over email
- B) Change your password immediately and enable 2FA
- C) Ignore the alert
- D) Delete your account without changing password

Answer: B) Change your password immediately and enable 2FA

Q53. Which of the following is generally the safest source to download software/apps from?

- A) Unknown third-party websites
- B) Email attachments from strangers
- C) Official websites/app stores
- D) Pirated software links

Answer: C) Official websites/app stores

Q54. Which of the following term describes tricking a person through a fraudulent phone call to reveal confidential information?

- A) Encryption
- B) Antivirus
- C) Firewall
- D) Vishing (Voice Phishing)

Answer: D) Vishing (Voice Phishing)

Q55. Which of the following term describes phishing carried out via SMS text messages?

- A) Vishing
- B) Firewall
- C) Malware
- D) Smishing

Answer: D) Smishing

Q56. Which of the following is a recommended step to secure a smartphone against theft?

- A) Disabling screen lock
- B) Sharing your device PIN publicly
- C) Avoiding any security app
- D) Enabling remote lock/wipe features

Answer: D) Enabling remote lock/wipe features

Q57. Which of the following is TRUE about software updates and security patches?

- A) They always harm the device
- B) They often fix known security vulnerabilities and should be installed promptly

- C) They should always be avoided
- D) They have no relation to security

Answer: B) They often fix known security vulnerabilities and should be installed promptly

Q58. Which of the following describes a firewall's main purpose?

- A) Creating presentations
- B) Monitoring and controlling incoming/outgoing network traffic based on security rules
- C) Formatting the hard disk
- D) Increasing printer speed

Answer: B) Monitoring and controlling incoming/outgoing network traffic based on security rules

Q59. Which of the following describes 'Access Control' in cyber security?

- A) Deleting all user accounts
- B) Restricting access to systems/data to only authorized users based on defined permissions
- C) Allowing unrestricted access to everyone
- D) Sharing admin passwords publicly

Answer: B) Restricting access to systems/data to only authorized users based on defined permissions

Q60. Which of the following organization in India handles cyber security incidents and issues advisories?

- A) DigiLocker
- B) UMANG
- C) CERT-In (Indian Computer Emergency Response Team)
- D) IRCTC

Answer: C) CERT-In (Indian Computer Emergency Response Team)

Q61. Which of the following describes the goal of studying 'basic concepts of threats, vulnerabilities, controls' together in Cyber Security?

- A) Understanding only how to disable antivirus software
- B) Understanding only how to build new malware
- C) Understanding how potential dangers (threats) exploit weaknesses (vulnerabilities) and how safeguards (controls) mitigate risk
- D) Understanding only how to bypass all security measures

Answer: C) Understanding how potential dangers (threats) exploit weaknesses

(vulnerabilities) and how safeguards (controls) mitigate risk

Q62. Which of the following best describes a 'Control' in the context of basic cyber security concepts (threats, vulnerabilities, controls)?

- A) A type of cyber attack
- B) A weakness that increases risk
- C) A safeguard or countermeasure implemented to reduce risk from a threat or vulnerability
- D) A type of malicious software

Answer: C) A safeguard or countermeasure implemented to reduce risk from a threat or vulnerability

Q63. Which of the following describes the purpose of studying 'security policies' as a foundational cyber security topic?

- A) Understanding only how to disable firewalls
- B) Understanding the documented rules that guide how an organization protects its information assets
- C) Understanding only how to create malware
- D) Understanding only how to bypass organizational rules

Answer: B) Understanding the documented rules that guide how an organization protects its information assets

Q64. Which of the following describes the purpose of studying 'security mechanisms' as a foundational cyber security topic?

- A) Understanding the technical and procedural measures used to enforce security policies and protect systems
- B) Understanding only how to disable antivirus software
- C) Understanding only how to attack systems
- D) Understanding only how to create phishing emails

Answer: A) Understanding the technical and procedural measures used to enforce security policies and protect systems

Q65. Which of the following describes 'creating strong passwords' as a data security and protection practice?

- A) Using simple, easily guessable passwords for convenience
- B) Reusing the same password across all accounts without variation
- C) Sharing passwords openly with colleagues

D) Using complex passwords with a mix of characters to reduce the risk of unauthorized access

Answer: D) Using complex passwords with a mix of characters to reduce the risk of unauthorized access

Q66. Which of the following describes 'how to stay safe when surfing on internet' using In Private Browsing?

- A) Browsing without saving history, cookies or form data locally on that device
- B) Browsing with all security features disabled
- C) Browsing only on unsecured public Wi-Fi with no precautions
- D) Browsing while sharing your screen publicly at all times

Answer: A) Browsing without saving history, cookies or form data locally on that device

Q67. Which of the following describes 'identifying a secure website' as a core cyber security skill covered in this module?

- A) Only trusting websites recommended by strangers online
- B) Only trusting websites with colorful designs
- C) Trusting any website regardless of its address bar indicators
- D) Recognizing indicators like HTTPS and a padlock symbol before entering sensitive information

Answer: D) Recognizing indicators like HTTPS and a padlock symbol before entering sensitive information

Q68. Which of the following describes 'clear cookies' as a safe browsing practice covered in this module?

- A) Removing stored tracking data that websites use to remember browsing activity/preferences
- B) Deleting the entire operating system
- C) Disconnecting from the internet permanently
- D) Uninstalling the web browser permanently

Answer: A) Removing stored tracking data that websites use to remember browsing activity/preferences

Q69. Which of the following describes 'understand the term malware' as a foundational topic in Security Considerations?

- A) Understanding only legitimate firewall hardware

B) Understanding only legitimate antivirus software

C) Building awareness of malicious software categories like viruses, worms, Trojan horses, and spyware

D) Understanding only legitimate operating system updates

Answer: C) Building awareness of malicious software categories like viruses, worms, Trojan horses, and spyware

Q70. Which of the following describes 'Be aware of the possibility of receiving fraudulent and unsolicited e-mail' as a key awareness point?

- A) Assuming email cannot be used for fraud
- B) Assuming every email received is completely safe and legitimate
- C) Recognizing that not all emails received are legitimate, and some may be scams or unwanted spam
- D) Assuming only phone calls can be used for fraud, never email

Answer: C) Recognizing that not all emails received are legitimate, and some may be scams or unwanted spam

Q71. Which of the following describes 'Recognize attempted phishing' as a practical skill covered in this module?

- A) Clicking on every link to determine if it is a phishing attempt
- B) Replying to suspicious emails with personal information to test them
- C) Identifying common warning signs of phishing attempts, such as urgent requests for personal information
- D) Ignoring all incoming emails entirely without evaluation

Answer: C) Identifying common warning signs of phishing attempts, such as urgent requests for personal information

Q72. Which of the following describes 'Basics of Software Licensing' as covered in the Cyber Security module?

- A) Understanding only hardware specifications
- B) Understanding legal terms governing the use, distribution, and modification rights of software
- C) Understanding only internet connectivity options
- D) Understanding only how to pirate software illegally

Answer: B) Understanding legal terms governing the use, distribution, and modification rights of software

Q73. Which of the following describes 'Overview and understanding of IT Act 2000' as covered in this module?

- A) Understanding only physical security laws unrelated to IT
- B) Gaining foundational knowledge of India's primary law governing electronic transactions and cyber crimes
- C) Understanding only foreign cyber laws with no relevance to India
- D) Understanding only laws unrelated to technology entirely

Answer: B) Gaining foundational knowledge of India's primary law governing electronic transactions and cyber crimes

Q74. Which of the following describes 'DOS' as covered under Security Considerations in this module?

- A) A type of antivirus software
- B) A legitimate operating system feature
- C) A Denial of Service attack that disrupts normal access to a system or network
- D) A type of encryption technique

Answer: C) A Denial of Service attack that disrupts normal access to a system or network

Q75. Which of the following describes 'DDOS' as covered under Security Considerations in this module?

- A) A legitimate load-testing tool with no malicious intent implied here
- B) A Distributed Denial of Service attack launched from multiple sources simultaneously
- C) A type of antivirus feature
- D) A single-source, low-impact network request

Answer: B) A Distributed Denial of Service attack launched from multiple sources simultaneously

Q76. Which of the following describes 'Netiquettes' as covered under this Cyber Security module?

- A) A type of network hardware
- B) Guidelines for respectful and appropriate behavior while communicating online
- C) A type of malware
- D) A type of antivirus feature

Answer: B) Guidelines for respectful and appropriate behavior while communicating online

Q77. Which of the following describes 'Know about security threats from web sites' as covered in this module?

- A) Assuming security threats can only originate from emails, never websites
- B) Assuming security threats can only originate from USB drives, never websites
- C) Recognizing that websites can be sources of threats like viruses, worms, Trojan horses, and spyware
- D) Assuming all websites are completely safe by default

Answer: C) Recognizing that websites can be sources of threats like viruses, worms, Trojan horses, and spyware

Q78. Which of the following best explains why 'confidentiality, integrity, availability' are together called foundational security goals?

- A) They are unrelated concepts with no connection to security
- B) They collectively represent the core objectives that security controls aim to protect within any system
- C) They only apply to physical security, not digital systems
- D) They are outdated concepts no longer used in modern cyber security

Answer: B) They collectively represent the core objectives that security controls aim to protect within any system

Q79. Which of the following describes 'risk' more specifically as it relates to combined threats and vulnerabilities?

- A) A risk-free scenario where no threats or vulnerabilities exist
- B) A term unrelated to threats or vulnerabilities
- C) A term used only in financial contexts, not cyber security
- D) The likelihood and potential impact of a threat successfully exploiting a vulnerability

Answer: D) The likelihood and potential impact of a threat successfully exploiting a vulnerability

Q80. Which of the following best summarizes the overall objective of the Cyber Security module as stated in the syllabus?

- A) To teach only spreadsheet formulas
- B) To teach only word processing skills
- C) To help students know about security features and vulnerabilities and secure their network from attacks
- D) To teach only presentation design

Answer: C) To help students know about security features and vulnerabilities and secure their network from attacks

Q81. Which of the following describes 'Understand the term malware' as covered specifically under Security Considerations?

- A) Assuming malware refers only to a single specific virus type
- B) Assuming malware cannot be defined or categorized at all
- C) Building foundational awareness that malware is a broad category including viruses, worms, Trojans, and spyware
- D) Assuming malware only affects hardware, never software

Answer: C) Building foundational awareness that malware is a broad category including viruses, worms, Trojans, and spyware

Q82. Which of the following best explains the connection between 'DOS/DDOS' and general 'Security Considerations' in this module?

- A) DOS/DDOS attacks have no practical relevance to this module's objectives
- B) These attacks represent a real-world threat category that security awareness should address alongside other risks like viruses and phishing
- C) DOS/DDOS attacks only affect government systems, never individuals or businesses
- D) DOS/DDOS attacks are unrelated to general cyber security awareness

Answer: B) These attacks represent a real-world threat category that security awareness should address alongside other risks like viruses and phishing

Q83. Which of the following best explains why 'Netiquettes' is grouped with core Security Considerations in this module?

- A) Netiquettes are unrelated to any security consideration
- B) Netiquettes only apply to formal business emails, never general online interaction

- C) Following proper online etiquette helps reduce risks like miscommunication, harassment, and exposure to scams
- D) Netiquettes have no connection to safe online behavior

Answer: C) Following proper online etiquette helps reduce risks like miscommunication, harassment, and exposure to scams

Q84. Which of the following best explains the purpose of grouping 'phishing awareness' with 'fraudulent and unsolicited e-mail' in this module?

- A) Only phishing matters for security; unsolicited email poses no risk
- B) Phishing and fraudulent email are entirely unrelated security topics
- C) Both relate to recognizing and protecting against deceptive attempts to steal personal or financial information via email
- D) Only unsolicited email matters for security; phishing poses no risk

Answer: C) Both relate to recognizing and protecting against deceptive attempts to steal personal or financial information via email

Q85. Which of the following describes the purpose of an 'Acceptable Use Policy (AUP)' within an organization's security policies?

- A) Defining rules for how employees may appropriately use company IT resources and systems
- B) A policy that eliminates the need for any other security measures
- C) A policy that has no relation to cyber security governance
- D) A policy that only applies to physical office equipment, never IT systems

Answer: A) Defining rules for how employees may appropriately use company IT resources and systems

Q86. Which of the following describes the general purpose of 'Security Awareness Training' for employees within an organization?

- A) Educating staff on recognizing and responding to common cyber threats like phishing and social engineering
- B) A one-time activity with no ongoing relevance to security
- C) Training that has no impact on an organization's overall security posture

D) Training relevant only to IT department staff, never general employees

Answer: A) Educating staff on recognizing and responding to common cyber threats like phishing and social engineering

Q87. Which of the following describes why 'Software Licensing' knowledge matters for organizations using computer software?

- A) Ensuring compliance with legal usage terms and avoiding risks associated with unlicensed/pirated software
- B) Software licensing has no legal or practical significance for organizations
- C) Licensing knowledge is only relevant to software developers, never end users
- D) Only individual users need to be aware of licensing, never organizations

Answer: A) Ensuring compliance with legal usage terms and avoiding risks associated with unlicensed/pirated software

Q88. Which of the following best describes the general purpose of the IT Act 2000 in relation to electronic commerce and digital transactions?

- A) A law that only applies to government transactions, never private business
- B) A law entirely unrelated to electronic commerce or digital transactions
- C) Providing a legal framework recognizing electronic records, digital signatures, and addressing cyber offences in India
- D) A law that has been fully repealed with no current relevance

Answer: C) Providing a legal framework recognizing electronic records, digital signatures, and addressing cyber offences in India

Q89. Which of the following describes the general concept of 'Data Protection' as it relates to organizational responsibility for customer information?

- A) Data protection measures are optional and have no legal basis
- B) Organizations have no responsibility to protect any data they collect
- C) Implementing appropriate measures to safeguard personal/sensitive data collected from customers or users
- D) Data protection only applies to government-held information, never private company data

Answer: C) Implementing appropriate measures to safeguard personal/sensitive data collected from customers or users

Q90. Which of the following describes a general best practice for handling sensitive company information via personal devices (BYOD)?

- A) Sensitive company data should never be considered at risk on personal devices
- B) Applying appropriate security controls, like encryption and remote wipe capability, on personal devices used for work
- C) Personal devices require no special security considerations for work use
- D) BYOD (Bring Your Own Device) practices eliminate all security risk automatically

Answer: B) Applying appropriate security controls, like encryption and remote wipe capability, on personal devices used for work

Q91. Which of the following best describes the general concept of 'Least Privilege' applied within an organizational security policy?

- A) Access rights should be assigned randomly with no relation to job function
- B) Granting employees only the access rights necessary to perform their specific job functions
- C) Denying all employees any access to organizational systems
- D) Granting every employee full administrative access by default

Answer: B) Granting employees only the access rights necessary to perform their specific job functions

Q92. Which of the following describes the purpose of periodic 'Security Audits' within an organization's broader security mechanisms?

- A) Security audits should only ever be conducted once, with no ongoing schedule
- B) Audits are relevant only to financial matters, never cyber security
- C) Security audits have no practical value for identifying vulnerabilities
- D) Systematically reviewing systems and practices to identify vulnerabilities and ensure compliance with security policies

Answer: D) Systematically reviewing systems and practices to identify vulnerabilities and ensure compliance with security policies

Q93. Which of the following best describes why understanding both 'threats' and their

corresponding 'controls' together is emphasized in this module?

- A) Threats and controls are entirely unrelated topics with no practical connection
- B) Only understanding controls is useful; threats have no practical relevance
- C) Effective security requires understanding potential dangers alongside the specific measures used to mitigate them
- D) Only understanding threats is useful; controls have no practical relevance

Answer: C) Effective security requires understanding potential dangers alongside the specific measures used to mitigate them

Q94. Which of the following best describes the overarching theme connecting 'Data Security and protection', 'safe internet surfing', and 'Security Considerations' within this Cyber Security module?

- A) This grouping serves no coherent educational purpose in the module
- B) These topics are entirely unrelated with no common thread
- C) They collectively build practical skills and awareness for protecting personal and organizational data and systems from common digital threats
- D) Only 'Data Security and protection' is relevant; the other topics are unrelated

Answer: C) They collectively build practical skills and awareness for protecting personal and organizational data and systems from common digital threats

Q95. Which of the following describes the practical value of learning to 'identify a secure web site' before making an online purchase or sharing personal data?

- A) It helps users avoid potentially fraudulent or insecure websites that could compromise their information
- B) All websites are equally safe regardless of any visible security indicators
- C) Identifying a secure website is only relevant for IT professionals, never general users
- D) This skill has no practical value for everyday internet users

Answer: A) It helps users avoid potentially fraudulent or insecure websites that could compromise their information

Q96. Which of the following describes the practical value of understanding phishing recognition skills within a broader digital literacy context?

- A) It helps protect individuals from financial loss and identity theft resulting from deceptive email/message scams
- B) Understanding phishing is only relevant to cyber security professionals
- C) Phishing awareness has no practical value for typical computer users
- D) Phishing only targets large organizations, never individual computer users

Answer: A) It helps protect individuals from financial loss and identity theft resulting from deceptive email/message scams

Q97. Which of the following describes the practical relevance of learning about 'DOS' and 'DDOS' attacks for a general computer user, even if they don't manage servers themselves?

- A) Only server administrators ever need any awareness of DOS/DDOS attacks
- B) This knowledge has zero practical relevance for anyone outside IT administration
- C) Building general awareness of common cyber attack types supports informed digital citizenship and better understanding of news/security discussions
- D) DOS/DDOS attacks are entirely fictional concepts with no real-world basis

Answer: C) Building general awareness of common cyber attack types supports informed digital citizenship and better understanding of news/security discussions

Q98. Which of the following describes the practical value of understanding basic software licensing concepts for an everyday computer user installing new applications?

- A) Understanding licensing has no bearing on the security of installed software
- B) All software, licensed or not, poses identical risk regardless of licensing status
- C) Helps users avoid legal risks and potential security dangers associated with using unlicensed/pirated software
- D) Licensing knowledge is only relevant to software companies, never end users installing software

Answer: C) Helps users avoid legal risks and potential security dangers associated with using unlicensed/pirated software

Q99. Which of the following best summarizes the overall value of completing the Cyber Security module within the broader ECC course?

- A) Cyber security awareness is only relevant to specialized IT security professionals, not general learners
- B) Building foundational digital safety awareness that complements technical computer skills learned throughout the course
- C) This module provides no practical value beyond the immediate exam
- D) Cyber security knowledge is entirely disconnected from the other technical skills taught in ECC

Answer: B) Building foundational digital safety awareness that complements technical computer skills learned throughout the course

Q100. Which of the following describes the general purpose of understanding 'controls' as a mitigation concept, using an antivirus program as a practical example?

- A) Antivirus programs have no relationship to the broader concept of security controls
- B) Controls are a purely theoretical concept with no real-world technical examples
- C) Antivirus software is best classified as a vulnerability rather than a control
- D) An antivirus program serves as a technical control that helps detect and prevent malware threats from causing harm

Answer: D) An antivirus program serves as a technical control that helps detect and prevent malware threats from causing harm