2025/2026 Cybersecurity Awareness Training Assessment of Knowledge (Test)

Employee Name (Printed): _____ Date: _____

Employer: _____ Department: _____

Original Test Score: _____ Corrected Test Score: _____

Please complete each question by picking the correct answer (circle one letter):

1. Examples of Personally Identifiable Information are:
    A. Full name (if not common)
    B. Birthplace
    C. Social Security Number
    D. Vehicle Plate Number
    E. All of the above

2. What is AI, as explained in the training?
    A. Autonomous Internet
    B. Artificial Intelligence
    C. Automatic Infiltration
    D. Application Interface

3. What is MFA?
    A. Multi-Faceted Account
    B. Multi-Factor Authentication
    C. May Face Authorization

4. Which of the following is a tactic used by a cyber criminal?
    A. Spear Phishing
    B. Phishing
    C. Vishing
    D. Quishing
    E. All of the above

5. What is the highest level of data that should be protected?
    A. Public
    B. Private
    C. Sensitive

6. Which of the following is an example of a best practice for working remotely?
   A. Use public WiFI whenever possible
   B. Always use your work device to access personal accounts
   C. Use a VPN whenever possible

7. Which of the following is an example of a motivation of a threat actor?
   A. Financial gain
   B. Damage the victim either financially or reputationally
   C. Gather data to trade or sell
   D. All of the above

8. If you click on an unknown link or attachment in a suspicious email and then wonder what you just clicked, what action should you take?
   A. Watch the screen for at least 5 minutes to make sure nothing out of the ordinary occurs
   B. Contact your IT department or person who is responsible for computer operations
   C. Restart your computer to make sure it has not been infected
   D. Continue with your normal activities and let the organization's firewall or virus scan address the threat

9. What is ransomware?
   A. Software that protects your computer from viruses
   B. Malware that locks users out of their devices or blocks access to files until a sum of money is paid
   C. Cryptocurrency, like BitCoin

10. If you receive an email or a phone call from an unknown individual asking about your invoice payment process, you should:
    A. Provide full and complete answers to all questions
    B. Write down all of the questions and respond via email
    C. Answer only the questions that you are sure of the answer
    D. Do not answer questions, get the caller's information, and contact your IT or Purchasing Department

Cybersecurity Awareness Training Assessment (Answer Key)

1. E, all of the above are examples of Personally Identifiable Information (PII)

2. B, AI stands for Artificial Intelligence

3. B, MFA is Multi-Factor Authentication

4. E, all of the above are tactics used by cyber criminals

5. C, sensitive data is the highest level of data

6. C, using a VPN whenever possible is a best practice for working remotely

7. D, all of the above are examples of motivations of threat actors

8. B, you should contact your IT department if you click on an unknown link or open an attachment from a suspicious email

9. B, ransomware is a form of malware that locks users from their devices or blocks access to files until a sum of money is paid

10. D, you should not answer questions, get the caller's information, and contact your IT or purchasing department if you receive a request for information about your invoice payment process