Cybersecurity Awareness Training Assessment of Knowledge (Test)

Employee Name (Printed): LETICIA RODRIGUEZ Date: JULY 24, 2023

Employer: CITY OF JACINTO CITY Department: WATER BILLING

Original Test Score: _____ Corrected Test Score: _____

Please complete each question (10 questions) and pick the correct answer. (Circle one letter).

1. Which of the following are personal identifiable information?
   A. Your IP address (an example is the number assigned to your computer)
   B. Your birthplace
   C. Driver's license number
   D. All of the above

2. If you are suspicious of an email, what should you do?
   A. Do not click on the links provided in the email.
   B. Do not open any attachments in the email.
   C. Do not provide personal information or data.
   D. Forward the email to your IT department
   E. All of the above

3. If you receive a phone call or email from an unknown individual asking about your invoice payment process, you should:
   A. Provide full and complete answers to all questions
   B. Take all questions down and send answers via email
   C. Answer only questions for which you know the answer for sure
   D. Do not answer questions, but take the caller's contact info, and consult your IT department and purchasing department

4. Which is a good password practice?
   A. Avoid single words found in a dictionary or proper nouns.
   B. Do not keep copies of passwords where others can see them, preferably not on paper anywhere, or in any clear-text electronic format.
   C. Do not share your passwords to anyone else.
   D. Do not use the same passwords, or close variation, on multiple systems, including personal ones.
   E. All of the above are good practices

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

6. What is the meaning of “threat” with regards information security?

A. The use of strong language to get wanted reaction
B. The potential targeting of a network or system in an attempt to damage, harm or disrupt its capability to operate.
C. Continual texting and communicating through social media
D. None of the above

7. Which is **not** a good security practice?

A. Use Multi-Factor Authentication for your accounts
B. Use one complex password for all your accounts
C. Use face recognition and/or password for your smartphone
D. Verify the email sender’s domain of a suspicious email and if you need to call, find another source for the phone number outside of the email.

8. Which of the following are types of tactics used in a cybersecurity attack?

A. Phishing
B. Malware
C. Ransomware
D. All of the above

9. What type of tactic used in a cybersecurity attack would be best described as “an email targeted at a specific individual or department within an organization that appears to be from a trusted source”?

A. Robocalling
B. Ghosting
C. Catfishing
D. Spear Phishing

10. If you click on an unknown link or attachment in a suspicious email and then wonder “what you just clicked”, what if any actions should you take?

A. Watch the screen for at least five minutes to make sure nothing out of the ordinary occurs
B. Restart your computer to make sure it has not been infected
C. Contact your IT department or person in your organization who is responsible for computer operations
D. Continue with your normal activities and let the organization’s firewall or virus scan address the threat