J5.6.1 Phishing Awareness Quiz

Amanda Success (Period 9) (replace with your information)
Monday December 25, 2023
Seat 99 (Grade level 13)
Cyber Capstone

1. What is phishing?
A. A cyber defense tactic
B. A cybercrime tactic used to deceive individuals
C. A software used to protect against malware
D. A type of encryption algorithm
___ <- Type answer here

2. How do phishing emails typically create urgency?
A. By offering rewards or prizes
B. By threatening consequences or demanding immediate action
C. By providing helpful information
D. By requesting feedback
___ <- Type answer here

3. What should you do if you receive a suspicious email?
A. Click on the links to verify their legitimacy
B. Download any attachments to inspect them
C. Reply to the sender requesting more information
D. Forward the email to your organization's IT or security team
___ <- Type answer here

4. How can you verify the legitimacy of a URL in a suspicious email?
A. Hover over it to reveal the actual URL
B. Click on it and see where it leads
C. Check the sender's email address
D. Ignore it and proceed with caution
___ <- Type answer here

5. What is a common characteristic of phishing emails regarding grammar and language?

A. They are written in professional language
B. They contain no grammatical errors
C. They often contain grammatical errors or awkward language
D. They are written in multiple languages
___ <- Type answer here

6. What action should you take if you've inadvertently provided sensitive information in response to a phishing email?
A. Ignore it and hope for the best
B. Report it to the relevant authorities
C. Delete the email immediately
D. Change your email address
___ <- Type answer here

7. Which of the following is a recommended step to prevent falling victim to phishing scams?
A. Share sensitive information via email
B. Keep antivirus and anti-malware software outdated
C. Click on links in suspicious emails to verify legitimacy
D. Educate yourself and others about phishing tactics
___ <- Type answer here

8. What should you do if you believe you've been targeted by a phishing attempt?
A. Report it to the appropriate authorities
B. Delete the email without further action
C. Reply to the sender requesting more information
D. Click on any links provided to investigate
___ <- Type answer here

9. Why should you be cautious of unexpected email attachments?
A. They often contain useful information
B. They may contain malware
C. They are typically sent by trusted sources
D. They are necessary for verifying sender authenticity
___ <- Type answer here

10. What is a key recommendation for recognizing phishing emails?
A. Trust all emails from familiar senders
B. Ignore misspellings or unusual domain names
C. Avoid verifying sender information
D. Share sensitive information readily
___ <- Type answer here