L2.2.4 - Misinformation and Impersonation Quiz

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

0. 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

1. What is the key difference between misinformation and disinformation in the context of cybersecurity?
A. Misinformation is unintentional, while disinformation is intentional.
B. Misinformation involves spreading false information with the intent to deceive, while disinformation involves spreading false information without the intent to deceive.
C. Misinformation is spread through email, while disinformation is spread through social media.
D. Misinformation is often exaggerated, while disinformation is factual.
___ <- Type answer here

2. Which of the following is an example of impersonation in cybersecurity attacks?
A. Sending fake invoices to trick employees into making payments to fraudulent accounts
B. Pretending to be a high-level executive and requesting financial transactions or sensitive information
C. Mimicking a legitimate brand's website to collect sensitive information from users
D. Spreading fake emails about malware threats to scare recipients
___ <- Type answer here

3. What is tailgating, also known as piggybacking, in the context of cybersecurity?
A. Creating fake invoices to trick employees or vendors
B. Spreading false narratives about cyber threats
C. Gaining entry to a restricted area without proper authentication by following an authorized person
D. Manipulating or creating fake emails that appear to be from a legitimate brand
___ <- Type answer here

4. What is a common tactic used in impersonation attacks?
A. Sending emails with exaggerated threats
B. Creating fake social media profiles
C. Demanding immediate action or access by making it appear to be an emergency

D. Using technical jargon to confuse the target
___ <- Type answer here

5. What is the primary goal of business email compromise (BEC. attacks?
A. Spreading false information to manipulate public perception
B. Gaining unauthorized access to business email accounts for financial gain
C. Mimicking legitimate brands to trick individuals into divulging sensitive information
D. Creating fake emails about malware threats to deceive recipients
___ <- Type answer here

6. How can organizations mitigate the risk of tailgating attacks?
A. Establishing clear verification processes for access to restricted areas
B. Implementing strong email security measures
C. Encouraging employees to forward suspicious emails to IT support
D. Conducting employee training on recognizing phishing attempts
___ <- Type answer here

7. What is the goal of brand impersonation attacks in cybersecurity?
A. To create humorous hoaxes that waste time and effort
B. To spread false narratives about cybersecurity threats
C. To trick individuals into divulging sensitive information or distributing malware
D. To manipulate individuals into forwarding fake emails to friends and family
___ <- Type answer here

8. What is the best defense against impersonation attacks?
A. Providing personal information to unknown individuals
B. Ignoring verification processes to speed up operations
C. Volunteer information freely to appear cooperative
D. Checking credentials, calling for proof, and verifying the identity of individuals
___ <- Type answer here