Review Test Submission: Week Two Midterm

User	Robert Alan Howell
Course	ITM470 Information Security Management
Test	Week Two Midterm
Started	9/12/21 9:25 AM
Submitted	9/12/21 11:07 AM
Due Date	9/12/21 11:59 PM
Status	Needs Grading
Attempt Score	Grade not available.
Time Elapsed	1 hour, 41 minutes out of 2 hours and 30 minutes
Instructions	Please answer each question below and click **Submit** when you have completed the Quiz.
Results Displayed	All Answers, Submitted Answers, Correct Answers, Feedback, Incorrectly Answered Questions

Question 1

Needs Grading

Define social engineering. Provide a detailed example of how an attacker might execute a social engineering attack? What kinds of things could an organization do to protect themselves from your attack?

Selected Answer:

Social engineering is a means of breaking security which can be inadvertant or intentonal. Social engineering methods can reveal passwords and confidential information which is intended only for an organizaion or employee. Differing methods of social engineering occur including phishing, pretexting and advance-fee frauds which each can reveal personally identifyable information (PII) such as name, date of birth, and social security numbers. Phishing involves the attempt of acquiring PII through emails designed to look authentic but actually are a way to get a user to reveal usernames and passwords through different methods like malicious links and websites. Pretexting is pretending to be an authority figure in an organization. By contacting members of the organization, the employees believe the authority figure is real and will do as they say. An example may be the (fake) authority figure suggests to employees to fill out contact information on a (also fake) website with names and addresses of yourself and/or emergency contact information of family or relatives. Advance-fee frauds involve scheming a person into paying additional fees or balances that are deemed to be true but actually are not.

Organizations have many methods to protect from social engineering. Reporting and deleting suspicious emails is one of these major preventative tactics. After a bad email is reported, the company can put out communications to IT departments and other departments of the malicious intent of the email and will suggest to everyone to delete the email or block the sender. Social engineering can be prevented further by employee training, due care and due diligence measures, and physical protections such as screen filters and departmentalization, which prevent unwanted shoulder surfers and separate