CONCORDIA COLLEGE
MOORHEAD, MINNESOTA

- Name: _____
- Date: _____
- Section: _____

BUSN 315: Management Information Systems

Problem Set #4: Suggested Solutions

Spring 2026

Problem 1. Definitions

DEFINITION QUESTIONS REPLACED

WITH 4 EXTRA T/F QUESTIONS IN QUIZ #4

Problem 2. True / False

Determine whether each statement is `TRUE` or `FALSE`. If `FALSE`, justify your answer briefly.

2.A. HTTPS encrypts data and is required for secure web transactions.

- `TRUE`

2.B. VoIP allows voice communication to travel over the same infrastructure as Internet data.

- `TRUE`

2.C. Phishing attacks exploit technical vulnerabilities in software rather than human behavior.

- `FALSE`
- Phishing attacks primarily exploit human behavior, not technical vulnerabilities.

2.D. Denial-of-service (DoS) attacks attempt to gain unauthorized access to data by stealing credentials.

- `FALSE`
- DoS attacks aim to disrupt system availability by overwhelming systems with traffic.

Problem 3. Multiple Choice

Select the BEST answer for each question.

3.A. Which of the following best describes a digital network?

a) A centralized database used for storing business records

b) A collection of connected devices that can communicate and exchange data

c) A system used only for Internet browsing

d) A set of software tools for web design

3.B. Which of the following best describes the role of a router?

a) It connects different networks together

b) It manages user permissions on a network

c) It stores files for multiple clients

d) It creates web pages using HTML

3.C. Which of the following best describes Voice over Internet Protocol (VoIP)?

a) A system that uses separate phone networks for local calls

b) A protocol that creates websites for businesses

c) A technology that converts voice signals into digital packets that travel across IP networks

d) A tool used to optimize search rankings

3.D. A firm adopts a cloud-based platform that combines voice, video, messaging, and email in one place. This is best described as:

a) Unified Communications as a Service (UCaaS)

b) Search Engine Marketing (SEM)

c) A Network Interface Controller (NIC)

d) A transmission medium

Problem 3. Multiple Choice (continued)

3.E. Which of the following best distinguishes SEO from SEM?

a) SEO uses paid ads, while SEM improves organic visibility
b) SEO improves organic visibility, while SEM uses paid search ads
c) SEO is used for email communication, while SEM is used for websites
d) SEO and SEM are identical concepts

3.F. Which of the following best describes a threat actor?

a) A system vulnerability
b) A type of firewall
c) An individual or group that exploits vulnerabilities
d) A security policy

3.G. Which of the following best describes ransomware?

a) Malware that monitors user behavior
b) Malware that spreads without user action
c) Malware that encrypts files and demands payment
d) Malware that improves system performance

3.H. Which of the following best describes phishing?

a) Malware that spreads through networks
b) Fraudulent communication designed to trick users into revealing information
c) A method of encrypting data
d) A tool for monitoring systems

Problem 3. Multiple Choice (continued)

3.I. An employee receives an email that appears to be from a trusted vendor requesting login credentials. This is an example of:

a) Malware
b) Encryption
c) Patch management
d) Phishing

3.J. A company's website becomes unavailable after being flooded with excessive traffic from multiple sources. This is an example of:

a) Phishing
b) DoS attack
c) Data redundancy
d) Encryption

3.K. Which of the following best describes multifactor authentication (MFA)?

a) Using a single password
b) Combining multiple forms of verification
c) Encrypting data during transmission
d) Blocking network traffic

3.L. Which of the following best describes digital forensics?

a) Preventing cyberattacks
b) Investigating and analyzing digital evidence after an incident
c) Encrypting sensitive data
d) Managing network traffic

Problem 4. Short Answers #1

Two competing online retailers are trying to increase traffic to their websites.

- Firm A hires a team to improve its website content, structure, and keywords so that its pages appear higher in unpaid search results. This process takes time, but the firm expects long-term improvements in visibility.
- Firm B instead allocates a significant budget to pay for advertisements that appear at the top of search engine results pages. These ads generate immediate visibility, but only as long as the firm continues to pay for them.

Both firms are also considering redesigning their websites to improve user experience, although this has not yet been implemented.

4.A. Identify the two different approaches being used by Firm A and Firm B.

- Firm A: Search Engine Optimization (SEO)
- Firm B: Search Engine Marketing (SEM)

4.B. Explain one key difference between these two approaches in terms of how search engine visibility is achieved.

- Search Engine Optimization (SEO)
  - Improves visibility in unpaid (organic) search results
  - Achieved by optimizing website content, structure, and keywords
  - Typically produces long-term results
- Search Engine Marketing (SEM)
  - Involves paid advertisements that appear in search results
  - Provides immediate visibility
  - Visibility depends on continued payment

Problem 5. Short Answers #2

A mid-sized retail company suddenly loses access to its internal files, including inventory records and sales data. When employees attempt to open these files, they see a message stating that the data has been encrypted and will only be restored if a payment is made in cryptocurrency. In recent months, the company had invested heavily in upgrading its hardware systems and increasing network bandwidth to improve performance. Some managers initially suspect that the issue may be related to these recent upgrades.

5.A. What type of security threat is the company experiencing?

- Ransomware

5.B. Explain why this type of attack can be particularly damaging to business operations.

- Ransomware encrypts critical files, making them inaccessible
- Disrupts normal business operations (e.g., inventory, sales, records)
- May cause downtime and financial losses
- Can force firms to pay ransom to regain access
- Can lead to data loss or reputational damage