**Name: Gumisid, Reah Jane C. Date: October 3, 2025**

**Section: BSIT - 31027 ITSPC1**

**Analysis, Application, and Exploration for Week 13**

**IDENTIFICATION**

1. Malware that replicates to damage computer files.

**Computer Virus**

2. Attempt to steal personal data by masquerading as a trusted entity.

**Phishing**

3. Unauthorized access to data by exploiting systems.

**Hacker**

4. Program that tracks online activities without consent.

**Spyware**

5. Data being transferred across a network.

**Data in Motion**

6. Data that is stored and not currently in use.

**Data at Rest**

7. Antivirus feature that protects against unauthorized access.

**Identity Theft Protection**

8. Data actively being accessed or used by the system.

**Data in Use**

9. Data protection by monitoring network traffic.

**Firewall**

10. Software that detects and removes malicious programs.

**Antivirus Software**

**MULTIPLE CHOICE (EVALUATION)**

1. Phishing is most commonly conducted through:

a. Direct phone calls

b. Social media posts

c. Paper mail

d. Emails and instant messages

**Answer: d. Emails and instant messages**

2. What type of data is "data in motion"?

a. Data that resides in memory but is not visible to the user

b. Data stored on physical media

c. Data that is actively being transferred across a network

d. Data that is stored on a computer system but not in use

**Answer: c. Data that is actively being transferred across a network**

3. Why is up-to-date antivirus software essential?

a. It allows unrestricted downloads

b. It protects against the latest security threats

c. It helps increase social media engagement

d. It reduces internet speed

**Answer: b. It protects against the latest security threats**

4. Which term describes an individual who breaks into computer systems for malicious purposes?

a. Cyberprotector

b. Hacker

c. Phisher

d. Data analyst

**Answer: b. Hacker**

5. What is the primary characteristic of a computer virus?

a. It protects data from unauthorized access

b. It is always visible to the user

c. It secures computer files

d. It modifies computer operation without user permission

**Answer: d. It modifies computer operation without user permission**

6. Which action can help reduce the risk of phishing?

a. Ignoring all emails from friends

b. Disabling all email alerts

c. Removing the browser's security settings

d. Using antivirus software with identity theft protection

**Answer: d. Using antivirus software with identity theft protection**

7. Which of the following is an example of "data in use"?

a. A closed document stored on a USB drive

b. A backup on an external hard drive

c. A web page being displayed in a browser

d. An image file stored on a DVD

**Answer: c. A web page being displayed in a browser**

8. What does spyware do?

a. It removes viruses from your computer

b. It monitors online activities without consent

c. It protects personal information

d. It enhances computer performance

**Answer: b. It monitors online activities without consent**

9. When data is loaded into memory for a program to run, it is considered:

a. Data in motion

b. Data at rest

c. Data off-site

d. Data in use

**Answer: d. Data in use**

10. A program that installs itself to monitor activities for profit is known as:

a. Spyware

b. Antivirus

c. Adware

d. Ransomware

**Answer: a. Spyware**

**TRUE OR FALSE**

1. Data at rest refers to data that is currently being transferred over a network.

**FALSE**

2. Spyware is a type of malware that monitors a user's online activities without their knowledge.

**TRUE**

3. Phishing attacks typically aim to steal sensitive information by impersonating a trusted entity.

**TRUE**

4. A firewall helps protect against computer viruses by scanning files for malicious code.

**FALSE**

5. Data in use is information that resides in memory and is actively being processed by a computer system.

**TRUE**