# Cyber Security and Privacy, IIT Madras
# Prof. Saji K Mathew

**Week 1 Quiz**
**(All questions carry 1 point each)**

1. A malicious email attack targeting a specific user or group of users, appearing to originate from a trusted source is:
   a. Spear Phishing
   b. Man in the Middle Attack
   c. Smurf Attack
   d. Social media phishing

**Ans: a. Spear Phishing**

**Explanation: Spear phishing attacks target specific users. It is similar to phishing, but attackers customize their approach for specific individuals or organizations.**

2. A malicious attack where hackers encrypt an organization's data and demand payment to restore access is known as:

   a. Spyware
   b. Ransomware
   c. Whaling
   d. Watering hole attack

**Ans: b. Ransomware**

**Explanation: Ransomware denies access to a computer system or data until a ransom is paid.**

3. Which of the following characteristics are most likely to be found in a phishing email?

   a. Sense of urgency and immediate action requests.
   b. Unusual or inappropriate requests
   c. Incorrect sender name or email address.
   d. All of the above.

**Ans: d. All of the above**

**Explanation: The above mentioned are some of the characteristics which make phishing emails more recognizable.**

4. From a managerial perspective, Information Security is generally understood as a:

   a. Product
   b. Technology
   c. Process
   d. Product, Technology and Process

**Ans: c. Process**

**Explanation: Information security, often referred to as InfoSec, refers to the processes and tools designed and deployed to protect sensitive business information from modification, disruption, destruction, and inspection.**

5. The practice of keeping an organization's network infrastructure secure from unauthorized access is known as:

a. Data Security
b. Network Security
c. Information Security
d. Operations Security

**Ans: b. Network Security**

**Explanation: Network security is the field of cybersecurity focused on protecting computer networks from cyber threats.**

6. Which of the following statements most accurately reflects the complex role of technology in cybersecurity?

a. Technology acts as both a source of threats and a tool for defense.
b. Technology is solely a source of threats and vulnerabilities.
c. Technology plays a triple role: source of threats, asset to protect, and defense weapon.
d. Technology solely serves as a defense weapon against cyberattacks.

**Ans: c. Technology plays a triple role: source of threats, asset to protect, and defense weapon**

**Explanation: In the realm of cybersecurity, it is essential to have a clear understanding of the specific meaning of the term "technology" when it is being utilized.**

**7.** _____ is a manipulation technique that exploits human weakness to gain private information, access, or valuables

a. Spyware
b. Logic Bomb
c. Social Engineering
d. Man in the Middle Attack

**Ans: c. Social Engineering**

**Explanation: Social engineering technique gathers information by exploiting the weakest part of security, people.**

8. True or False: The word "Cyber" in "Cybernetics" originates from the French language.

a. True
b. False

**Ans: False**

Explanation: Its of Greek origin derived from "κυβερνήτης" meaning steerman or pilot

9. The impact of a cyber security incident on organizations can include:

a. Financial Loss
b. Reputation Damage
c. Regulatory fine
d. All the above

**Ans: d. All the above**

**Explanation: A cyber incident can have short-term as well as long-term impacts on a business, such as financial loss, reputation damage, loss of competitive advantage, reduction in credit rating, and increase in cyber insurance premiums.**

10. True or False: A Vendor guarantees that their IoT solutions are 100% safe from cyberattacks. This statement can be

a. True
b. False

**Ans: b. False**

**Explanation: Even robust systems are not truly 100% secure. Regardless of vendor claims, any connected device or software faces potential vulnerabilities that could be exploited by attackers with enough time, resources, and skill.**