1. What is the term for falsifying email headers to make an email appear as if it came from a different source?
a) Email Encryption
b) Email Hijacking
c) Email Spoofing
d) Email Phishing

Answer: c) Email Spoofing
Explanation: Email Spoofing is the act of altering the email header information to make it appear as though the email originated from a different sender. This technique is commonly used in phishing attacks to deceive recipients into disclosing sensitive information.

2. Which of the following cybercrimes involves the mass distribution of unsolicited emails for commercial purposes?
a) Email Spoofing
b) Phishing
c) Spamming
d) Internet Time Theft

Answer: c) Spamming
Explanation: Spamming is the unauthorized sending of bulk unsolicited messages, often for advertising or phishing purposes. It inundates recipients' inboxes with unwanted emails, causing inconvenience and potential security risks.

3. What cybercrime involves an unauthorized use of internet hours paid for by another user?
a) Email Spoofing
b) Phishing

c) Internet Time Theft
d) Cyber Extortion

Answer: c) Internet Time Theft
Explanation: Internet Time Theft refers to the unauthorized use of internet hours that were paid for by someone else. It commonly occurs in environments where internet access is billed based on usage time.

4. Which cybercrime involves stealing small amounts of resources or money from numerous accounts to avoid detection?
a) Email Spoofing
b) Salami Attack
c) Phishing
d) Denial of Service (DoS) Attack

Answer: b) Salami Attack
Explanation: A Salami Attack, also known as Salami Technique, involves stealing small amounts of resources or money from numerous accounts. Perpetrators execute this in a manner that avoids detection by taking such small amounts from each account.

5. What term describes the deceptive attempt to obtain sensitive information, such as usernames, passwords, and credit card details, by masquerading as a trustworthy entity in an electronic communication?
a) Email Spoofing
b) Spamming
c) Phishing
d) Salami Attack

Answer: c) Phishing
Explanation: Phishing is the fraudulent practice of sending emails or messages claiming to be from reputable companies to induce individuals to reveal personal information, such as passwords and credit card numbers.

6. Which of the following is NOT a type of cybercrime mentioned?
a) Email Spoofing
b) Data Breach
c) Internet Time Gifting
d) Salami Attack

Answer: c) Internet Time Gifting
Explanation: While cybercrimes like Email Spoofing, Data Breach, and Salami Attack involve malicious activities, “Internet Time Gifting” isn’t a recognized form of cybercrime.

7. What is the primary motive behind Email Spoofing?
a) To gain unauthorized access to networks
b) To distribute malware
c) To falsify the sender’s identity
d) To steal personal information

Answer: c) To falsify the sender’s identity
Explanation: The primary motive behind Email Spoofing is to deceive recipients by falsifying the sender’s identity, often for the purpose of phishing or spreading malware.

8. Which cybercrime aims to disrupt the normal functioning of a network or website by overwhelming it with a flood of traffic?

a) Email Spoofing
b) Data Breach
c) Denial of Service (DoS) Attack
d) Salami Attack

Answer: c) Denial of Service (DoS) Attack
Explanation: A Denial of Service (DoS) Attack floods a system, server, or network with traffic to exhaust resources and bandwidth, thereby disrupting normal operations and denying access to legitimate users.

9. What is the main goal of a Salami Attack?
a) To directly steal large sums of money
b) To avoid detection by taking small amounts from multiple sources
c) To distribute malware to unsuspecting users
d) To gain unauthorized access to sensitive data

Answer: b) To avoid detection by taking small amounts from multiple sources
Explanation: The main goal of a Salami Attack is to avoid detection by stealing small amounts from numerous sources. This incremental theft reduces the likelihood of detection while accumulating illicit gains over time.

10. Which of the following cybercrimes involves obtaining unauthorized access to confidential information stored in a computer system?
a) Email Spoofing
b) Data Breach
c) Internet Time Theft
d) Phishing

Answer: b) Data Breach
Explanation: A Data Breach occurs when unauthorized individuals gain access to confidential information stored in computer systems, often resulting in the exposure of sensitive data such as personal or financial records.

Related posts:

1. Introduction to Information Security
2. Introduction to Information Security MCQ
3. Introduction to Information Security MCQ
4. Symmetric Key Cryptography MCQ
5. Asymmetric Key Cryptography MCQ
6. Authentication & Integrity MCQ
7. E-mail, IP and Web Security MCQ