

**Qtext:-**

In an organization, IT Help Desk received several complaints that the employees are receiving Viagra spam. Investigation revealed that one of the employee's computers was sending out those Viagra spam. They found that a program was installed (probably by a hacker) on the employee's computer that made it automatically send out tons of spam emails without the computer owner's knowledge. Identify five ways a hacker could get into the computer to set this up? [1 X 5 = 5]

**Qtext:-**

(a) Explain clearly with examples between threat, vulnerability, and risk

(b) Explain a scenario in which existence of a threat might not pose any risk to the organization. [6 + 2 = 8]

In olden days, wax sealant was used to seal documents (they are probably used even today). They help verify that documents were unopened. When sealed with a custom signet ring, the sealant could also be used to verify the sender's identity. Because these rings were difficult to replicate. Recipients of the documents could have reasonable certainty that the message was legitimate if they recognized the seal. What aspect of cybersecurity does this concept signifies? Explain this cybersecurity aspect using an example. What kind of assurance does this cybersecurity aspect provides. [1 + 3 + 3 = 7]

(a) Cybercrime can be categorized based on the role that the computer plays in the criminal activity. Name and explain those different categories.

(b) Consider the following cybercrimes and indicate in which category it falls

- a. Offences related to child pornography involving
  - i. Producing
  - ii. Offering or making child pornography available
  - iii. Distributing or transmitting child pornography
- b. Credit card fraud; gambling
- c. Data Interference
  - i. The damaging, deletion, deterioration, alteration or suppression of computer data without right. [6 + 3 = 9]

If you forget your password for a website and you click [Forgot my password], sometimes the company sends you a new password by email, sometimes it sends you your old password by email, sometimes it sends you a link for you to reset your password. Compare these three cases in terms of vulnerability of the website owner. [2 + 2 + 2 = 6]

You receive an email from your bank telling you there is a problem with your account. The email provides instructions and a link so you can log into your account and fix the problem.

- a. Is there any problem here? Explain clearly.
- b. What action you should take? Explain at least two different alternatives. [2 + 2 = 4]

Describe the 'Weaponization' phase of Cyber Kill Chain. This stage is considered challenging for defenders. Why? Give at least one example of activities that adversaries perform at this stage. What kind of actions can defenders take during this state? [2 + 2 + 1 + 1 = 6]