websites. Pretexting is pretending to be an authority figure in an organization. By contacting members of the organization, the employees believe the authority figure is real and will do as they say. An example may be the (fake) authority figure suggests to employees to fill out contact information on a (also fake) website with names and addresses of yourself and/or emergency contact information of family or relatives. Advance-fee frauds involve scheming a person into paying additional fees or balances that are deemed to be true but actually are not.

Organizations have many methods to protect from social engineering. Reporting and deleting suspicious emails is one of these major preventative tactics. After a bad email is reported, the company can put out communications to IT departments and other departments of the malicious intent of the email and will suggest to everyone to delete the email or block the sender. Social engineering can be prevented further by employee training, due care and due diligence measures, and physical protections such as screen filters and departmentalization, which prevent unwanted shoulder surfers and separate groups sharing similar responsibilities in data, respectively.

Correct Answer: [None]

Response Feedback: [None Given]

Question 2

3 out of 3 points

The Secret Service is charged with safeguarding the nation's financial infrastructure and payments systems to preserve the integrity of the economy.

Selected Answer: ✓ True

Answers: ✓ True

False

Question 3

3 out of 3 points

The possession of information is the quality or state of having value for some purpose or end.

Selected Answer: ✓ False

Answers: True

✓ False

Question 4

3 out of 3 points

An act of theft performed by a hacker falls into the category of "theft," but is also often accompanied by defacement actions to delay discovery and thus may also be placed within the category of "forces of nature."

Selected Answer: ✓ False

Answers: True

✓ False