Question: 1

Which of the following is NOT an ethical canon of the ISC2?

A. B. C. D.
Protect society, the common good, necessary public trust and confidence, and the infrastructure
Provide active and qualified service to principal
Advance and protect the profession
Act honorably, honestly, justly, responsibly and legally

Answer: B

Explanation:

The Code of Ethics states, "Provide diligent and competent service to principals," not "Provide active and qualified service to principals."; all other options are valid canons of the Code of Ethics (see ISC2 Study Guide, Domain 1). "Provide active and qualified service to principals" is not listed among the ISC2 ethical canons, which focus on broader societal, professional and ethical guidelines rather than specific service obligations to principals.

The other options are incorrect because they directly reflect ISC2's ethical canons. "Protect society, the common good, necessary public trust, and infrastructure" emphasizes the responsibility of cybersecurity professionals to protect broader societal interests. "Act honorably, honestly, fairly, responsibly, and legally" outlines the personal integrity and ethical behavior expected of professionals. "Advance and protect the profession" encourages actions that enhance the credibility and standards of the cybersecurity field. Each of these principles is closely aligned with ISC2's commitment to ethics and professional conduct in cybersecurity.

Domain

Understand ISC2 Code of Ethics

Question: 2

Which of the following is NOT an example of a physical security control?

A. B. C. D.
Security cameras
Remote control electronic locks
Biometric access controls
Firewalls

Answer: D

Explanation:

Firewalls are network security devices that monitor and control incoming and outgoing network traffic based on predetermined security rules to create a barrier between a trusted internal network and untrusted external networks, such as the Internet, to prevent unauthorized access to the network. Firewalls are not physical controls; they are a type of technical control.

For example, an organization might use a firewall to block incoming connections from certain IP addresses that are known to be associated with malicious activity. This setup helps protect the network from unauthorized access, viruses, or denial-of-service attacks. The firewall acts as a filter, allowing or blocking traffic based on the network administrator's set of security rules.

On the other hand, security cameras, lighting, and guards are all examples of physical security controls. Security cameras monitor and record physical activity in and around a facility. Lighting enhances visibility and can deter criminal activity by making it difficult for intruders to hide. Guards are personnel employed to protect property and individuals by maintaining a physical presence to prevent and deter illegal or unauthorized activity. Each of these controls directly impacts the physical security of an environment by adding layers of protection against physical threats.

Domain

Understand Security Controls

Question: 3

Which type of attack attempts to trick the user into revealing personal information by sending a fraudulent message?

A. Cross-Site Scripting

B. Trojans

C. Phishing

D. Denials of Service

Answer:C

Explanation:

A phishing attack emails a fraudulent message to trick the recipient into disclosing sensitive information to the attacker. A Cross-Site Scripting attack tries to execute code on another website. Trojans are software that appear legitimate, but that have hidden malicious functions. Trojans may be sent in a message, but are not the message themselves. A denial of service attack (DoS) consists in compromising the availability of a system or service through a malicious overload of requests, which causes the activation of safety mechanisms that delay or limit the availability of that system or service.

Domain Understand Network (Cyber) Threats and Attacks

Question: 4

Which of the following is NOT a feature of a cryptographic hash function?

A. Useful

B. Deterministic

C. Reversible

D. Unique

Answer:C

Explanation:

A cryptographic hash function should be unique, deterministic, useful, tamper-evident (also referred to as 'the avalanche effect' or 'integrity assurance') and non-reversible (also referred to as 'one-way'). Nonreversible means it is impossible to reverse the hash function to derive the original text of a message from its hash output value (see ISC2 Study Guide, chapter 5, module 1, under Encryption Overview). Thus, the 'reversible' feature is not a feature of a hash function.

Domain

Understand Data Security

Question: 5

Which physical access control would be MOST effective against tailgating?

A. Turnstiles
B. Barriers
C. Locks
D. Fences

Answer: A

Explanation:

Turnstiles aredesigned to allow only one person through at a time, making them the most effective physical access control against tailgating. Tailgating occurs when an unauthorized person follows an authorized person into a secured area.

For example, consider a secure corporate office that uses a turnstile at the main entrance. Each employee has a unique badge. When the card is swiped, the turnstile allows one person through. If another person tries to follow (or bypass) without swiping the card, the turnstile remains locked, effectively preventing unauthorized access.

The other options are not as effective against tailgating. Fences and barriers are wrong because while they can restrict access to an area, they do not prevent tailgating once an authorized person opens a gate or barrier. Locks are also incorrect because, like fences and barriers, they can secure an area but do not prevent tailgating. Once an authorized person unlocks a door, an unauthorized person can easily follow them inside.

Domain

Understand Physical Access Controls