



SY0-701^{Q&As}

CompTIA Security+ 2024

Pass CompTIA SY0-701 Exam with 100% Guarantee

Free Download Real Questions & Answers **PDF** and **VCE** file from:

<https://www.pass4itsure.com/sy0-701.html>

100% Passing Guarantee
100% Money Back Assurance

Following Questions and Answers are all new published by CompTIA
Official Exam Center

-  **Instant Download** After Purchase
-  **100% Money Back** Guarantee
-  **365 Days** Free Update
-  **800,000+** Satisfied Customers



**QUESTION 1**

After a security awareness training session, a user called the IT help desk and reported a suspicious call. The suspicious caller stated that the Chief Financial Officer wanted credit card information in order to close an invoice. Which of the following topics did the user recognize from the training?

- A. Insider threat
- B. Email phishing
- C. Social engineering
- D. Executive whaling

Correct Answer: C

Social engineering is the practice of manipulating people into performing actions or divulging confidential information, often by impersonating someone else or creating a sense of urgency or trust. The suspicious caller in this scenario was trying to use social engineering to trick the user into giving away credit card information by pretending to be the CFO and asking for a payment. The user recognized this as a potential scam and reported it to the IT help desk. The other topics are not relevant to this situation.

References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page 19 1

QUESTION 2

A company wants to improve end users experiences when they tog in to a trusted partner website The company does not want the users to be issued separate credentials for the partner website

Which of the following should be implemented to allow users to authenticate using their own credentials to log in to the trusted partner\\'s website?

- A. Directory service
- B. AAA server
- C. Federation
- D. Multifactor authentication

Correct Answer: C

Federation means the company trusts accounts created and managed by a different network. It connects the identity management services of multiple systems

QUESTION 3

A user is attempting to patch a critical system, but the patch fails to transfer. Which of the following access controls is most likely inhibiting the transfer?

- A. Attribute-based



- B. Time of day
- C. Role-based
- D. Least privilege

Correct Answer: D

The least privilege principle states that users and processes should only have the minimum level of access required to perform their tasks. This helps to prevent unauthorized or unnecessary actions that could compromise security. In this case, the patch transfer might be failing because the user or process does not have the appropriate permissions to access the critical system or the network resources needed for the transfer. Applying the least privilege principle can help to avoid this issue by granting the user or process the necessary access rights for the patching activity.

References: CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, page

QUESTION 4

A security analyst and the management team are reviewing the organizational performance of a recent phishing campaign. The user click-through rate exceeded the acceptable risk threshold, and the management team wants to reduce the impact when a user clicks on a link in a phishing message. Which of the following should the analyst do?

- A. Place posters around the office to raise awareness of common phishing activities.
- B. Implement email security filters to prevent phishing emails from being delivered
- C. Update the EDR policies to block automatic execution of downloaded programs.
- D. Create additional training for users to recognize the signs of phishing attempts.

Correct Answer: C

An endpoint detection and response (EDR) system is a security tool that monitors and analyzes the activities and behaviors of endpoints, such as computers, laptops, mobile devices, and servers. An EDR system can detect, prevent, and respond to various types of threats, such as malware, ransomware, phishing, and advanced persistent threats (APTs). One of the features of an EDR system is to block the automatic execution of downloaded programs, which can prevent malicious code from running on the endpoint when a user clicks on a link in a phishing message. This can reduce the impact of a phishing attack and protect the endpoint from compromise. Updating the EDR policies to block automatic execution of downloaded programs is a technical control that can mitigate the risk of phishing, regardless of the user's awareness or behavior. Therefore, this is the best answer among the given options. The other options are not as effective as updating the EDR policies, because they rely on administrative or physical controls that may not be sufficient to prevent or stop a phishing attack. Placing posters around the office to raise awareness of common phishing activities is a physical control that can increase the user's knowledge of phishing, but it may not change their behavior or prevent them from clicking on a link in a phishing message. Implementing email security filters to prevent phishing emails from being delivered is an administrative control that can reduce the exposure to phishing, but it may not be able to block all phishing emails, especially if they are crafted to bypass the filters. Creating additional training for users to recognize the signs of phishing attempts is an administrative control that can improve the user's skills of phishing detection, but it may not guarantee that they will always be vigilant or cautious when receiving an email. Therefore, these options are not the best answer for this question.

References: Endpoint Detection and Response -CompTIA Security+ SY0-701 -2.2, video at 5:30; CompTIA Security+ SY0-701 Certification Study Guide, page 163.

**QUESTION 5**

An administrator assists the legal and compliance team with ensuring information about customer transactions is archived for the proper time period. Which of the following data policies is the administrator carrying out?

- A. Compromise
- B. Retention
- C. Analysis
- D. Transfer
- E. Inventory

Correct Answer: B

A data retention policy is a set of rules that defines how long data should be stored and when it should be deleted or archived. An administrator assists the legal and compliance team with ensuring information about customer transactions is archived for the proper time period by following the data retention policy of the organization. This policy helps the organization to comply with legal and regulatory requirements, optimize storage space, and protect data privacy and security.

References CompTIA Security+ Study Guide: Exam SY0-701, 9th Edition, Chapter 3, Section 3.4, page 1211 CompTIA Security+ Practice Tests: Exam SY0-701, 3rd Edition, Chapter 3, Question 15, page 832

[SY0-701 PDF Dumps](#)

[SY0-701 Practice Test](#)

[SY0-701 Exam Questions](#)