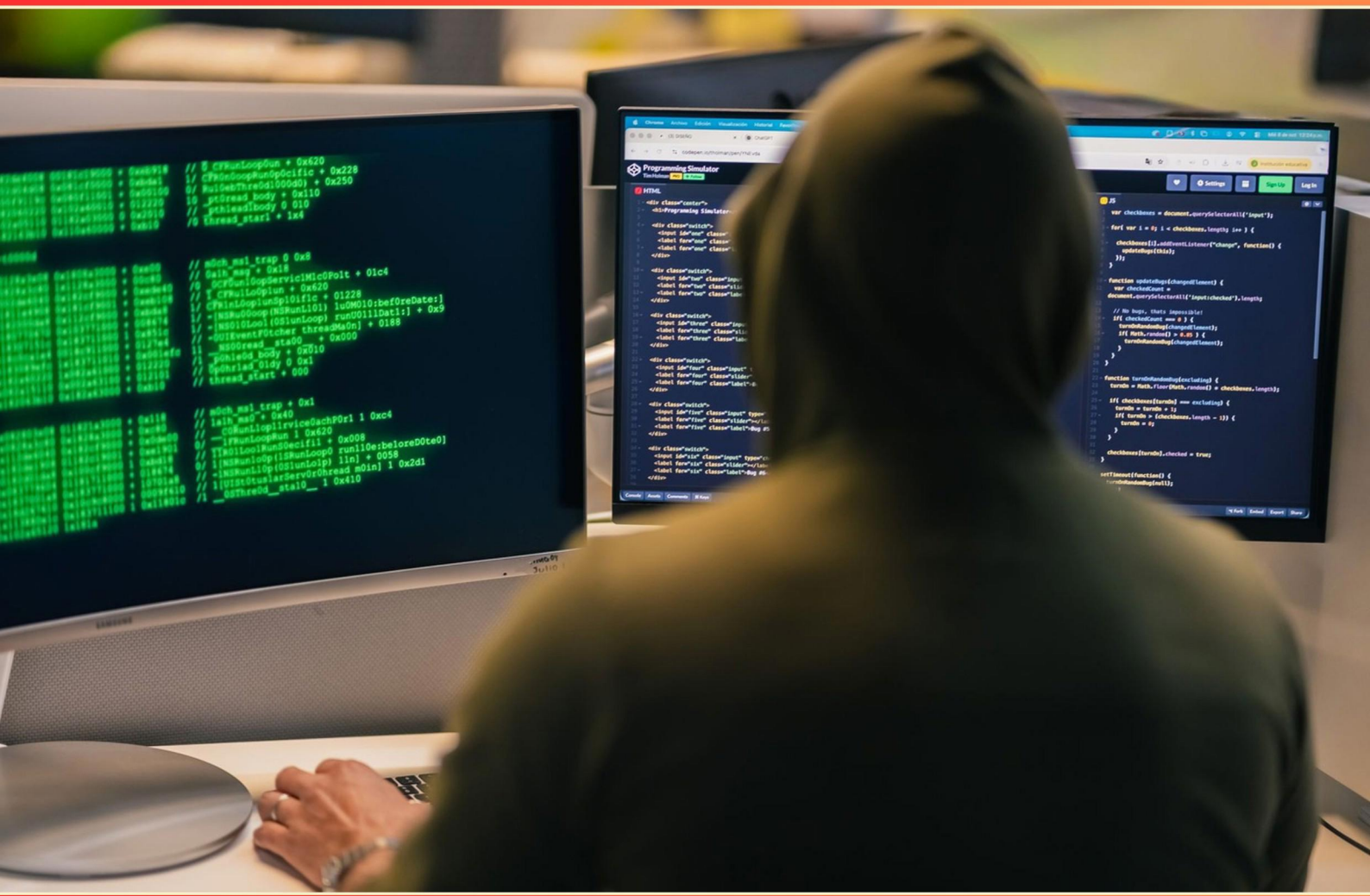
KNOWBE4 TRAINING PRACTICE TEST (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://knowbe4training.examzify.com

Copyright © 2026 by Examzify - A Kaluba Technologies Inc. product.

ALL RIGHTS RESERVED.

No part of this book may be reproduced or transferred in any form or by any means, graphic, electronic, or mechanical, including photocopying, recording, web distribution, taping, or by any information storage retrieval system, without the written permission of the author.

Notice: Examzify makes every reasonable effort to obtain accurate, complete, and timely information about this product from reliable sources.

SAMPLE

Table of Contents

Copyright 1

Table of Contents 2

Introduction 3

How to Use This Guide 4

Questions 5

Answers 8

Explanations 10

Next Steps 15

SAMPLE

Introduction

Preparing for a certification exam can feel overwhelming, but with the right tools, it becomes an opportunity to build confidence, sharpen your skills, and move one step closer to your goals. At Examzify, we believe that effective exam preparation isn't just about memorization, it's about understanding the material, identifying knowledge gaps, and building the test-taking strategies that lead to success.

This guide was designed to help you do exactly that.

Whether you're preparing for a licensing exam, professional certification, or entry-level qualification, this book offers structured practice to reinforce key concepts. You'll find a wide range of multiple-choice questions, each followed by clear explanations to help you understand not just the right answer, but why it's correct.

The content in this guide is based on real-world exam objectives and aligned with the types of questions and topics commonly found on official tests. It's ideal for learners who want to:

- Practice answering questions under realistic conditions,
- Improve accuracy and speed,
- Review explanations to strengthen weak areas, and
- Approach the exam with greater confidence.

We recommend using this book not as a stand-alone study tool, but alongside other resources like flashcards, textbooks, or hands-on training. For best results, we recommend working through each question, reflecting on the explanation provided, and revisiting the topics that challenge you most.

Remember: successful test preparation isn't about getting every question right the first time, it's about learning from your mistakes and improving over time. Stay focused, trust the process, and know that every page you turn brings you closer to success.

Let's begin.

SAMPLE

How to Use This Guide

This guide is designed to help you study more effectively and approach your exam with confidence. Whether you're reviewing for the first time or doing a final refresh, here's how to get the most out of your Examzify study guide:

1. Start with a Diagnostic Review

Skim through the questions to get a sense of what you know and what you need to focus on. Your goal is to identify knowledge gaps early.

2. Study in Short, Focused Sessions

Break your study time into manageable blocks (e.g. 30 – 45 minutes). Review a handful of questions, reflect on the explanations.

3. Learn from the Explanations

After answering a question, always read the explanation, even if you got it right. It reinforces key points, corrects misunderstandings, and teaches subtle distinctions between similar answers.

4. Track Your Progress

Use bookmarks or notes (if reading digitally) to mark difficult questions. Revisit these regularly and track improvements over time.

5. Simulate the Real Exam

Once you're comfortable, try taking a full set of questions without pausing. Set a timer and simulate test-day conditions to build confidence and time management skills.

6. Repeat and Review

Don't just study once, repetition builds retention. Re-attempt questions after a few days and revisit explanations to reinforce learning. Pair this guide with other Examzify tools like flashcards, and digital practice tests to strengthen your preparation across formats.

There's no single right way to study, but consistent, thoughtful effort always wins. Use this guide flexibly, adapt the tips above to fit your pace and learning style. You've got this!

SAMPLE

Questions

SAMPLE

1. **Which assessment tool checks if an organization's users' passwords are in breaches?**

   A. Password Strength Tester

   B. Breached Password Test

   C. Security Risk Analyzer

   D. Password Reuse Checker

2. **What is the primary significance of data backup?**

   A. It duplicates data for easier access

   B. It ensures data can be recovered in case of loss or ransomware attacks

   C. It increases the speed of file retrieval

   D. It prevents unauthorized access to data

3. **What is meant by the term “shoulder surfing" in cybersecurity?**

   A. Watching someone type their password from a distance

   B. Looking over someone's shoulder to gain unauthorized access to information

   C. Viewing data on a public computer screen

   D. Monitoring a network for unusual activity

4. **What is the function of a whitelist?**

   A. A list of banned websites

   B. A list of trusted websites you have allowed access to for safer surfing

   C. A list of websites under review

   D. A backup of all user data

5. **What is the primary function of a firewall in a computer system?**

   A. To enhance software performance

   B. To allow all traffic access to the system

   C. To monitor and filter incoming and outgoing network traffic

   D. To provide data storage solutions

6. **What is a core feature of the Phish Alert Button?**

   A. Allows users to share emails with colleagues

   B. Enables users to report potential phishing attempts safely

   C. Updates the company's email security policy automatically

   D. Automatically blocks spam from known senders

SAMPLE

7. What aspect does Active Directory help manage within an organization?

A. Financial resources

B. User access and permissions

C. Network hardware

D. Customer relationships

8. What does LMS stand for in the context of cybersecurity training?

A. Learning Management System

B. Legal Management System

C. Logical Management Suite

D. Layered Management Security

9. What role does a utility software play in computer operation?

A. Enhancing graphics and video processing

B. Maintaining and optimizing the performance of a computer

C. Developing new web applications

D. Providing real-time communication tools

10. What is a key component of the Payment Card Industry Data Security Standard (PCI-DSS)?

A. Keeping cardholder data secure

B. Tracking customer behavior

C. Enhancing customer experience

D. Marketing promotional offers

SAMPLE

Answers

SAMPLE

1. B
2. B
3. B
4. B
5. C
6. B
7. B
8. A
9. B
10. A

SAMPLE

Explanations

SAMPLE

1. Which assessment tool checks if an organization's users' passwords are in breaches?

A. Password Strength Tester

B. Breached Password Test

C. Security Risk Analyzer

D. Password Reuse Checker

The Breached Password Test is designed specifically to evaluate whether the passwords used by an organization's users have been compromised in known data breaches. This tool typically cross-references the passwords entered against databases of leaked passwords collected from various data breaches, helping organizations identify weak points in their security strategy. By using the Breached Password Test, organizations can encourage users to change passwords that may have been exposed, thus reducing the risk of unauthorized access to accounts. This proactive approach to password security is essential for maintaining a robust cybersecurity posture. In contrast, options like the Password Strength Tester focus on evaluating the complexity and security level of passwords rather than checking if they have been previously exposed. The Security Risk Analyzer assesses a broader range of security issues beyond just passwords, and the Password Reuse Checker determines whether users are recycling passwords across different accounts, which is not the same as identifying already breached passwords.

2. What is the primary significance of data backup?

A. It duplicates data for easier access

B. It ensures data can be recovered in case of loss or ransomware attacks

C. It increases the speed of file retrieval

D. It prevents unauthorized access to data

The primary significance of data backup lies in its role in ensuring that data can be recovered in the event of loss, whether due to accidental deletion, hardware failure, or malicious actions such as ransomware attacks. Backups create a secure copy of critical information, allowing organizations and individuals to restore their data and continue their operations without significant disruption. This recovery capability is vital for maintaining data integrity and business continuity, especially in an increasingly digital world where data is paramount. The other options, while they may describe benefits or features associated with data management, do not capture the essential purpose of backups. The idea of duplication for easier access is related but does not address recovery needs. Speed of file retrieval is not a primary function of backups, as their main focus is on preservation and restoration. Lastly, while preventing unauthorized access is important for data security, it does not relate directly to the concept of creating backup copies, which is fundamentally about recovery rather than access control.

SAMPLE

3. What is meant by the term “shoulder surfing" in cybersecurity?

A. Watching someone type their password from a distance

B. Looking over someone's shoulder to gain unauthorized access to information

C. Viewing data on a public computer screen

D. Monitoring a network for unusual activity

The term “shoulder surfing" in cybersecurity refers specifically to the act of looking over someone's shoulder to gain unauthorized access to sensitive information, such as passwords or personal identification numbers. This typically occurs in public places or environments where personal devices are being used, making it easy for an attacker to observe what another individual is entering or viewing on their screen. This behavior is particularly concerning because it can happen without the victim's awareness, leading to the compromise of sensitive information. It emphasizes the importance of practicing security measures in public settings, such as being mindful of surroundings when entering personal information. The other options, while related to cybersecurity, don't capture the specific action referred to by "shoulder surfing." Watching someone from a distance doesn't imply direct observation of sensitive information, and viewing data on a public screen, while a security risk, is a different type of intrusion. Monitoring a network involves tracking unusual activity but does not pertain to physically observing someone's actions.

4. What is the function of a whitelist?

A. A list of banned websites

B. A list of trusted websites you have allowed access to for safer surfing

C. A list of websites under review

D. A backup of all user data

A whitelist functions as a list of trusted websites that has been permitted access for users, enhancing safer browsing experiences. This approach helps to protect users from potentially harmful content by only allowing connections to sites deemed safe. Organizations often employ whitelists to guarantee that only verified, reliable resources are accessible, reducing the risk of exposure to malicious sites which could contain malware or phishing attempts. The purpose of whitelisting is to create a controlled environment for internet usage, aligning with security protocols that minimize the potential for threats. Unlike bans on sites, which could be more restrictive and less targeted, a whitelist directly focuses on promoting safety by encouraging access to verified and safe sources on the internet.

5. What is the primary function of a firewall in a computer system?

A. To enhance software performance

B. To allow all traffic access to the system

C. To monitor and filter incoming and outgoing network traffic

D. To provide data storage solutions

The primary function of a firewall in a computer system is to monitor and filter incoming and outgoing network traffic. Firewalls act as a security barrier between a trusted internal network and untrusted external networks, such as the internet. They analyze data packets based on predefined security rules and policies to decide whether to allow or block the traffic. By monitoring this traffic, firewalls help protect systems from unauthorized access, cyber attacks, and various types of malicious activities. They can provide essential logging and reporting features that help administrators understand traffic patterns and potential security threats. Overall, the role of a firewall is critical in maintaining the overall security posture of a networked environment. Other choices, such as enhancing software performance or providing data storage, do not accurately reflect the security-centric function of a firewall. Similarly, allowing all traffic access directly contradicts the protective purpose of a firewall, which is to restrict and manage network access.

SAMPLE

6. What is a core feature of the Phish Alert Button?

A. Allows users to share emails with colleagues

B. Enables users to report potential phishing attempts safely

C. Updates the company's email security policy automatically

D. Automatically blocks spam from known senders

The Phish Alert Button is designed primarily to empower users by enabling them to report suspected phishing attempts safely and efficiently. This functionality is crucial because it allows employees to contribute actively to the organization's cybersecurity efforts. When a user suspects an email might be phishing, they can click the button to alert the IT or security team, who can then investigate the report and take necessary action, such as blocking malicious senders or warning other employees. This proactive approach not only aids in preventing potential breaches but also raises awareness among users about identifying phishing attempts. Highlighting a culture of vigilance and response helps organizations stay ahead of threats. Other features mentioned, such as sharing emails with colleagues or automatically blocking spam, are not part of the core function of the Phish Alert Button; its primary purpose is focused on enabling users to report potential threats effectively.

7. What aspect does Active Directory help manage within an organization?

A. Financial resources

B. User access and permissions

C. Network hardware

D. Customer relationships

Active Directory plays a critical role within an organization by managing user access and permissions. It serves as a centralized directory service that allows administrators to create and manage user accounts, enforce security policies, and control access to various resources within the network. By organizing users into groups, assigning permissions, and implementing policies, Active Directory ensures that only authorized individuals can access specific data and applications, helping to maintain security and compliance within the organization. The ability to manage permissions effectively not only enhances security but also streamlines user management, making it easier for IT personnel to onboard and offboard employees, as well as to adjust access levels according to changing roles and responsibilities. This centralized management is key for maintaining the integrity of user access across the entire organization.

8. What does LMS stand for in the context of cybersecurity training?

A. Learning Management System

B. Legal Management System

C. Logical Management Suite

D. Layered Management Security

The term "LMS" stands for Learning Management System in the context of cybersecurity training. A Learning Management System is a software application or web-based technology designed to plan, implement, and assess a specific learning process. In cybersecurity training, organizations utilize LMS to deliver training materials, track employee progress, manage course content, and analyze training results. This ensures that employees are equipped with essential knowledge about cybersecurity threats, best practices, and compliance requirements. By using an LMS, organizations can enhance their training effectiveness and user engagement, making it a key component in ongoing cybersecurity education initiatives.

SAMPLE

9. What role does a utility software play in computer operation?

A. Enhancing graphics and video processing

B. Maintaining and optimizing the performance of a computer

C. Developing new web applications

D. Providing real-time communication tools

Utility software plays a crucial role in maintaining and optimizing the performance of a computer. This type of software is designed to help manage, maintain, and control computer resources, ensuring that the system operates efficiently. It includes tools for disk management, file management, system diagnostics, and performance monitoring. By performing tasks such as cleaning up temporary files, defragmenting the hard drive, or managing system backups, utility software helps improve the overall functionality and longevity of a computer system. This focus on system maintenance differentiates it from other types of software. For instance, enhancing graphics and video processing typically falls under the category of application software or drivers, not utility software. Similarly, developing new web applications is a task performed by development tools, whereas providing real-time communication tools aligns more closely with communication software. Thus, the primary function of utility software is focused on optimizing performance and maintaining the health of the computing environment.

10. What is a key component of the Payment Card Industry Data Security Standard (PCI-DSS)?

A. Keeping cardholder data secure

B. Tracking customer behavior

C. Enhancing customer experience

D. Marketing promotional offers

A key component of the Payment Card Industry Data Security Standard (PCI-DSS) is keeping cardholder data secure. The primary objective of PCI-DSS is to protect sensitive payment information and ensure that organizations handling credit card transactions do so in a secure manner. This involves implementing a set of security standards designed to safeguard cardholder data against theft and fraud. Properly securing cardholder data includes measures such as encrypting data during transmission, regularly updating security software, conducting vulnerability assessments, and maintaining a secure network. These elements are essential for reducing the risk of data breaches and protecting both businesses and customers from potential financial harm. The other options, while they may serve important functions in a business context, don't align with the primary focus of PCI-DSS, which is centered around data security. Therefore, keeping cardholder data secure is fundamental to the intended purpose of PCI-DSS compliance.

SAMPLE

Next Steps

Congratulations on reaching the final section of this guide. You've taken a meaningful step toward passing your certification exam and advancing your career.

As you continue preparing, remember that consistent practice, review, and self-reflection are key to success. Make time to revisit difficult topics, simulate exam conditions, and track your progress along the way.

If you need help, have suggestions, or want to share feedback, we'd love to hear from you. Reach out to our team at hello@examzify.com.

Or visit your dedicated course page for more study tools and resources:

https://knowbe4training.examzify.com

We wish you the very best on your exam journey. You've got this!

SAMPLE