DEPARTMENT OF DEFENSE (DOD) CYBER AWARENESS PRACTICE EXAM (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://dod-cyberawareness.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 16

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. What should you do if you suspect a cybersecurity incident?

A. Ignore it

B. Conduct your own investigation

C. Report it immediately to the designated authority or IT department

D. Change all your passwords

2. What does "boundary defense" refer to in cybersecurity?

A. Protecting internal users

B. Using methods to secure network perimeters

C. Training users on security staffs

D. Implementing physical security measures

3. What is the importance of regular software updates?

A. To enable more user features

B. To fix vulnerabilities and improve security

C. To increase application load time

D. To clutter devices with unnecessary data

4. Which designation includes Personally Identifiable Information (PII) and Protected Health Information (PHI)?

A. Controlled Unclassified Information (CUI)

B. Top Secret Information

C. Unclassified Information

D. Publicly Available Information

5. What is a cybersecurity incident?

A. Any suspected breach of data or unauthorized access to systems

B. Routine maintenance of IT systems to enhance performance

C. A common software update process

D. Periodic user training on security measures

SAMPLE

6. What type of damage could the disclosure of Top Secret information cause to national security?

A. Minimal damage

B. Severe damage

C. Moderate damage

D. Exceptionally grave damage

7. What does social engineering involve in the context of cybersecurity?

A. Teaching users about security policies

B. Manipulating individuals into giving confidential information

C. Employing strong encryption methods

D. Updating software regularly

8. What is defined as a "zero-day" exploit?

A. A vulnerability that has been fixed by developers

B. A new software feature released without testing

C. A vulnerability that is exploited before developers can create a fix

D. An outdated security measure

9. What does "pretexting" involve?

A. Creating a secure network

B. Developing new software

C. Creating a fabricated scenario to steal personal information

D. Implementing firewalls

10. When should software updates typically be applied?

A. At the end of each month

B. Whenever the user remembers

C. As soon as updates are available

D. Only when a major issue arises

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. What should you do if you suspect a cybersecurity incident?

A. Ignore it

B. Conduct your own investigation

C. Report it immediately to the designated authority or IT department

D. Change all your passwords

If you suspect a cybersecurity incident, the appropriate action is to report it immediately to the designated authority or the IT department. This response is crucial because cybersecurity incidents can potentially lead to significant data breaches or harmful consequences if not addressed promptly by trained professionals. The designated authority is equipped with the resources and expertise necessary to assess the situation, mitigate any risks, and take appropriate actions to protect the organization's systems and data. Prompt reporting not only facilitates a faster response to the threat but also helps in preserving evidence that may be needed for further investigation and remediation efforts. Waiting or taking personal action could complicate the situation or lead to unintentional damage or data loss, highlighting the importance of following established procedures in the event of a suspected incident.

2. What does "boundary defense" refer to in cybersecurity?

A. Protecting internal users

B. Using methods to secure network perimeters

C. Training users on security staffs

D. Implementing physical security measures

"Boundary defense" in cybersecurity specifically refers to the strategies and methods used to secure the network perimeters from unauthorized access and cyber threats. This includes deploying firewalls, intrusion detection systems, and other security technologies and protocols that provide a protective barrier between the internal network and external threats. By focusing on the network's boundary, organizations aim to minimize the risk posed by external attacks, thereby safeguarding sensitive data and ensuring the integrity of their systems. The other options, while related to cybersecurity, do not precisely define boundary defense. Protecting internal users pertains to user access control and security within the network, which is a different focus. Training users on security practices is vital for fostering a security-aware culture, but it does not directly involve boundary defense measures. Implementing physical security measures is also critical for protecting hardware and sensitive data, but it addresses a different aspect of cybersecurity, focusing more on the physical environment rather than the digital network perimeter.

3. What is the importance of regular software updates?

A. To enable more user features

B. To fix vulnerabilities and improve security

C. To increase application load time

D. To clutter devices with unnecessary data

Regular software updates are critical primarily for fixing vulnerabilities and improving security. Software is frequently targeted by cybercriminals who exploit security weaknesses to gain unauthorized access to systems or data. When vulnerabilities are identified, developers release updates to patch these security holes, thereby protecting systems from potential attacks. In addition to security enhancements, updates often include improvements in performance, stability, and functionality. However, the foremost priority of these updates is to ensure that systems remain secure from evolving threats. By keeping software up to date, users mitigate risks and help safeguard sensitive information, which is vital for maintaining the integrity of systems, especially in environments related to the Department of Defense and other sensitive operations. While some updates might introduce new features or adjustments to how applications operate, the primary reason for conducting regular updates in cybersecurity contexts is to enhance security measures and protect against potential vulnerabilities.

SAMPLE

4. Which designation includes Personally Identifiable Information (PII) and Protected Health Information (PHI)?

A. Controlled Unclassified Information (CUI)

B. Top Secret Information

C. Unclassified Information

D. Publicly Available Information

The correct designation that encompasses both Personally Identifiable Information (PII) and Protected Health Information (PHI) is Controlled Unclassified Information (CUI). CUI is a category of unclassified information that requires specific safeguarding and dissemination controls as mandated by law, regulation, or government-wide policy. PII refers to any information that can be used to identify an individual and must be protected to prevent identity theft and other privacy violations. Similarly, PHI is related to health information that can be tied to an individual, and it is particularly sensitive due to its implications in health privacy laws, such as HIPAA (Health Insurance Portability and Accountability Act). This classification acknowledges the sensitive nature of both types of information, establishing that they require protection from unauthorized access, misuse, or disclosure. By recognizing PII and PHI as CUI, government agencies are mandated to implement appropriate security measures to secure this data and comply with relevant regulations. Other designations, such as Top Secret Information, Unclassified Information, or Publicly Available Information do not involve the same level of sensitivity or required protections as CUI regarding personal and health-related data. They either refer to higher security levels or do not necessitate the same standard of safeguarding for sensitive information.

5. What is a cybersecurity incident?

A. Any suspected breach of data or unauthorized access to systems

B. Routine maintenance of IT systems to enhance performance

C. A common software update process

D. Periodic user training on security measures

A cybersecurity incident refers to any event that indicates a potential breach of data or unauthorized access to systems. This definition encompasses various scenarios where sensitive information is compromised or systems are accessed without proper authorization, leading to potential harm to the organization's integrity, confidentiality, or availability of its data and resources. Recognizing this distinction is vital, as it allows organizations to respond appropriately by investigating, mitigating, and preventing further incidents. The other options do not fit the definition of a cybersecurity incident. Routine maintenance of IT systems is a proactive measure intended to keep systems functioning efficiently and securely, rather than a response to any unauthorized actions. Similarly, a common software update process is a necessary task meant to patch vulnerabilities and enhance functionality, while periodic user training focuses on educating staff about cybersecurity best practices, which is a preventive measure rather than an incident.

SAMPLE

6. What type of damage could the disclosure of Top Secret information cause to national security?

A. Minimal damage

B. Severe damage

C. Moderate damage

D. Exceptionally grave damage

The disclosure of Top Secret information could cause exceptionally grave damage to national security because Top Secret information relates to the most sensitive national security matters. This classification indicates that unauthorized disclosure could cause exceptionally grave damage to the United States or its allies, potentially compromising military operations, intelligence sources and methods, or national defense strategies. Such a breach could provide adversaries with critical insights that lead to strategic disadvantages, loss of life, or greater risks to the nation's security interests. This level of impact is distinctly recognized within the classification system to underscore the seriousness of safeguarding such information.

7. What does social engineering involve in the context of cybersecurity?

A. Teaching users about security policies

B. Manipulating individuals into giving confidential information

C. Employing strong encryption methods

D. Updating software regularly

Social engineering in the context of cybersecurity primarily revolves around the manipulation of individuals to obtain confidential information or unauthorized access. This tactic exploits psychological factors rather than technical vulnerabilities. Attackers often use deception to trick individuals into revealing personal details, such as passwords or financial information, by creating a sense of urgency, trust, or fear. For instance, an attacker might impersonate an IT support technician and ask a user for their login credentials under the pretense of needing to resolve an issue. This approach relies heavily on human behavior and can be particularly effective because it bypasses conventional security measures that focus on systems and technology rather than the human element. The other options revolve around proactive security measures such as educating users about policies, using encryption, and ensuring software updates are applied. While these are essential components of an overall cybersecurity strategy, they do not directly pertain to the deceptive tactics and manipulation that define social engineering.

SAMPLE

8. What is defined as a "zero-day" exploit?

A. A vulnerability that has been fixed by developers

B. A new software feature released without testing

C. A vulnerability that is exploited before developers can create a fix

D. An outdated security measure

A "zero-day" exploit refers specifically to a vulnerability that is actively exploited by attackers before the developers have had the opportunity to create and issue a fix or patch for the identified security flaw. This means that the developers are unaware of the vulnerability at the time it is being exploited, hence the term "zero-day," which indicates that there have been zero days available for the developers to address the issue. These types of exploits are particularly dangerous because they can be used to infiltrate systems, steal sensitive information, or cause damage without any warning or mitigation available to the users or administrators of the affected systems. Cybersecurity professionals emphasize the importance of proactive measures to identify and address potential vulnerabilities before they can be exploited in a zero-day manner. Other options describe concepts related to security but do not accurately define what a zero-day exploit is. A vulnerability that has been fixed by developers would not be classified as zero-day, as that indicates it has already been addressed. A new software feature released without testing pertains to development practices but doesn't convey the specific threat posed by zero-day vulnerabilities. Finally, an outdated security measure lacks relevance to the concept of zero-day exploits since the term specifically focuses on new vulnerabilities being exploited before a patch is available.

9. What does "pretexting" involve?

A. Creating a secure network

B. Developing new software

C. Creating a fabricated scenario to steal personal information

D. Implementing firewalls

Pretexting involves creating a fabricated scenario to steal personal information. This social engineering technique is commonly used by attackers who impersonate legitimate organizations or individuals to manipulate targets into divulging sensitive information. By establishing trust through a false narrative, the attacker can extract details like passwords, credit card numbers, or other confidential data from unsuspecting victims. It often requires careful planning and an understanding of the target's environment, making it a sophisticated form of deception. This is particularly relevant for individuals and organizations concerned about data security, as attacks can have significant implications if personal information is compromised. The other options focus on cybersecurity infrastructure and software development rather than the psychological tactics used in pretexting. For instance, creating a secure network and implementing firewalls are proactive measures aligning with defensive strategies, while developing software pertains to the technological side rather than interpersonal manipulation tactics.

SAMPLE

10. When should software updates typically be applied?

A. At the end of each month

B. Whenever the user remembers

C. As soon as updates are available

D. Only when a major issue arises

Applying software updates as soon as they are available is critical for maintaining the security and functionality of systems. Software updates often include important patches that address vulnerabilities, fix bugs, and provide enhancements. When these updates are delayed, systems remain exposed to potential security breaches that could exploit the very vulnerabilities the updates are designed to mitigate. Timely updates help ensure that all security measures are up to date, which is particularly essential in a Department of Defense context where the stakes are high for sensitive information. By prioritizing immediate application of updates, users can proactively defend against threats and improve the overall integrity and performance of their software. In contrast, setting a monthly schedule for updates, relying on memory, or waiting until a major issue occurs could leave systems unprotected and susceptible to attacks in the interim. Therefore, the practice of applying updates as soon as they are available is a best practice in cybersecurity.

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://dod-cyberawareness.examzify.com

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

SAMPLE