US NAVY CYBER AWARENESS CHALLENGE 2026 PRACTICE TEST (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://usnavycyberawarenesschallenge2025.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. **How many social engineering indicators are present in the "E-mail Storage Quota Exceeded" notice?**

   A. 0

   B. 1

   C. 2

   D. 3+

2. **What action is Tessa prohibited from taking with payroll data while working remotely?**

   A. Using her home computer to print the data while working remotely

   B. Storing it in her locked desk drawer after working hours

   C. Securely e-mailing it to a colleague who needs to provide missing data

   D. Encrypting it

3. **Which statement about spillage is accurate?**

   A. It occurs when authorization to transfer information is granted and then later revoked.

   B. It refers specifically to classified information that becomes publicly available.

   C. It describes information that is "spilled" to either a lower or higher protection level.

   D. It can be either inadvertent or intentional.

4. **What is a strong password?**

   A. A password that is easily memorable

   B. A password that includes only letters

   C. A password that is at least 12 characters long with mixed characters

   D. A password that consists of the user's birthday

5. **What should you do after using a public computer?**

   A. Leave the computer logged in for the next user

   B. Only clear the history of visited websites

   C. Log out of accounts and clear the browsing data

   D. Download files for offline use

SAMPLE

6. What action should be taken upon receiving an unexpected package at work?

A. Open the package carefully

B. Ignore it and continue working

C. Report it to security personnel

D. Deliver it to the mailroom

7. What must you do when using an unclassified laptop in a collateral classified environment?

A. Use a wireless headset

B. Disable the embedded camera, microphone, and Wi-Fi

C. Use government-issued wired peripherals

8. What is a recommended practice for creating strong passwords?

A. Using personal information such as birthdays

B. Using a combination of letters, numbers, and special characters

C. Using the same password across multiple sites

D. Using simple words that are easy to remember

9. Why are software licenses important?

A. They allow unlimited use of software

B. They ensure compliance with legal requirements and protect against unauthorized software use

C. They are required only for commercial software

D. They guarantee the software will not contain bugs

10. What should Bob's colleagues do in response to his actions?

A. Confront Bob

B. Report Bob

C. Avoid Bob

D. Ignore Bob

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. How many social engineering indicators are present in the "E-mail Storage Quota Exceeded" notice?

A. 0

B. 1

C. 2

D. 3+

The presence of social engineering indicators in the "E-mail Storage Quota Exceeded" notice can be attributed to various tactics commonly used by cybercriminals to deceive individuals into divulging sensitive information or taking specific actions that may compromise their security. When evaluating such notices, one can identify indicators such as urgency, a request for personal information, unclear or unusual sender addresses, and prompts to click on links or provide login credentials. These tactics are often designed to exploit individuals' fears of losing access to their accounts or missing important communications. This particular notice may exhibit several of these red flags, suggesting a sophisticated approach to manipulating recipients. By identifying three or more indicators—such as a sense of urgency about the quota being exceeded, a request for immediate action, and an unfamiliar sender—one can conclude that the notice embodies multiple characteristics typical of social engineering attempts, justifying the answer of three or more indicators. Recognizing such signs is crucial for maintaining cybersecurity awareness and preventing potential fraud or data breaches.

2. What action is Tessa prohibited from taking with payroll data while working remotely?

A. Using her home computer to print the data while working remotely

B. Storing it in her locked desk drawer after working hours

C. Securely e-mailing it to a colleague who needs to provide missing data

D. Encrypting it

Tessa is prohibited from using her home computer to print payroll data while working remotely due to security concerns and the potential for data breaches. Printing sensitive information, especially payroll data, on devices that are not secured or controlled by the organization poses a significant risk. Home computers may not have the same level of security as work computers, making them vulnerable to unauthorized access and cyber threats. Additionally, unmonitored prints can lead to exposure where documents might be left unattended, seen by unauthorized individuals, or disposed of improperly. Maintaining the confidentiality and integrity of payroll data is critical to safeguarding personal information and overall data security, which is why organizations enforce strict policies around dealing with sensitive information remotely. The other options involve actions that either align with best practices for data security (like encrypting or using secure methods of communication) or do not expose the data to risk, like storing it securely when not in use. Thus, using a home computer to print sensitive payroll data is particularly problematic.

SAMPLE

3. Which statement about spillage is accurate?

A. It occurs when authorization to transfer information is granted and then later revoked.

B. It refers specifically to classified information that becomes publicly available.

C. It describes information that is "spilled" to either a lower or higher protection level.

D. It can be either inadvertent or intentional.

The statement that accurately describes spillage is that it can be either inadvertent or intentional. Spillage refers to a situation where information, particularly classified information, is exposed or transferred improperly to an environment where it should not be, such as a lower classification level or to unauthorized personnel. Inadvertent spillage typically occurs due to mistakes, such as sending an email to the wrong recipient or improperly handling classified materials. Intentional spillage, on the other hand, may involve a deliberate act to disseminate classified information without proper authorization. Understanding that spillage can occur in both volitional and non-volitional circumstances highlights the importance of strict adherence to security protocols and guidelines in protecting sensitive information.

4. What is a strong password?

A. A password that is easily memorable

B. A password that includes only letters

C. A password that is at least 12 characters long with mixed characters

D. A password that consists of the user's birthday

A strong password is characterized by its complexity and length, making it significantly more difficult for unauthorized users to guess or brute-force. Specifically, a password that is at least 12 characters long and includes a mixture of upper and lower case letters, numbers, and special characters is generally considered strong. This combination enhances security because longer passwords with varied character types exponentially increase the number of possible combinations, thereby making it harder for attackers to crack the password. In contrast, passwords that are easily memorable or based only on letters can often be simpler and more predictable, reducing their effectiveness as security measures. Similarly, a password that consists solely of a user's birthday is weak because such personal information can frequently be obtained or guessed by potential attackers. Therefore, including a variety of characters and increasing the password's length are key factors in creating a robust password that can better safeguard sensitive information.

5. What should you do after using a public computer?

A. Leave the computer logged in for the next user

B. Only clear the history of visited websites

C. Log out of accounts and clear the browsing data

D. Download files for offline use

Using a public computer, such as one in a library or internet café, poses unique security risks. Therefore, it is crucial to take specific steps after using such a device to protect your personal information and accounts. Logging out of all accounts and clearing the browsing data ensures that no one else who uses the computer afterward can access your personal email, social media, banking information, or any files you may have accessed. When you log out, you terminate your session and make sure that your credentials aren't left vulnerable. Additionally, clearing the browsing data, which includes cookies, cached files, and browsing history, prevents subsequent users from being able to retrieve any remnants of your session, further securing your information. This process serves as a safeguard against identity theft and protects your sensitive data from being easily accessed by others. Taking these actions creates a more secure environment, ensuring that your personal information is not accidentally exposed.

SAMPLE

6. What action should be taken upon receiving an unexpected package at work?

A. Open the package carefully

B. Ignore it and continue working

C. Report it to security personnel

D. Deliver it to the mailroom

When you receive an unexpected package at work, it is crucial to report it to security personnel. This action is important for several reasons. First, unexpected packages can pose security risks, such as containing harmful substances or being part of a more extensive security breach. By reporting the package, you allow trained security personnel to assess the situation appropriately and ensure the safety of everyone in the workplace. Additionally, security personnel have protocols in place for handling suspicious items. They can investigate further, determine if the package is safe, and take necessary actions based on their assessments. This response protects not only you but also your colleagues and the overall integrity of the workspace. Opening the package yourself could expose you to potential hazards, while ignoring it could allow a potential threat to persist. Delivering it to the mailroom might not be appropriate, as they may not have the necessary training or protocols to handle unexpected or suspicious packages efficiently. Thus, reporting the situation to security is the most responsible and safety-focused action to take.

7. What must you do when using an unclassified laptop in a collateral classified environment?

A. Use a wireless headset

B. Disable the embedded camera, microphone, and Wi-Fi

C. Use government-issued wired peripherals

When using an unclassified laptop in a collateral classified environment, disabling the embedded camera, microphone, and Wi-Fi is essential to maintaining security and safeguarding sensitive information. Unclassified devices can inadvertently compromise classified information through various channels, especially if they have active transmission capabilities such as Wi-Fi or listening capabilities from microphones and cameras. By disabling these features, you reduce the risk of unintentional data leakage or unauthorized access. This is a critical practice aligned with cybersecurity protocols that emphasize minimizing vulnerability when handling sensitive information in classified settings. The goal is to create a controlled environment where unclassified devices do not have the potential to interact with or gather classified data. Using wireless headsets or government-issued wired peripherals could pose additional risks, depending on their connection and functionality in relation to classified systems. Thus, the focus on disabling the built-in features of the laptop is a primary measure to ensure operational security within a classified environment.

SAMPLE

8. What is a recommended practice for creating strong passwords?

A. Using personal information such as birthdays

B. Using a combination of letters, numbers, and special characters

C. Using the same password across multiple sites

D. Using simple words that are easy to remember

Using a combination of letters, numbers, and special characters is a recommended practice for creating strong passwords because it significantly increases the complexity and unpredictability of the password. This approach makes it much harder for malicious actors to guess or crack the password using brute-force methods or dictionary attacks. A strong password that incorporates a diverse set of characters reduces the likelihood of unauthorized access to sensitive information, as it is less vulnerable to common password attacks. In contrast, relying on personal information, such as birthdays, or using simple words that are easy to remember can compromise security, as these types of passwords are often predictable and can be easily guessed by attackers who might know or research personal details. Furthermore, using the same password across multiple sites creates a security risk because if one account is compromised, all accounts with the same password become vulnerable. This underscores the importance of creating unique, complex passwords for each account to enhance overall cybersecurity.

9. Why are software licenses important?

A. They allow unlimited use of software

B. They ensure compliance with legal requirements and protect against unauthorized software use

C. They are required only for commercial software

D. They guarantee the software will not contain bugs

Software licenses are crucial because they establish the legal framework for the use of software. They define the rights and responsibilities of both the software developer and the user, ensuring that users have permission to use the software under specific terms and conditions. This compliance with legal requirements helps protect intellectual property rights and ensures that software is not used inappropriately or without proper authorization. By adhering to the terms of the license, organizations can mitigate the risk of legal repercussions that can arise from unauthorized software use, such as fines or other penalties. This understanding also reinforces the importance of respecting software ownership and the ethical considerations surrounding software usage, which are key tenets of cybersecurity awareness.

10. What should Bob's colleagues do in response to his actions?

A. Confront Bob

B. Report Bob

C. Avoid Bob

D. Ignore Bob

Reporting Bob is the appropriate action for his colleagues to take in response to his actions, especially if those actions pose a risk to cybersecurity or violate policy. When colleagues notice concerning behavior—such as mishandling sensitive data, engaging in unauthorized use of company resources, or any action that undermines security protocols—it is crucial that they report it to the designated authorities, such as a supervisor or the security team. This ensures that proper investigations can be conducted, and necessary measures can be taken to mitigate any potential threats. Addressing such situations through reporting not only helps in maintaining the integrity of the command and protecting sensitive information but also contributes to a culture of accountability and vigilance in cybersecurity practices. Reporting is formal, sets an example for accountability, and may lead to corrective actions that ensure the security of the entire team or organization.

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://usnavycyberawarenesschallenge2025.examzify.com

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

SAMPLE