US Navy Cyber Awareness Challenge 2026 Practice Test (Sample)

Study Guide

BY EXAMZIFY

Everything you need from our exam experts!

This is a sample study guide. To access the full version with hundreds of questions,

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

Table of Contents

Copyright 1

Table of Contents 2

Introduction 3

How to Use This Guide 4

Questions 6

Answers 9

Explanations 11

Next Steps 17

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.

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. Don't worry about getting everything right, 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, and take breaks to retain information better.

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.

7. Use Other Tools

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!

Questions

1. **What type of training can help employees identify phishing attempts?**
   - **A. Technical skills training**
   - **B. Cybersecurity awareness training**
   - **C. Leadership training**
   - **D. Customer relationship management training**

2. **What should Bob's colleagues do in response to his actions?**
   - **A. Confront Bob**
   - **B. Report Bob**
   - **C. Avoid Bob**
   - **D. Ignore Bob**

3. **Which statement is true regarding Controlled Unclassified Information (CUI)?**
   - **A. It is marked as CUI at the discretion of the information owner.**
   - **B. It poses no risk to Government missions or interests.**
   - **C. It belongs to a defined category established in the DoD CUI Registry.**
   - **D. It is another term for any Unclassified information that has not been cleared for public release.**

4. **How can you filter out fake news on the internet?**
   - **A. Trust the headlines that seem extreme or shocking**
   - **B. Cross-check information with reliable sources**
   - **C. Share immediately if it aligns with your beliefs**
   - **D. Ignore fact-checks and focus on popularity**

5. **What action is best if an unknown caller is asking for sensitive information?**
   - **A. Politely decline and hang up**
   - **B. Gather information and call back**
   - **C. Provide the information to them**
   - **D. Report the call to authorities**

6. Which of the following is a potential insider threat indicator?

A. Authorized handling of classified information.

B. Work-related foreign travel.

C. Financial windfall from an inheritance.

D. Death of a spouse.

7. What is an allowed use of government furnished equipment (GFE)?

A. Conducting transactions on your side business

B. Viewing family photos from your shared DropBox

C. Lending it to your spouse to watch a movie

D. E-mailing your supervisor

8. Which of the following should you do to protect against malware on personal devices?

A. Install both antivirus and antispyware software

B. Rely solely on built-in operating system defenses

C. Turn off security features when not in use

D. Only use devices that have never been connected to the internet

9. What indicates a potential insider threat?

A. Excessive overtime

B. Frequent travels

C. Unusual spending habits

D. Close connections to coworkers

10. What is a primary role of cybersecurity regarding national security?

A. To enhance military capabilities

B. To protect critical infrastructure and sensitive information

C. To manage human resources in defense

D. To develop new communication technologies

Answers

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

Explanations

1. What type of training can help employees identify phishing attempts?

A. Technical skills training

B. Cybersecurity awareness training

C. Leadership training

D. Customer relationship management training

Cybersecurity awareness training is essential for helping employees identify phishing attempts. This type of training specifically focuses on educating individuals about various cyber threats, including phishing, which is a common tactic used by cybercriminals to deceive users into providing sensitive information such as passwords or financial details. Through targeted training, employees learn to recognize the signs of phishing, such as suspicious email addresses, unexpected attachments, and urgent requests for personal information. They also receive guidance on best practices for assessing the legitimacy of communications, thereby empowering them to handle potential threats more effectively. This specialized training can significantly reduce the chances of successful phishing attempts by enhancing the employees' ability to spot these attacks and respond appropriately, which is a crucial aspect of maintaining organizational cybersecurity.

2. 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.

3. Which statement is true regarding Controlled Unclassified Information (CUI)?

A. It is marked as CUI at the discretion of the information owner.

B. It poses no risk to Government missions or interests.

C. It belongs to a defined category established in the DoD CUI Registry.

D. It is another term for any Unclassified information that has not been cleared for public release.

Controlled Unclassified Information (CUI) is indeed categorized under specific guidelines set by the Department of Defense (DoD) CUI Registry. This classification framework is designed to standardize how unclassified information that requires safeguarding or dissemination controls is managed across federal agencies. The CUI designation helps ensure that sensitive but unclassified information is properly protected and handled, fostering uniformity in procedures and compliance. The purpose of this structured approach is to ensure that all personnel understand the requirements around handling such information, which can include anything from sensitive research data to operational details that, while unclassified, still require protection to prevent unauthorized access or misuse. Thus, C, identifying CUI as belonging to a defined category established in the DoD CUI Registry, accurately conveys the importance of management and protection that is inherent to CUI. This correct understanding is crucial for maintaining the integrity and security of unclassified information, particularly within military and defense contexts.

4. How can you filter out fake news on the internet?

A. Trust the headlines that seem extreme or shocking

B. Cross-check information with reliable sources

C. Share immediately if it aligns with your beliefs

D. Ignore fact-checks and focus on popularity

Filtering out fake news on the internet is crucial for maintaining an informed perspective. Cross-checking information with reliable sources is an effective method because it ensures that the information you are consuming is validated by trustworthy entities. Reliable sources, such as established news organizations, academic publications, or expert opinions, have protocols in place for fact-checking and verifying information before sharing it with the public. This process minimizes the risk of falling prey to misinformation, which can spread quickly across social media and other platforms. By contrasting claims with multiple authoritative sources, you can gauge the accuracy of the information and identify any discrepancies or biases. This practice encourages critical thinking and responsible consumption of news. In the age of information overload, taking the time to verify facts can significantly enhance your understanding and prevent the spread of false narratives.

5. What action is best if an unknown caller is asking for sensitive information?

A. Politely decline and hang up

B. Gather information and call back

C. Provide the information to them

D. Report the call to authorities

When dealing with an unknown caller requesting sensitive information, the best action is to politely decline and hang up. This response is critical as it helps protect your personal and sensitive data from potential phishing attacks or social engineering tactics. Unknown callers may pose as legitimate representatives from organizations, manipulative officials, or even trusted acquaintances to extract confidential information. By choosing to end the call without providing any details, you eliminate the risk of inadvertently sharing sensitive data that could lead to identity theft or unauthorized access to secure information. It is also advisable to verify the identity of any callers through official channels rather than engaging in conversation with them. This practice minimizes the opportunity for fraud and ensures that personal information remains secure.

6. Which of the following is a potential insider threat indicator?

A. Authorized handling of classified information.

B. Work-related foreign travel.

C. Financial windfall from an inheritance.

D. Death of a spouse.

The selection indicating "death of a spouse" as a potential insider threat indicator is grounded in the understanding that significant personal life changes can influence an individual's behavior and decision-making. Such a profound event can lead to emotional distress, changes in financial status, or even a susceptibility to manipulation by adversaries. These factors may heighten the risk of an individual engaging in reckless or harmful activities, which could include the unauthorized disclosure of sensitive information. Monitoring personal circumstances, including loss and grief, is essential for identifying individuals who may be experiencing a crisis that could lead to insider threats. Organizations need to ensure that they have measures in place to support employees during such challenging times, as well as to maintain vigilance regarding any changes in behavior that may emerge following significant life events.

7. What is an allowed use of government furnished equipment (GFE)?

A. Conducting transactions on your side business

B. Viewing family photos from your shared DropBox

C. Lending it to your spouse to watch a movie

D. E-mailing your supervisor

The permitted use of government-furnished equipment (GFE) includes activities that support official duties and responsibilities. Communicating with your supervisor via email falls within this category because it is a part of performing your job responsibilities. Proper use of GFE requires that it be utilized for tasks related to government work, which includes correspondence regarding assignments, reporting, collaboration, and general work-related communication. Activities that divert from your official role, such as conducting personal business, sharing personal files, or loaning equipment to others, do not align with acceptable use policies. Therefore, using GFE to email your supervisor is appropriate and maintains the integrity of government resources.

8. Which of the following should you do to protect against malware on personal devices?

A. Install both antivirus and antispyware software

B. Rely solely on built-in operating system defenses

C. Turn off security features when not in use

D. Only use devices that have never been connected to the internet

Installing both antivirus and antispyware software is a crucial step in protecting personal devices against malware. Antivirus software is designed to detect, prevent, and remove viruses and other malicious software, while antispyware specifically focuses on protecting against spyware—programs that can gather personal information from your device without your knowledge. By utilizing both types of software, you create a more robust defense system to address a wider range of potential threats. Relying solely on built-in operating system defenses may leave your system vulnerable, as these features can sometimes be inadequate against sophisticated malware threats. Turning off security features when not in use significantly increases the risk of infection, as it can leave your device exposed to attacks when you are unaware or not actively engaged in safe browsing behaviors. Lastly, only using devices that have never been connected to the internet is impractical for most users, as it limits access to essential resources and communication. These alternatives do not provide the same comprehensive protection that installing antivirus and antispyware software together offers.

9. What indicates a potential insider threat?

A. Excessive overtime

B. Frequent travels

C. Unusual spending habits

D. Close connections to coworkers

Excessive overtime can often signal a potential insider threat for several reasons. When an employee consistently works far beyond normal hours, it may suggest that they are engaged in activities that do not align with regular job responsibilities or protocols. This behavior could indicate that the individual is attempting to access sensitive information or perform unauthorized actions during times when fewer coworkers are present and oversight is minimal. Additionally, excessive overtime may point to stress or dissatisfaction in the workplace, which can sometimes lead to malicious behavior. An employee who feels undervalued or threatened might resort to threatening actions such as data theft or sabotage. Monitoring work hours can provide valuable insights into employee behavior and help identify individuals who may pose a risk to organizational security. In contrast, frequent travels, unusual spending habits, and close connections to coworkers might have various benign explanations and may not necessarily indicate a risk. Thus, while these factors can potentially raise concerns, excessive overtime more directly relates to behaviors that could signal deeper issues warranting closer attention.

10. What is a primary role of cybersecurity regarding national security?

A. To enhance military capabilities

B. To protect critical infrastructure and sensitive information

C. To manage human resources in defense

D. To develop new communication technologies

The role of cybersecurity in national security is fundamentally about protecting critical infrastructure and sensitive information. This encompasses safeguarding systems, networks, and data that are essential to the functioning of government and private sector entities that support national security. Such protection is vital not only to prevent unauthorized access and cyberattacks but also to ensure the continuity of critical services that the nation relies on, such as energy grids, financial institutions, and communication networks. By securing sensitive information, cybersecurity helps maintain the integrity and confidentiality of data related to national defense, intelligence operations, and other government activities. This proactive approach reduces vulnerabilities and helps mitigate the risks of cyber threats, which, if successful, could lead to significant disruptions, economic loss, or even compromise national security itself. In contrast, while enhancing military capabilities, managing human resources, and developing new communication technologies are important aspects of defense, they do not directly address the primary function of cybersecurity, which specifically focuses on protecting crucial information and systems from cyber threats.

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!