US Navy Cyber Awareness Challenge 2026 Practice Test (Sample)

Study Guide

BY EXAMZIFY

Everything you need from our exam experts!

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

Table of Contents

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. 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!

Questions

1. In a SCIF, if a conversation is held after verifying no one was nearby, does this behavior represent a security concern?

A. Yes

B. No

2. Is it acceptable to use home computers for official government work?

A. Yes, always

B. Yes, if protocols are followed

C. No, never

D. Only for urgent tasks

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

A. Confront Bob

B. Report Bob

C. Avoid Bob

D. Ignore Bob

4. What is an effective way to secure sensitive data on your devices?

A. Regularly share your passwords with trusted individuals

B. Use strong, unique passwords for each account

C. Store all passwords in a plain text document

D. Change passwords only when you suspect a breach

5. How can malicious code cause damage?

A. Corrupt files.

B. Encrypting or erasing your hard drive.

C. Allowing hackers access.

D. All of these.

6. Why is physical security a critical aspect of cybersecurity?

A. To enhance internet speed

B. To prevent unauthorized access to devices and data centers

C. To facilitate remote work

D. To support employee training programs

7. **Which of the following is an appropriate use of a DoD Public Key Infrastructure (PKI) token?**

   A. Use a SIPRNet token for NIPRNet access as well.

   B. Only leave it in a system while actively using it for a PKI-required task.

   C. Use a NIPRNet token for SIPRNet access as well.

   D. Only use it on a publicly accessible computer with up-to-date antivirus software.

8. **What is a common sign of phishing attempts?**

   A. Personalized content

   B. Urgency or threats

   C. Clear sender information

   D. Professional formatting

9. **What action will keep DoD data the safest?**

   A. Change seats

   B. Leave the coffee shop

   C. Disable Wi-Fi

   D. Notify a supervisor

10. **What is a VPN and why is it used?**

   A. A Virtual Private Network for secure data transmission

   B. A tool for accelerating internet speed

   C. A type of malware detection software

   D. A backup solution for data storage

Answers

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

Explanations

1. In a SCIF, if a conversation is held after verifying no one was nearby, does this behavior represent a security concern?

A. Yes

B. No

The behavior of holding a conversation in a SCIF (Sensitive Compartmented Information Facility) after verifying that no one was nearby does not represent a security concern because the main purpose of a SCIF is to provide a controlled environment for discussing sensitive information securely. The act of verifying that no unauthorized personnel are present aligns with established security protocols meant to protect classified information.   In a SCIF, measures are in place to ensure that communications remain secure, and as long as personnel are vigilant about their surroundings and take the necessary steps to ensure confidentiality—such as confirming the area is clear—this conduct is acceptable. The key factor is maintaining awareness of the environment and ensuring that no one who should not have access is listening or could overhear the conversation. Therefore, as long as proper procedures are followed, this behavior is within the bounds of acceptable security practices in a SCIF.

2. Is it acceptable to use home computers for official government work?

A. Yes, always

B. Yes, if protocols are followed

C. No, never

D. Only for urgent tasks

Using home computers for official government work can be acceptable if specific protocols are followed. This is primarily because organizations often have guidelines and cybersecurity measures in place to mitigate risks associated with remote work. When using personal devices, it is essential to adhere to security policies established by the government or the respective agency, which may include using a virtual private network (VPN), utilizing encrypted connections, ensuring antivirus and antimalware software is up to date, and following strict data handling procedures. These protocols are designed to protect sensitive information and reduce the risk of data breaches. Failing to follow such guidelines can expose government data to threats, potentially compromising both national security and individual privacy. The importance of these protocols is reflected in the increasing focus on maintaining security in hybrid and remote work environments. Individuals must be adequately trained and informed about the procedures to follow when accessing government systems from personal devices. Hence, while using home computers is not universally acceptable, it can be appropriate under carefully controlled circumstances.

3. 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.

4. What is an effective way to secure sensitive data on your devices?

A. Regularly share your passwords with trusted individuals

B. Use strong, unique passwords for each account

C. Store all passwords in a plain text document

D. Change passwords only when you suspect a breach

Using strong, unique passwords for each account is essential for securing sensitive data on your devices. Strong passwords typically contain a combination of uppercase and lowercase letters, numbers, and special characters, which make them more difficult for unauthorized users to guess or crack. Additionally, having unique passwords for different accounts helps to prevent a single point of failure; if one account is compromised, other accounts remain secure. This practice is important because many data breaches occur when attackers gain access to a password and exploit it across multiple services. By ensuring that each password is distinct, the risk of widespread access to sensitive data is significantly reduced. On the other hand, sharing passwords with others, storing them in plain text, or changing them only when a breach is suspected compromises security and increases the risk of unauthorized access to sensitive information. Each of these practices can lead to vulnerabilities that jeopardize the safety of data.

5. How can malicious code cause damage?

A. Corrupt files.

B. Encrypting or erasing your hard drive.

C. Allowing hackers access.

D. All of these.

Malicious code can cause damage in multiple ways, and the correct choice encompasses all of these potential impacts. Corrupting files is one method through which malicious software can cause havoc, rendering important data unreadable or unusable, thereby compromising the integrity of the information. Another significant threat is the encryption or erasure of hard drives, where malicious code can lock users out of their own data or completely wipe it, leading to total loss of important files and information. Additionally, malicious software often creates backdoors or vulnerabilities that allow hackers to gain unauthorized access to systems, further putting data and security at risk. By acknowledging that all of these outcomes can occur, the correct answer reflects the broad spectrum of threats posed by malicious code in cybersecurity. Understanding these various mechanisms emphasizes the importance of proactive security measures and vigilance in recognizing and mitigating cyber threats.

6. Why is physical security a critical aspect of cybersecurity?

A. To enhance internet speed

B. To prevent unauthorized access to devices and data centers

C. To facilitate remote work

D. To support employee training programs

Physical security is a critical aspect of cybersecurity primarily because it helps prevent unauthorized access to devices and data centers. This is essential because many cyber threats can begin from physical breaches where an unauthorized individual gains access to an organization's hardware, networks, or sensitive information. By securing physical locations, organizations can protect sensitive equipment and data from theft, tampering, or sabotage. This includes implementing measures such as access control systems like keycards or biometric scans, surveillance cameras, security personnel, and clearly defined visitor protocols. This holistic approach ensures that even if systems are technically secure from digital attacks, they are also safeguarded from physical vulnerabilities that could compromise cybersecurity efforts. Ensuring strong physical security measures directly supports overall cybersecurity posture by reducing the risk of data breaches and maintaining the integrity of information systems.

7. Which of the following is an appropriate use of a DoD Public Key Infrastructure (PKI) token?

A. Use a SIPRNet token for NIPRNet access as well.

B. Only leave it in a system while actively using it for a PKI-required task.

C. Use a NIPRNet token for SIPRNet access as well.

D. Only use it on a publicly accessible computer with up-to-date antivirus software.

Using a PKI token only while actively engaged in a PKI-required task is appropriate because it minimizes the risk of unauthorized access and potential misuse of the token. PKI tokens are designed to authenticate and secure communications, and leaving them connected to a system when not in use can expose them to vulnerabilities, such as theft or exploitation. By ensuring that tokens are only utilized for designated tasks, users contribute to a more secure environment, aligning with best practices for cybersecurity within the Department of Defense. This approach emphasizes the importance of vigilance and careful management of sensitive security tools in the digital landscape.

8. What is a common sign of phishing attempts?

A. Personalized content

B. Urgency or threats

C. Clear sender information

D. Professional formatting

Urgency or threats are commonly used tactics in phishing attempts to manipulate individuals into reacting quickly without thinking critically. Phishing attacks often create a sense of panic or pressure, urging a recipient to take immediate action, such as clicking on a link or providing sensitive information. By invoking fear or a sense of urgency, attackers hope to distract users from their usual scrutiny of the communication. In contrast, personalized content, clear sender information, and professional formatting can sometimes make an email or message seem legitimate. However, these factors alone do not necessarily indicate a phishing attempt, as attackers have become increasingly sophisticated in their methods. They often employ personalized elements to make their attacks more convincing, and they may also mimic legitimate company branding to enhance the appearance of their communications.

9. What action will keep DoD data the safest?

A. Change seats

B. Leave the coffee shop

C. Disable Wi-Fi

D. Notify a supervisor

Leaving the coffee shop is a prudent action that can significantly increase the safety of DoD data. Public spaces like coffee shops are often breeding grounds for cyber threats, where unauthorized individuals can easily observe sensitive information being accessed on devices, particularly if those devices are connected to unsecured Wi-Fi networks. By physically removing oneself from such an environment, the risk of falling prey to shoulder surfing or eavesdropping by malicious actors is greatly diminished. In contrast, other actions such as changing seats or disabling Wi-Fi may provide only a temporary shield against potential threats. Changing seats might still leave a user vulnerable to prying eyes, while disabling Wi-Fi doesn't fully address the risk of someone accessing your data directly if a device is compromised. Notifying a supervisor, although important in certain contexts, does not provide immediate protection against data breaches or cyber threats that can occur in public settings. Thus, leaving the coffee shop stands out as the most effective measure for safeguarding DoD data in this scenario.

10. What is a VPN and why is it used?

A. A Virtual Private Network for secure data transmission

B. A tool for accelerating internet speed

C. A type of malware detection software

D. A backup solution for data storage

A Virtual Private Network (VPN) is a technology that creates a secure, encrypted connection over a less secure network, such as the Internet. This secure connection allows users to send and receive data while ensuring that their online activities remain private and protected from eavesdropping. The primary purpose of using a VPN is to enhance security and privacy for the user. By encrypting the data, a VPN protects sensitive information from being intercepted by malicious actors or unauthorized users. It also masks the user's IP address, which provides anonymity while browsing. This capability is especially important in situations where individuals are accessing sensitive information or using public Wi-Fi networks, which can be particularly vulnerable to cyber threats. Understanding this technology is crucial for maintaining cybersecurity standards and ensuring the protection of personal and organizational data when engaging with online networks.

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!