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

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. What does "data at rest" mean?

A. Data actively moving through networks

B. Data stored in a database or storage

C. Data being processed by applications

D. Data sent for backup purposes

2. What type of data could reasonably be expected to cause damage to national security?

A. Secret

B. Confidential

C. Controlled Unclassified Information (CUI)

D. Top Secret

3. What provides precise guidance regarding elements of information that can be classified?

A. Classification Management Tool

B. Local Security Official

C. Security Classification Guide

D. Classification Registry

4. How can you assess the security of a mobile device?

A. By checking for available apps in the app store

B. By ensuring the battery life is optimized

C. By checking for security updates and ensuring security features such as lock screen and encryption are enabled

D. By clearing all stored photos and videos

5. How can you verify the authenticity of a website?

A. Look for a busy site traffic indicator

B. Check for HTTPS in the URL and look for a padlock icon in the browser address bar

C. Ensure that the website has a large number of images

D. See if the site has been recommended by social media

6. When emailing a personnel roster, what should you include to ensure the information is protected?

A. Encrypt the PII.

B. Digitally sign the email.

C. Use your Government email account.

D. All of the above.

7. Why should removable media be handled with caution in government facilities?

A. They are more costly than traditional storage.

B. They are prone to physical damage.

C. They may transmit malicious software.

D. They offer limited storage capacity.

8. What is required to transport Sensitive Compartmented Information (SCI)?

A. You must be courier-briefed for SCI to transport it.

B. SCI does not require a coversheet in an open storage environment.

C. You may only transmit SCI via certified mail.

D. You must never print SCI.

9. How does cybersecurity impact the economy?

A. By creating employment in art and culture

B. By protecting businesses from data loss

C. By promoting international tourism

D. By reducing government spending

10. Which of the following uses of removable media is allowed?

A. Alex uses personally owned removable media on an Unclassified government laptop to transfer personal music files.

B. Nicky uses Unclassified government owned removable media to transfer work files to a personal laptop.

C. Cameron connects a personal phone to an Unclassified government laptop to charge.

D. Sam uses approved Government owned removable media to transfer files between government systems as authorized.

Answers

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

Explanations

1. What does "data at rest" mean?

A. Data actively moving through networks

B. Data stored in a database or storage

C. Data being processed by applications

D. Data sent for backup purposes

"Data at rest" refers specifically to data that is stored in a database, on a storage device, or in any other form of persistent storage. This includes information that is not actively moving between devices or being processed; rather, it is in a state of inactivity. The significance of understanding "data at rest" lies in the importance of securing this type of information, as it is often crucial to an organization's operations and could contain sensitive or confidential information. Protecting data at rest involves implementing security measures such as encryption, access controls, and physical security to ensure that the data remains secure against unauthorized access. While data actively moving through networks or being processed may involve different security concerns, they do not fall under the definition of "data at rest." Additionally, data sent for backup purposes is related to data protection strategies but, again, does not specifically define the state of the data when it is on storage media.

2. What type of data could reasonably be expected to cause damage to national security?

A. Secret

B. Confidential

C. Controlled Unclassified Information (CUI)

D. Top Secret

The type of data that could reasonably be expected to cause damage to national security when improperly disclosed is classified as "Confidential." This classification is specifically designed for information that, if released, could cause damage to national security but not as severe as information classified as "Secret" or "Top Secret." The "Confidential" designation indicates that the information is sensitive and requires certain safeguards to prevent unauthorized access. It reflects a balance between the level of sensitivity and the potential consequences of leaking the data. While "Top Secret" data carries the most critical risk of causing exceptionally grave damage to national security, "Confidential" is more accessible while still being protective of national interests. In this context, "Secret" and "Top Secret" represent higher classifications with more severe implications for national security than "Confidential." "Controlled Unclassified Information" (CUI), while also sensitive, does not typically pose a risk significant enough to cause damage to national security in the same way that "Confidential" information does. Thus, "Confidential" is the appropriate classification when considering data that could lead to a reasonable expectation of causing damage to national security.

3. What provides precise guidance regarding elements of information that can be classified?

A. Classification Management Tool

B. Local Security Official

C. Security Classification Guide

D. Classification Registry

The correct answer is the Security Classification Guide. This guide serves as an authoritative document that outlines the specific categories and criteria under which information can be classified. It provides the necessary details about the classification levels – such as Confidential, Secret, or Top Secret – and elaborates on what types of information may fall under these classifications based on national security interests. The Security Classification Guide is crucial for ensuring that personnel understand what information needs protection and the rationale behind those requirements. By following the guide, individuals can consistently and accurately classify information, thereby supporting government regulations and safeguarding national security. The other options may have roles in the classification process but do not provide the comprehensive and detailed guidance that a Security Classification Guide does when it comes to determining what elements can be classified. For instance, while tools and officials might assist in managing or overseeing classification efforts, they lack the specificity of a guide that explicitly delineates classification criteria.

4. How can you assess the security of a mobile device?

A. By checking for available apps in the app store

B. By ensuring the battery life is optimized

C. By checking for security updates and ensuring security features such as lock screen and encryption are enabled

D. By clearing all stored photos and videos

Assessing the security of a mobile device is fundamentally about evaluating its defenses against unauthorized access and potential threats. One of the most effective ways to ensure this security is by checking for security updates and verifying that essential security features, such as a lock screen and encryption, are enabled. Security updates are critical because they address vulnerabilities that could be exploited by attackers. Manufacturers regularly release updates to patch these vulnerabilities, making it important to install the latest versions of the operating system and software. Additionally, enabling a lock screen is a primary security measure that helps prevent unauthorized physical access to the device. It acts as a barrier for anyone trying to use the device who does not possess the correct PIN, password, or biometric identifiers. Encryption further enhances security by ensuring that the data stored on the device is encoded and requires a decryption key to access. This means that even if someone gains physical access to the device, the data remains safe unless they can also bypass the encryption. In contrast, checking for available apps in the app store, optimizing battery life, or clearing stored photos and videos do not directly relate to the core security features of the device. While these actions may be part of overall device management and maintenance, they do not specifically assess or enhance the security posture of the

5. How can you verify the authenticity of a website?

A. Look for a busy site traffic indicator

B. Check for HTTPS in the URL and look for a padlock icon in the browser address bar

C. Ensure that the website has a large number of images

D. See if the site has been recommended by social media

Verifying the authenticity of a website is crucial for ensuring safe internet browsing and protecting sensitive information. The most reliable way to confirm that a website is legitimate is to check for HTTPS in the URL along with the presence of a padlock icon in the browser's address bar. When a website uses HTTPS (Hypertext Transfer Protocol Secure), it indicates that the data transmitted between your browser and the website is encrypted, adding a layer of security. The padlock icon serves as a visual cue that the connection is secure. This verification process is a widely accepted method to determine the authenticity of a site, as it helps protect against potential threats such as phishing and man-in-the-middle attacks. In contrast, other choices may not provide definitive indicators of a website's authenticity. For example, busy site traffic indicators, the number of images, and recommendations on social media do not necessarily correlate with a website's legitimacy or security. Thus, focusing on HTTPS and the padlock icon is the most effective way to ensure that you're dealing with a credible website.

6. When emailing a personnel roster, what should you include to ensure the information is protected?

A. Encrypt the PII.

B. Digitally sign the email.

C. Use your Government email account.

D. All of the above.

To ensure that a personnel roster containing sensitive information remains protected, it is essential to utilize a combination of security measures that include encryption, digital signatures, and the use of a government email account. Each of these components plays a crucial role in safeguarding sensitive data. Encrypting Personally Identifiable Information (PII) ensures that even if the email is intercepted, the data remains unreadable to unauthorized users. This adds a robust layer of security that is vital when handling any personal information about personnel. Digitally signing the email provides authentication for both the sender and the content. This process verifies that the email genuinely comes from the identified sender and that the content has not been altered in transit, which is key in maintaining the integrity and trustworthiness of the communication. Using a government email account is fundamental because these accounts are typically equipped with enhanced security features and are subject to stricter controls compared to personal email accounts. This helps protect sensitive information within a controlled and secure environment. By employing all these measures simultaneously, the likelihood of unauthorized access or data breaches is significantly reduced, thus ensuring that the information contained in the personnel roster is adequately protected.

7. Why should removable media be handled with caution in government facilities?

A. They are more costly than traditional storage.

B. They are prone to physical damage.

C. They may transmit malicious software.

D. They offer limited storage capacity.

Removable media should be handled with caution in government facilities because they may transmit malicious software. This transmission can occur when removable media, such as USB drives or external hard drives, are connected to government computers or networks. Malware can easily be stored on these devices, ensuring a rapid and undetected spread of harmful software once the device is plugged into a system. Given the sensitive nature of government data, the introduction of malicious software can lead to significant security breaches, loss of data integrity, or unauthorized access to confidential information. In a cybersecurity context, the risk associated with removable media makes it imperative to implement policies controlling their use, including scanning devices for malware before connection and restricting access to necessary personnel. This precaution helps mitigate the potential for cyber threats emanating from external sources.

8. What is required to transport Sensitive Compartmented Information (SCI)?

A. You must be courier-briefed for SCI to transport it.

B. SCI does not require a coversheet in an open storage environment.

C. You may only transmit SCI via certified mail.

D. You must never print SCI.

To transport Sensitive Compartmented Information (SCI), it is essential to be courier-briefed specifically for SCI. This briefing ensures that individuals are aware of the secure handling, transportation protocols, and the necessity of protecting sensitive information from unauthorized access. Being courier-briefed emphasizes the importance of understanding the risks associated with transporting classified material, including adhering to specific procedures and security measures essential for safeguarding SCI from potential threats. In contrast, the other options outline incorrect information or inadequate practices regarding the handling of SCI. For example, not requiring a coversheet in an open storage environment contradicts established protocols that emphasize the need for protective measures even in secure locations. The notion that SCI can only be transmitted via certified mail is overly restrictive, as various approved communication methods exist for transmission depending on the context and security classification protocols. Lastly, while it's advisable to avoid printing SCI to prevent unauthorized access, there may be legitimate cases where dissemination in printed form occurs under strict controls, meaning this statement does not universally apply. Therefore, being courier-briefed follows established security guidelines and is necessary for anyone tasked with the responsibility of transporting SCI.

9. How does cybersecurity impact the economy?

A. By creating employment in art and culture

B. By protecting businesses from data loss

C. By promoting international tourism

D. By reducing government spending

Cybersecurity plays a crucial role in protecting businesses from data loss, which directly impacts the economy. When businesses implement strong cybersecurity measures, they safeguard sensitive information, intellectual property, and customer data. This protection minimizes the risk of data breaches, which can lead to significant financial losses, loss of customer trust, and potential legal ramifications. When businesses experience data loss or are victims of cyberattacks, the economic impact can be considerable. Not only do the affected companies often face costly recovery processes, but they may also experience long-term effects such as reputational damage and decreased customer loyalty. By investing in cybersecurity, businesses can ensure operational continuity, protect their assets, and ultimately contribute to a more stable economic environment. This security fosters innovation and growth, as companies can focus on their core activities without the constant threat of cyber-related disruptions.

10. Which of the following uses of removable media is allowed?

A. Alex uses personally owned removable media on an Unclassified government laptop to transfer personal music files.

B. Nicky uses Unclassified government owned removable media to transfer work files to a personal laptop.

C. Cameron connects a personal phone to an Unclassified government laptop to charge.

D. Sam uses approved Government owned removable media to transfer files between government systems as authorized.

The use of approved Government-owned removable media to transfer files between government systems as authorized is aligned with the policies and guidelines governing cybersecurity and data handling within the Navy and broader government context. This practice ensures that the removable media is managed, monitored, and secured according to established protocols, minimizing the risk of data breaches and unauthorized access. Authorized uses of government-supplied removable media are typically subjected to security controls, such as encryption and access logging, ensuring that the files being transferred are protected and that the media itself is not compromised. Adhering to these guidelines helps maintain the integrity and confidentiality of sensitive or classified information. In contrast, other scenarios present situations that typically violate cybersecurity best practices. Using personal devices or media for transferring files related to government work exposes sensitive information to potential risks. Personal devices and media may not have the necessary security measures in place, making them vulnerable to malware or unauthorized access. Thus, option D stands out as compliant with the policies governing acceptable IT practices within a government context.

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!