NLC Digital Citizenship Practice Exam (Sample)

Study Guide

BY EXAMZIFY

Everything you need from our exam experts!

Sample study guide. Visit https://nlcdigitalcitizenship.examzify.com

Copyright © 2025 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 from reliable sources accurate, complete, and timely information about this product.

SAMPLE

Questions

SAMPLE

1. **Which term refers to a secret word or phrase used together with a username for authentication?**

   A. Token

   B. Password

   C. Username

   D. PIN

2. **Which security model operates on the principle that no one can be trusted by default?**

   A. Zero Trust

   B. Firewall Protection

   C. Public Key Infrastructure

   D. Network Segmentation

3. **What describes the SaaS (Software as a Service) model?**

   A. Hosting applications locally on a device

   B. Accessing applications over the internet

   C. Providing virtualized computing resources

   D. Developing applications with managed platforms

4. **Which type of malware is disguised as legitimate software to trick users?**

   A. Worm

   B. Trojan

   C. Virus

   D. Botnet

5. **What are trusted digital sources?**

   A. Content providers with a low user rating.

   B. Websites known for accurate and reliable information.

   C. Any site delivering free content.

   D. Niche blogs with personal opinions.

SAMPLE

6. What role does digital communication play in citizenship?

- **A. It restricts opinions to private messages only.**
- **B. It allows individuals to participate in discussions and collaborate online.**
- **C. It limits engagement to texting and private chats.**
- **D. It discourages sharing personal opinions in public.**

7. Which of the following describes digital responsibility?

- **A. The act of ignoring harmful online content.**
- **B. Understanding the ethical implications of online actions.**
- **C. Withholding personal information at all times.**
- **D. The requirement to share all online activities.**

8. What is the main feature of spyware?

- **A. Locking data for ransom**
- **B. Connecting different systems**
- **C. Monitoring user activities**
- **D. Managing system resources**

9. What does the process of compiling involve?

- **A. Translating code line by line**
- **B. Running code instructions**
- **C. Translating entire source code into machine code**
- **D. Fixing errors in code**

10. What is the term for switching between different processes in a computer system, typically managed by the operating system?

- **A. Execution**
- **B. Thread Management**
- **C. Process Switch**
- **D. Task Scheduling**

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. Which term refers to a secret word or phrase used together with a username for authentication?

A. Token

B. Password

C. Username

D. PIN

The term that refers to a secret word or phrase used together with a username for authentication is "password." Passwords are an essential part of account security, ensuring that only authorized users can access a specific account or service. When a user logs in, they typically provide their username, which identifies their account, followed by the corresponding password, which acts as a secret key that verifies their identity. Passwords are designed to be confidential and should be created using a mix of letters, numbers, and special characters to enhance security. The careful combination of a username and password helps prevent unauthorized access. This practice is fundamental to maintaining digital security, as it helps protect personal information and sensitive data from being compromised. In contrast, terms like token, username, and PIN serve different functions in the realm of authentication. A token may refer to a temporary digital key or code that grants access, while a username identifies the user. A PIN (personal identification number) is typically a numeric code used for authentication, often in conjunction with a card or device, but it operates differently than a password, which is often alphanumeric. Thus, the nature and function of a password distinctly define it as the correct answer in this context.

2. Which security model operates on the principle that no one can be trusted by default?

A. Zero Trust

B. Firewall Protection

C. Public Key Infrastructure

D. Network Segmentation

The security model that operates on the principle that no one can be trusted by default is the Zero Trust model. This approach emphasizes that both internal and external network requests must be verified, regardless of their origin. In a Zero Trust framework, every user and device is authenticated, authorized, and continuously evaluated for trustworthiness before granting access to any network resources. This model is especially relevant in today's digital environments, where threats can come from anyone, even those inside the organization. Instead of assuming that users within a network perimeter are safe, Zero Trust suggests a proactive stance towards security, acknowledging that breaches can happen at any moment. By implementing strict access controls and not trusting any user or device by default, organizations can significantly minimize their attack surface and better protect sensitive data. The other choices represent different security concepts that do not inherently abide by the Zero Trust principle. For example, firewall protection typically relies on predefined rules to allow or deny traffic, which can assume certain levels of trust within a network. Public Key Infrastructure helps in managing digital keys for encryption and is based on trust relationships among entities, while network segmentation involves dividing a network into segments to improve performance and security but does not encapsulate the trust model inherent in Zero Trust.

SAMPLE

3. What describes the SaaS (Software as a Service) model?

A. Hosting applications locally on a device

B. Accessing applications over the internet

C. Providing virtualized computing resources

D. Developing applications with managed platforms

The Software as a Service (SaaS) model is characterized by accessing applications over the internet. In this model, software applications are hosted on a cloud infrastructure and provided to users via the web. This means that users do not need to install or run the software on their personal devices; instead, they can access these applications through a web browser, often requiring only an internet connection for functionality. This model offers numerous advantages, including scalability, automatic updates, and a pay-as-you-go pricing structure, which can lead to cost savings for individuals and organizations. Users benefit from the ability to access their software from anywhere, enabling greater flexibility and collaboration, especially in a world where remote work is becoming increasingly common. The other options describe different concepts. Hosting applications locally refers to traditional software installation, while providing virtualized computing resources aligns more closely with Infrastructure as a Service (IaaS). Developing applications with managed platforms is more relevant to Platform as a Service (PaaS), where developers are provided with a framework to build and manage software applications without the need for underlying infrastructure management.

4. Which type of malware is disguised as legitimate software to trick users?

A. Worm

B. Trojan

C. Virus

D. Botnet

The correct answer is Trojan. This type of malware is specifically designed to appear as legitimate software or to be bundled with legitimate applications, effectively tricking users into downloading and executing it. Once installed, Trojans can perform various malicious actions, such as stealing personal information, opening backdoors for further attacks, or allowing unauthorized access to the infected system. The key characteristic of a Trojan is its ability to mislead users; it does not replicate itself like viruses or worms and is often disguised in a way that looks appealing or useful, which is why users might unknowingly install it. Understanding this concept helps in recognizing the importance of being cautious about the software that one chooses to install and being vigilant about the sources from which it is obtained.

SAMPLE

5. What are trusted digital sources?

A. Content providers with a low user rating.

B. Websites known for accurate and reliable information.

C. Any site delivering free content.

D. Niche blogs with personal opinions.

Trusted digital sources refer to websites or platforms that are widely recognized for providing accurate, reliable, and well-researched information. These sources typically undergo rigorous editorial processes and adhere to established standards of journalism or academic integrity. This reliability is crucial in the digital age, where misinformation can easily spread through unverified content. Trusted digital sources often include established news organizations, educational institutions, and official government websites that present factual data and are vetted by experts in their respective fields. Their reputation for accuracy helps users feel confident that the information they are accessing is valid, helping them make informed decisions and form educated opinions. In contrast, other options present different types of digital content sources that do not necessarily guarantee reliability or accuracy. Websites with low user ratings may reflect poor quality or unreliable content, and while free content can be beneficial, it does not inherently signify trustworthiness. Similarly, niche blogs might provide personal insights but often lack the rigorous fact-checking processes needed to be classified as trusted sources.

6. What role does digital communication play in citizenship?

A. It restricts opinions to private messages only.

B. It allows individuals to participate in discussions and collaborate online.

C. It limits engagement to texting and private chats.

D. It discourages sharing personal opinions in public.

Digital communication plays a crucial role in citizenship by enabling individuals to actively participate in discussions and collaborate online. This functionality supports the exchange of ideas, opinions, and information on a wide array of topics, fostering a more engaged and informed citizenry. Through platforms such as social media, forums, and blogs, people can express their views publicly, join community initiatives, and mobilize support for social causes. This open dialogue is essential for democratic processes, as it allows for diverse perspectives to come together, encouraging collective problem-solving and civic engagement. By facilitating immediate communication and interaction across distances, digital communication enhances the ability of citizens to connect, organize, and advocate for change in their communities and beyond. The other options suggest limitations that do not align with the empowering potential of digital communication. Rather than restricting opinions or engagement, the role of digital communication is to broaden the channels through which citizens can express themselves and collaborate.

SAMPLE

7. Which of the following describes digital responsibility?

A. The act of ignoring harmful online content.

B. Understanding the ethical implications of online actions.

C. Withholding personal information at all times.

D. The requirement to share all online activities.

Digital responsibility encompasses the understanding and acknowledgment of the ethical implications surrounding one’s actions in the online environment. This includes recognizing that online behavior can have real-world consequences, both for oneself and for others. Acting responsibly in a digital context means being aware of how shared content can affect individuals’ reputations, feelings, and privacy. It necessitates a thoughtful approach to online interactions, ensuring that individuals engage with others respectfully and mindfully, and consider the impact of their digital footprint. While concepts like withholding personal information or ignoring harmful content play roles in online safety, they do not capture the broader and more nuanced understanding of digital responsibility that involves ethical decision-making and accountability. Sharing all online activities fails to reflect responsible conduct, as it could compromise personal safety and privacy. Thus, recognizing the ethical dimensions of online behavior is the essence of being digitally responsible.

8. What is the main feature of spyware?

A. Locking data for ransom

B. Connecting different systems

C. Monitoring user activities

D. Managing system resources

The main feature of spyware is its ability to monitor user activities. Spyware is a type of malicious software designed to gather information about a person or organization without their knowledge. It can track a user's internet browsing habits, collect personal data such as login credentials or credit card details, and send this information back to the entity that created or deployed it. This covert surveillance can occur through various means, including keylogging, where every keystroke is recorded, or through tracking cookies that can monitor web activity. The primary intent is to gather sensitive information which can be used for identity theft, financial fraud, or unauthorized access to private data. Understanding this helps highlight the importance of using robust security measures and maintaining privacy online.

SAMPLE

9. What does the process of compiling involve?

A. Translating code line by line

B. Running code instructions

C. Translating entire source code into machine code

D. Fixing errors in code

The process of compiling is primarily about translating entire source code into machine code. When a programmer writes code, it is typically in a high-level programming language that is human-readable. However, for the computer to execute instructions, it must be in machine code, which is composed of binary instructions that the computer's processor can understand. The compiler takes the full set of source code and transforms it all at once into machine code, creating an executable program. This allows the program to run efficiently as a single unit, rather than translating instructions individually at runtime, which can be slower and more error-prone. This process is essential in programming and software development because it ensures that the program can be executed smoothly by the computer hardware, optimizing performance and functionality. The distinction here is significant; while some processes may involve running or debugging code, compiling specifically refers to the translation of an entire codebase rather than handling code execution or error resolution.

10. What is the term for switching between different processes in a computer system, typically managed by the operating system?

A. Execution

B. Thread Management

C. Process Switch

D. Task Scheduling

The term for switching between different processes in a computer system, typically managed by the operating system, is known as "Process Switch." A process switch occurs when the operating system saves the state of one process and loads the state of another, allowing multiple processes to share the CPU efficiently. This is a crucial aspect of multitasking operating systems, which enable users to run several applications simultaneously without noticeable delay. In the context of operating systems, this switching is essential for maintaining an effective flow of operations, as it allows for the fluctuation of resources based on current demands and priorities. Each process has its own state, including the program counter, registers, and memory management information. The operating system's management of these aspects during a process switch ensures that processes can resume from where they left off. Understanding "Process Switch" helps explain how modern operating systems achieve multitasking, thereby maximizing the performance and usability of computer systems.

SAMPLE