Technical Support Fundamental Practice Test (Sample)

Study Guide

Everything you need from our exam experts!

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. Which of the following is a primary function of a firewall?

- **A. Store data**
- **B. Monitor network traffic**
- **C. Encrypt files**
- **D. Provide customer support**

2. Where are your BIOS settings typically stored?

- **A. Flash drive**
- **B. Hard drive**
- **C. CMOS chip**
- **D. RAM**

3. What does 'byte' represent in computing?

- **A. A unit of digital information that consists of 4 bits**
- **B. A unit of digital information that consists of 8 bits**
- **C. A standard measure of computer speed**
- **D. A type of storage device**

4. What does 'malware' refer to in technology?

- **A. Hardware that enhances computer performance**
- **B. Software intended to harm or disrupt systems**
- **C. Updates that improve functionality**
- **D. Programs for data recovery**

5. What is 'two-factor authentication'?

- **A. A single verification method for logins**
- **B. A process that requires two verification methods to access an account**
- **C. An encryption technique for data protection**
- **D. A type of malware that attacks online accounts**

6. True or false: You can create a network with two computers.

- **A. TRUE**
- **B. FALSE**

7. What command would be used to check the integrity of a hard drive in Windows?

A. format

B. diskpart

C. chkdsk

D. checkdisk

8. What was the main limitation of computer networking that the invention of the World Wide Web solved?

A. The TCP/IP protocol could only be used in universities, governments, and businesses.

B. People around the world could not send data to one another.

C. Networks couldn't talk to each other.

D. People could only receive the information in the form of text.

9. Which of these is application software?

A. Web browser

B. CPU

C. Email client

D. RAM

10. Which of the following are examples of IoT (Internet of Things)?

A. Online car dealerships

B. Refrigerators that track food inventory

C. Teachers posting assignments online

D. Thermostats that turn off automatically

Answers

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

Explanations

1. Which of the following is a primary function of a firewall?

A. Store data

B. Monitor network traffic

C. Encrypt files

D. Provide customer support

The primary function of a firewall is to monitor network traffic. Firewalls serve as a barrier between a trusted internal network and untrusted external networks, such as the internet. They analyze incoming and outgoing traffic and enforce pre-defined security rules to determine which traffic should be allowed or blocked. This vital role helps prevent unauthorized access to or from a private network and protects against various cyber threats, making it an essential component of network security. In contrast to monitoring network traffic, other options do not align with a firewall's primary function. Storing data pertains more to data storage systems rather than the traffic management role of a firewall. Encrypting files is a security measure that secures data, but it is typically handled by encryption software rather than a firewall. Customer support is a service function unrelated to the security features of firewalls. Therefore, monitoring network traffic effectively captures the core purpose of a firewall in the realm of cybersecurity.

2. Where are your BIOS settings typically stored?

A. Flash drive

B. Hard drive

C. CMOS chip

D. RAM

The BIOS settings are typically stored on a CMOS chip. This chip maintains the system's configuration settings, such as hardware settings and system time, even when the computer is powered off. The CMOS technology allows these settings to be preserved using a small battery on the motherboard, ensuring that the BIOS can access the configuration when the system is turned back on. The other options represent temporary or unrelated storage. A flash drive and hard drive are used for data storage and do not retain BIOS settings. RAM is volatile memory, which means it loses its contents when power is removed and is not used for storing BIOS settings. Therefore, the CMOS chip is the designated component for retaining those essential system settings between power cycles.

3. What does 'byte' represent in computing?

A. A unit of digital information that consists of 4 bits

B. A unit of digital information that consists of 8 bits

C. A standard measure of computer speed

D. A type of storage device

A byte is a fundamental unit of digital information in computing that consists of 8 bits. Each bit is a binary digit that can hold a value of either 0 or 1. The grouping of these 8 bits allows for the representation of 256 different values (from 0 to 255), which is sufficient for encoding a variety of characters in computer systems, including letters, digits, and special symbols. Understanding the byte as 8 bits is crucial for grasping how data is structured and processed within computer systems, as it serves as a building block for larger data types such as kilobytes, megabytes, gigabytes, and so forth. This concept is foundational in data analysis, programming, and any technical discussions about memory and data storage in computers.

4. What does 'malware' refer to in technology?

A. Hardware that enhances computer performance

B. Software intended to harm or disrupt systems

C. Updates that improve functionality

D. Programs for data recovery

Malware, short for malicious software, refers specifically to software designed with the intent to cause harm or disruption to systems, networks, or data. This encompasses a variety of harmful programs such as viruses, worms, Trojans, ransomware, and spyware. Malware can lead to unauthorized access, data theft, system damage, or other forms of malicious activity that compromise the security and integrity of computer systems. The other options describe different aspects of computing that do not align with the concept of malware. Enhancements to performance, updates for better functionality, and programs for data recovery all serve positive or constructive purposes in the realm of technology. In contrast, malware is fundamentally about malicious intent and damage, which solidifies option B as the accurate definition.

5. What is 'two-factor authentication'?

A. A single verification method for logins

B. A process that requires two verification methods to access an account

C. An encryption technique for data protection

D. A type of malware that attacks online accounts

Two-factor authentication (2FA) is a security process that enhances the protection of user accounts by requiring two distinct forms of verification before granting access. This typically involves something the user knows (like a password) and something the user has (like a mobile device to receive a verification code). The strength of 2FA lies in its layered approach to security. Even if a malicious actor manages to obtain the password, they would still be unable to access the account without the second factor, which significantly reduces the risk of unauthorized access. This method is widely used across various platforms to secure sensitive data and improve overall account security. The other options do not accurately capture the essence of two-factor authentication. For instance, relying on a single verification method would be considered less secure than 2FA. Encryption techniques and malware are unrelated concepts that pertain to data protection and online threats, respectively, making them unsuitable in the context of 2FA.

6. True or false: You can create a network with two computers.

A. TRUE

B. FALSE

The statement is true because it is indeed possible to create a network with just two computers. Networking fundamentally involves connecting devices to share resources and information. When two computers are connected, they can communicate with each other, share files, and even access shared peripherals like printers. This type of minimal setup can be accomplished using various methods, such as a direct cable connection or through a small home Wi-Fi network. For example, using an Ethernet cable, both computers can be linked directly, forming a simple network. Alternatively, if both computers are connected to a router or switch, they can communicate over a local area network (LAN). In addition, small networks don't require a large number of devices to be functional or to demonstrate network concepts; even a two-computer setup can serve educational purposes or satisfy specific practical needs, such as file sharing or gaming. The key concept is that any interconnected devices, regardless of quantity, are considered a network.

7. What command would be used to check the integrity of a hard drive in Windows?

A. format

B. diskpart

C. chkdsk

D. checkdisk

The command used to check the integrity of a hard drive in Windows is "chkdsk." This utility scans the file system and file system metadata of a volume for logical and physical errors. When executed, chkdsk can identify problems such as bad sectors, lost clusters, and cross-linked files. Depending on the parameters used with the command, it can also attempt to fix these errors by repairing the file system. This command is particularly valuable for maintaining the health of the hard drive, diagnosing issues, and ensuring data integrity. Running chkdsk regularly can help prevent data loss and increase system performance by addressing potential problems before they escalate. Other commands listed have different functions. For instance, "format" is primarily used to prepare a disk for use by erasing all existing data and setting up a file system. "diskpart" is a tool for managing disk partitions, allowing users to create, delete, or resize partitions but not to check disk integrity. "checkdisk" is not a recognized command in Windows; the correct command is "chkdsk." Therefore, choosing "chkdsk" is the appropriate action for verifying hard drive integrity.

8. What was the main limitation of computer networking that the invention of the World Wide Web solved?

A. The TCP/IP protocol could only be used in universities, governments, and businesses.

B. People around the world could not send data to one another.

C. Networks couldn't talk to each other.

D. People could only receive the information in the form of text.

The main limitation addressed by the World Wide Web was that networks couldn't effectively communicate with each other, which is reflected in the correct choice. Before the web, networking protocols existed, such as TCP/IP, but there were significant barriers to seamless integration among different networks. The World Wide Web established a standardized system, allowing diverse networks to interconnect and share information easily across the globe, breaking down silos of isolated networks. This interconnectivity was crucial for expanding the reach of information and services available online. By establishing hyperlinks and a common language through HTML and HTTP, the World Wide Web enabled a more integrated and user-friendly experience, vastly improving accessibility to information. Other factors like the ability to send data globally or the presentation of information were certainly enhanced by the web, but they were not the primary limitation that the web directly solved. The ability of different networks to communicate and exchange data was fundamental for creating the interconnected structure that is essential to the functionality of the internet today.

9. Which of these is application software?

A. Web browser

B. CPU

C. Email client

D. RAM

Application software refers to programs designed to carry out specific tasks for users, rather than performing system management tasks. A web browser is an example of application software because its primary function is to enable users to access and navigate the internet. It provides a user interface for viewing web pages, allows for interaction with web-based applications, and supports various media formats. An email client is also considered application software as it facilitates the sending, receiving, and organizing of email, but the chosen answer highlights the role of a web browser in broader access to internet content. Understanding the category of application software helps differentiate it from system software and hardware components such as the CPU and RAM, which serve different purposes in the computing environment.

10. Which of the following are examples of IoT (Internet of Things)?

A. Online car dealerships

B. Refrigerators that track food inventory

C. Teachers posting assignments online

D. Thermostats that turn off automatically

The choice highlighting refrigerators that track food inventory is a clear example of the Internet of Things (IoT) because it illustrates the core principle of IoT: devices connected to the internet that collect and exchange data. In this case, the refrigerator uses sensors to monitor the contents inside and send that data to a smartphone app or cloud service, enabling users to track what food items they have and receive notifications when supplies are low. This connectivity allows the device to execute functions beyond traditional capabilities, providing users with real-time updates and increasing convenience in managing household inventory. The nature of IoT is fundamentally about enhancing the functionality of everyday objects through connectivity and data sharing, which this example exemplifies well. While online car dealerships, teachers posting assignments online, and smart thermostats exhibit aspects of technology and connectivity, they do not fundamentally capture the essence of IoT devices as those in the food tracking scenario do. These other options don't necessarily involve the kind of device-to-device or device-to-internet data exchange specific to IoT.

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://techsupportfundamental.examzify.com

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