University of Central Florida (UCF) CGS2100 Computer Fundamentals for Business Practice Exam 2 (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. Which of the following statements is true regarding digital footprints?

- **A. They are completely invisible to users**
- **B. They only consist of user-generated content**
- **C. They can be monitored by various online services**
- **D. They cannot be changed or deleted once created**

2. Which of the following is NOT a type of printer?

- **A. Dot-Matrix printer**
- **B. LED printer**
- **C. Scanner printer**
- **D. Laser jet printer**

3. What does FTP stand for?

- **A. File Transfer Protocol**
- **B. Fast Transfer Process**
- **C. File Type Process**
- **D. Formatted Text Protocol**

4. What is the purpose of an antivirus program?

- **A. To create backups of files**
- **B. To detect, prevent, and remove malware**
- **C. To enhance internet browsing speed**
- **D. To improve system graphics**

5. In computer security, what is a virus?

- **A. A software that helps protect against malware**
- **B. A type of hardware component**
- **C. A type of malware that replicates and spreads**
- **D. A utility that cleans up files**

6. What does phishing refer to?

- **A. A method of data encryption**
- **B. A type of cybersecurity measure**
- **C. A cyber attack that deceives individuals into sharing sensitive information**
- **D. A legitimate business transaction**

7. **What does URL stand for?**

   A. Universal Resource Locator

   B. Uniform Resource Locator

   C. Universal Record Link

   D. Uniform Record Locator

8. **What could be a consequence of a computer virus for a business?**

   A. Improved customer data analysis

   B. Increased employee productivity

   C. Loss of sensitive information

   D. Enhanced software performance

9. **What process can a computer virus disrupt within an organization?**

   A. Mail delivery systems

   B. Financing options for customers

   C. Access to electronic documents and systems

   D. Employee training programs

10. **What is phishing in cybersecurity?**

    A. A method to enhance network performance

    B. A means to trick individuals into revealing confidential information

    C. A technique to encrypt data during transfer

    D. A form of direct hacking into user accounts

Answers

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

Explanations

1. Which of the following statements is true regarding digital footprints?

A. They are completely invisible to users

B. They only consist of user-generated content

C. They can be monitored by various online services

D. They cannot be changed or deleted once created

Digital footprints refer to the trail of data and information that users leave behind while using the internet. These footprints can be created through a variety of online activities, such as browsing websites, posting on social media, or interacting with online services. The statement indicating that digital footprints can be monitored by various online services is accurate because many platforms and companies track user behavior to improve their services, personalize advertisements, or gather analytics data. For example, web browsers use cookies to monitor user sessions, and social media platforms analyze user interactions to curate content and ads. The other options do not reflect the true nature of digital footprints. They are not completely invisible to users; in fact, many online tools provide visibility into aspects of a person's digital footprint. While user-generated content is a part of digital footprints, they also include passive data collected without user input. Additionally, while some aspects of a digital footprint can be challenging to change or delete, they are not entirely immutable; users have the ability to manage their digital presence to some extent by deleting accounts, adjusting privacy settings, or clearing browsing history.

2. Which of the following is NOT a type of printer?

A. Dot-Matrix printer

B. LED printer

C. Scanner printer

D. Laser jet printer

The choice of "Scanner printer" as the option that is NOT a type of printer is based on the fact that a scanner is primarily a device used for digitizing physical documents and images, rather than producing physical printed outputs. While there are multifunction devices that include scanning capabilities along with printing, the term "scanner printer" itself does not accurately represent a distinct type of printer like the other options do. Dot-matrix, LED, and laser jet printers are all established categories of printers that utilize different technologies to produce printed material. Dot-matrix printers use a series of pins to strike an ink ribbon and transfer ink onto paper. LED printers use a light-emitting diode array to create an image on a drum that in turn applies toner to paper. Laser jet printers use a laser beam to produce an image on a drum, which is then coated with toner and fused onto paper. Understanding this distinction emphasizes the specific functionalities of printers versus scanning devices, which is key in computer fundamentals for business practice. Each printer type mentioned produces printed material, while the "scanner printer" terminology lacks a standardized definition in the context of printers.

3. What does FTP stand for?

A. File Transfer Protocol

B. Fast Transfer Process

C. File Type Process

D. Formatted Text Protocol

FTP stands for File Transfer Protocol, which is a standard network protocol used to transfer files from one host to another over a TCP-based network, such as the Internet. It allows users to upload and download files efficiently between a client and a server. The protocol operates on a client-server model, where the client requests a file and the server responds by sending the file or receiving files to be stored. Understanding FTP is crucial for various applications, particularly in business practices that require sharing large amounts of data securely and efficiently. It supports features such as authentication, where users are required to provide credentials to access files, and it can operate in both active and passive modes to accommodate different network configurations. This functionality makes FTP a foundational tool in network management and data transfers. The incorrect options reflect misunderstandings of the protocol's true purpose. For instance, "Fast Transfer Process" and "File Type Process" mistakenly imply attributes or functions that are not officially recognized in the field of computer networking, while "Formatted Text Protocol" incorrectly suggests that FTP is specifically tied to text formatting, which is not its primary function.

4. What is the purpose of an antivirus program?

A. To create backups of files

B. To detect, prevent, and remove malware

C. To enhance internet browsing speed

D. To improve system graphics

The purpose of an antivirus program is to detect, prevent, and remove malware. This includes a variety of harmful software types such as viruses, worms, trojans, ransomware, and spyware. These malicious programs can compromise system security, steal personal information, or cause significant damage to data and systems. Antivirus software continuously monitors the system for suspicious activity, scans files for known virus signatures, and offers real-time protection against new threats. By identifying and neutralizing these threats before they can affect system integrity, an antivirus program plays a crucial role in maintaining the security and health of computers and networks. The other options, while related to computer functionality, do not accurately describe the primary function of antivirus software. Creating backups of files pertains to data management and recovery, enhancing internet browsing speed is related to network performance, and improving system graphics involves hardware and software adjustments for visual output.

5. In computer security, what is a virus?

A. A software that helps protect against malware

B. A type of hardware component

C. A type of malware that replicates and spreads

D. A utility that cleans up files

A virus is defined as a type of malware that replicates and spreads by inserting copies of itself into other programs, files, or the boot sector of a computer's hard drive. When the infected program is executed, the virus activates and can disrupt system operations, corrupt data, or even compromise security. This self-replicating nature allows viruses to spread to other systems, often without the user's knowledge, making them a significant threat in the realm of computer security. The other options do not accurately describe what a virus is. For instance, the first choice refers to anti-virus software, which is designed to detect and remove malware, not function as the malware itself. The second option inaccurately categorizes a virus as hardware, while viruses are strictly software programs. The fourth option describes a utility function, which is focused on file cleanup rather than the propagation of malicious software. Therefore, the correct identification of a virus as a type of malware that replicates and spreads is crucial for understanding how to defend against and mitigate its impact on computer systems.

6. What does phishing refer to?

A. A method of data encryption

B. A type of cybersecurity measure

C. A cyber attack that deceives individuals into sharing sensitive information

D. A legitimate business transaction

Phishing refers to a cyber attack that deceives individuals into sharing sensitive information by posing as a trustworthy entity in electronic communications. This typically involves fraudulent emails, messages, or websites that mimic legitimate organizations to trick users into revealing personal data, such as passwords, credit card numbers, or social security numbers. The attackers often create a sense of urgency or manipulate emotions to compel victims to act quickly without thinking critically about the authenticity of the request.   Understanding phishing is essential for cybersecurity awareness because it highlights the importance of verifying the sources of electronic communications and being cautious about the information shared online. This context is critical for recognizing the threat posed by phishing attempts and implementing appropriate security measures to protect personal and organizational data.

7. What does URL stand for?

A. Universal Resource Locator

B. Uniform Resource Locator

C. Universal Record Link

D. Uniform Record Locator

The correct term that URL stands for is "Uniform Resource Locator." A URL is a specific type of Uniform Resource Identifier (URI) that is used to specify the address of a resource on the internet. It provides not just the location of a resource, such as a webpage, but also the protocol used to access it, such as HTTP or HTTPS. In the context of web technology, a URL enables users to retrieve resources from the web by providing a clear and standardized way to identify and locate them. This uniformity is key because it allows different systems and browsers to understand and access resources consistently. The term "uniform" reflects the standardized format of the address, which is critical for interoperability across different web services and platforms. This ensures that regardless of the device or browser being used, the URL can be interpreted correctly to locate the desired resource. Other options refer to terms that are either incorrect or not widely recognized in relation to web addresses or resource identification, which helps clarify why "Uniform Resource Locator" is the correct and widely accepted definition.

8. What could be a consequence of a computer virus for a business?

A. Improved customer data analysis

B. Increased employee productivity

C. Loss of sensitive information

D. Enhanced software performance

A computer virus can have devastating effects on a business, one of the most significant being the loss of sensitive information. When a virus infects a system, it can corrupt or even delete critical data, such as customer information, financial records, and proprietary business data. This loss can lead to severe operational disruptions, damage to brand reputation, and even legal implications if sensitive customer data is compromised. In contrast, the other options imply positive outcomes, which are not outcomes typically associated with a virus. Improved customer data analysis or increased employee productivity tends to result from effective data management and systems, not from a virus. Similarly, enhanced software performance is unlikely as a virus generally degrades performance rather than improves it. Thus, the most realistic and severe consequence of a computer virus for a business is indeed the potential loss of sensitive information.

9. What process can a computer virus disrupt within an organization?

A. Mail delivery systems

B. Financing options for customers

C. Access to electronic documents and systems

D. Employee training programs

A computer virus can significantly disrupt access to electronic documents and systems within an organization. When a virus infects a computer network, it can corrupt files, compromise data integrity, and restrict user access to essential programs and documents. This disruption can lead to loss of productivity, as employees may be unable to retrieve necessary information or use critical applications to carry out their tasks. The impact can spread throughout the organization, affecting collaboration and operational efficiency, which are vital for smooth business operations.   While mail delivery systems, financing options for customers, and employee training programs are also essential elements of an organization, they are not as directly impacted by a virus as access to electronic documents and systems is. A virus primarily targets computers and files rather than directly affecting policies or processes related to financing or training.

10. What is phishing in cybersecurity?

A. A method to enhance network performance

B. A means to trick individuals into revealing confidential information

C. A technique to encrypt data during transfer

D. A form of direct hacking into user accounts

Phishing is a technique used in cybersecurity that involves tricking individuals into revealing sensitive or confidential information, such as passwords, credit card numbers, or personal identification information. Attackers typically use deceptive emails, messages, or websites that appear to be legitimate to lure victims into providing their information voluntarily.   By masquerading as a trustworthy entity, phishing attempts exploit human psychology, leveraging the instinct to trust familiar sources. Victims often do not realize they are providing their information to a malicious actor until it is too late, leading to potential identity theft or financial loss.   Understanding the nature of phishing is crucial for maintaining cybersecurity, as recognizing the tactics used in these scams is a key defensive strategy for protecting personal and organizational data.

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://ucf-cgs2100-exam2.examzify.com

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