SAFESCHOOLS TRAINING 2 PRACTICE TEST (SAMPLE)

STUDY GUIDE

SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://safeschoolstraining2.examzify.com

Table of Contents

Copyright 1

Table of Contents 2

Introduction 3

How to Use This Guide 4

Questions 5

Answers 8

Explanations 10

Next Steps 15

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. Educators must learn everything there is to know about every culture to be culturally competent.

A. True

B. False

C. Only for certain cultures

D. In higher education required

2. As specified by FERPA, noncustodial parents have the full rights as parents for access to student records.

A. True

B. False

C. Only if granted by court order

D. Only for certain records

3. Which of these attacks targets employees today?

A. Phishing

B. Malware

C. All of these

D. Password spraying

4. FERPA regulations require that local education agencies provide parents and eligible students with notification of their rights under FERPA

A. Upon request only

B. In the student handbook

C. In a place where it's likely to be seen

D. Annually by mail

5. Which practice helps verify that a website is legitimate?

A. Take a screenshot and share with colleagues

B. Ignore certificate warnings

C. Check for indicators such as HTTPS, valid certificate, and a padlock icon

D. Enter sensitive information if the site loads quickly

6. Tailgating, dumpster diving, and shoulder surfing are forms of which type of attacks?

A. Social engineering attacks

B. Physical security attacks

C. Network attacks

D. Malware attacks

7. What steps should you take to report suspected child abuse or neglect?

A. Immediately report to the designated child protective services or district hotline, then document the report and follow up per policy

B. Discuss concerns with a coworker before reporting

C. Wait 24 hours before reporting

D. Report only if the student requests it

8. What is recommended to ensure safety information is accessible to students with disabilities during drills?

A. Use only verbal instructions

B. Limit drills to able-bodied students

C. Ignore accessibility issues

D. Provide accommodations, accessible formats, and ensure staff are trained

9. Jailbreaking or rooting a portable device can lead to which consequences?

A. Increased performance

B. Access to official app stores

C. Improved stability

D. All of these

10. Which of the following are the two forms of identity theft?

A. True name and account takeover

B. Phishing and spoofing

C. Social engineering and data breach

D. Malware and ransomware

Answers

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

Explanations

1. Educators must learn everything there is to know about every culture to be culturally competent.

A. True

B. False

C. Only for certain cultures

D. In higher education required

Cultural competence is about engaging respectfully and effectively with students from diverse backgrounds, through ongoing learning and humility rather than trying to know everything about every culture. It's unrealistic to expect educators to master every culture in depth, since cultures are diverse, fluid, and can vary widely among individuals within the same group. The goal is to avoid stereotypes by asking questions, listening to students and families, and using culturally responsive teaching practices that honor students' experiences. This approach focuses on building relationships, validating students' identities, and adapting instruction to reflect diverse perspectives, not on achieving exhaustive knowledge of all cultures. Therefore, the statement is false because cultural competence is a continual process, applicable to all educators in all settings, not a matter of knowing every culture exhaustively.

2. As specified by FERPA, noncustodial parents have the full rights as parents for access to student records.

A. True

B. False

C. Only if granted by court order

D. Only for certain records

FERPA protects a parent's right to access their child's education records. Those rights are held by the parent, and noncustodial parents are included unless a court has restricted access. In practice, this means a noncustodial parent can inspect and obtain disclosures of the student's records without the student's consent, provided there isn't a court order or state law that says otherwise. If a court order limits a parent's access, schools must follow that order. So, generally, noncustodial parents have the same access as other parents under FERPA, making the statement true.

3. Which of these attacks targets employees today?

A. Phishing

B. Malware

C. All of these

D. Password spraying

Many attacks today rely on exploiting people as the entry point into an organization. Phishing directly targets employees by sending deceptive emails or messages designed to trick them into revealing credentials or clicking a malicious link or attachment. Password spraying focuses on employees by trying common or reused passwords across many accounts, taking advantage of weak password practices across the workforce. Malware often reaches employees' devices because they click a malicious link or open an infected attachment, giving attackers a foothold on the network. Since each of these tactics can involve leveraging employees or their devices, all of these are ways attackers target employees today.

4. FERPA regulations require that local education agencies provide parents and eligible students with notification of their rights under FERPA

A. Upon request only

B. In the student handbook

C. In a place where it's likely to be seen

D. Annually by mail

FERPA requires annual notification of rights to parents and eligible students, and the way that notice is delivered matters for making sure people actually know their rights. The best approach is to provide it in a place likely to be seen. Posting the information in a public, easily accessible location—such as the school or district site, a visible bulletin in the building, or in materials that families regularly read—helps ensure every family and student becomes aware without having to request it. While mailing the notice or including it in a student handbook can also work, relying only on requests or a single document isn't as reliable for ensuring broad, ongoing awareness.

5. Which practice helps verify that a website is legitimate?

A. Take a screenshot and share with colleagues

B. Ignore certificate warnings

C. Check for indicators such as HTTPS, valid certificate, and a padlock icon

D. Enter sensitive information if the site loads quickly

Verifying a website's legitimacy comes from confirming a secure connection and a valid identity. When a site uses HTTPS and presents a valid certificate, with a padlock icon shown by the browser, you have visual indicators that the connection is encrypted and the site's identity has been validated by a trusted authority. HTTPS means data between you and the site is protected from interception, while a valid certificate means the site's certificate is issued by a trusted authority, is not expired, and matches the site's domain. The padlock icon is a quick cue that these checks have passed, giving you more confidence before entering any sensitive information. Taking a screenshot and sharing with colleagues doesn't verify legitimacy. Ignoring certificate warnings bypasses critical protections and can expose you to attacks. Entering sensitive information just because a site loads quickly is risky, since speed doesn't confirm legitimacy and phishing sites can load rapidly as well.

6. Tailgating, dumpster diving, and shoulder surfing are forms of which type of attacks?

A. Social engineering attacks

B. Physical security attacks

C. Network attacks

D. Malware attacks

These attacks target physical security by exploiting people and the environment to gain access or obtain sensitive information. Tailgating happens when someone follows an authorized person through a secure door, bypassing access controls. Dumpster diving involves searching through discarded materials to find documents or data that can be used to breach security. Shoulder surfing is watching someone enter a password or PIN to steal credentials. None of these rely on hacking networks or deploying malware; they rely on physical access, disposal practices, and human behavior, which is why they're categorized as physical security attacks. To reduce risk, strengthen access controls, train people to avoid letting others piggyback, securely dispose of sensitive information, and use privacy measures when entering credentials.

7. What steps should you take to report suspected child abuse or neglect?

A. Immediately report to the designated child protective services or district hotline, then document the report and follow up per policy

B. Discuss concerns with a coworker before reporting

C. Wait 24 hours before reporting

D. Report only if the student requests it

The main concept here is that when you suspect child abuse or neglect, you must report it immediately to the designated child protective services or district hotline, then document the report and follow your policy for any required follow-up. This approach ensures the concern is evaluated quickly, the child's safety is prioritized, and there's a clear, official record of what happened and what actions were taken. Reporting right away is required because it triggers timely protective intervention and helps reduce risk to the child. Thorough documentation creates a traceable account for investigators and helps ensure appropriate next steps are taken. Other options fall short because they can delay protection or rely on the child to initiate action. Discussing concerns with a coworker first may slow the response and raise confidentiality issues. Waiting 24 hours postpones potential intervention. Reporting only if the student requests it fails to meet mandated reporting obligations and could leave the child in danger.

8. What is recommended to ensure safety information is accessible to students with disabilities during drills?

A. Use only verbal instructions

B. Limit drills to able-bodied students

C. Ignore accessibility issues

D. Provide accommodations, accessible formats, and ensure staff are trained

Ensuring safety information during drills is accessible to students with disabilities by providing accommodations, accessible formats, and trained staff. This approach means planning in advance so every student can participate and understand what to do. Accommodations might include extra time to move, the presence of a buddy or aide, or sign language interpretation. Accessible formats cover large print, Braille, plain-language written instructions, captions, and audio descriptions. Well-trained staff know how to communicate clearly, guide students safely, adapt evacuation routes, and coordinate supports like interpreters or assistive technologies. This combination helps all students react quickly and safely, fulfilling both safety and inclusion goals. Verbal instructions alone miss many learners, and limiting drills to able-bodied students excludes people who need accommodations, creating unnecessary risk. Ignoring accessibility issues is unsafe and unfair.

9. Jailbreaking or rooting a portable device can lead to which consequences?

A. Increased performance

B. Access to official app stores

C. Improved stability

D. All of these

Removing built-in restrictions to gain control over the device allows you to customize beyond what the manufacturer permits. This can open the door to tweaks and apps not available in the official store, and in some cases people try performance-focused tweaks that might make the device feel snappier. But these gains come with tradeoffs. Security is weaker because you're bypassing safeguards and vetting, which raises the risk of malware and data exposure. Stability can suffer as unofficial tweaks and apps may conflict with system updates or other software, leading to crashes or instability. Warranty and official support are often voided, making future repairs or updates more difficult. You can still access the official app store, but that access isn't the primary effect of jailbreaking or rooting, and relying on unofficial sources introduces the biggest risks. So the idea that all these outcomes reliably occur together isn't accurate; the practice mainly trades increased control for higher security and stability risks.

10. Which of the following are the two forms of identity theft?

A. True name and account takeover

B. Phishing and spoofing

C. Social engineering and data breach

D. Malware and ransomware

Identity theft comes in two main forms: true name identity theft, where someone uses your real name and identifying details to commit fraud in your name (for example, opening new credit accounts or taking out loans), and account takeover, where a thief gains control of an existing account you own and uses it to steal funds or information. The other terms describe methods or broader attack types rather than the form of theft itself: phishing and spoofing are tricks to obtain information, social engineering and data breaches are tactics or events that enable theft, and malware and ransomware are malicious software used to disrupt systems or extract data. So the two forms of identity theft are true name identity theft and account takeover.

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://safeschoolstraining2.examzify.com

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