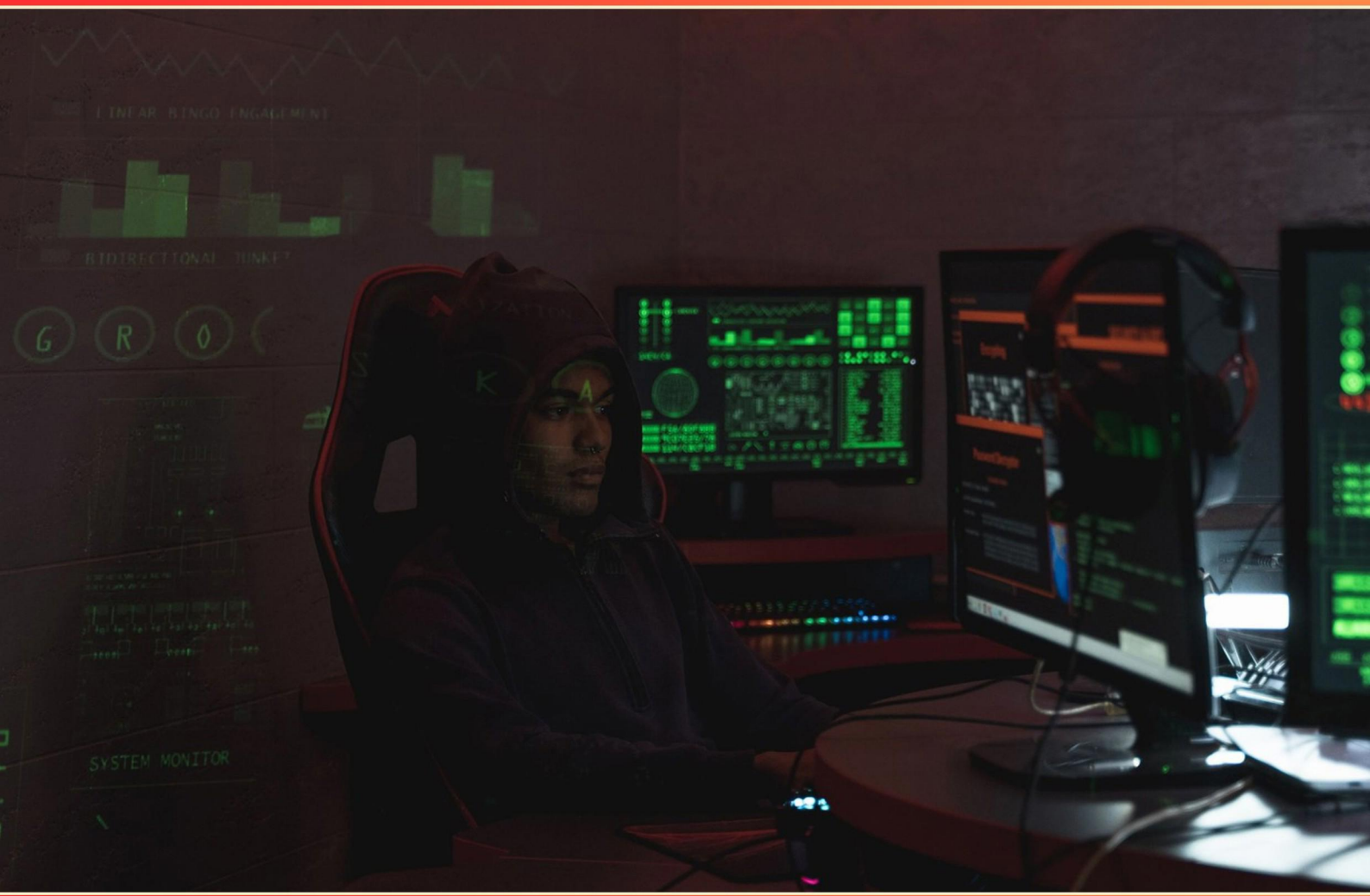
CYBERCRIME PRACTICE TEST (SAMPLE)

STUDY GUIDE



SAMPLE STUDY GUIDE WITH LIMITED QUESTIONS

VISIT US ONLINE FOR THE FULL VERSION STUDY GUIDE

https://cybercrime.examzify.com

Copyright © 2026 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 accurate, complete, and timely information about this product from reliable sources.

SAMPLE

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

SAMPLE

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.

SAMPLE

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!

SAMPLE

Questions

SAMPLE

1. **The CSSS arrests and prosecutes the sale and distribution of counterfeit pharmaceuticals and controlled substances over the Internet through which operation?**

   A. Operation Pillwise

   B. Operation Apothecary

   C. Operation NetRx

   D. Operation Counterfeit

2. **Which center is the primary channel for submitting Internet crime complaints to federal authorities?**

   A. Internet Crime Complaint Center

   B. National Security Agency

   C. Federal Bureau of Investigation Cyber Division

   D. Department of Homeland Security

3. **The claim that the NSA has provided code-breaking capabilities since the Civil War is historically accurate.**

   A. False

   B. True

   C. Not Mentioned

   D. Always True

4. **Which of the following is NOT a form of telecommunications fraud?**

   A. Phone phreaking

   B. Theft of telephone credit card numbers

   C. Hacking into telecommunications 'switches'

   D. Wireless phone theft and fraud

5. **Which agency leads investigations into access device fraud?**

   A. FBI

   B. Secret Service

   C. DEA

   D. ATF

SAMPLE

6. Which statement best describes ransomware?

A. It encrypts data and demands payment

B. It self-replicates by attaching to files

C. It hides inside legitimate software

D. It steals user credentials

7. The entity that provides victims of Internet fraud with a mechanism to report suspicious online activities is known as which?

A. Internet Crime Complaint Center

B. FBI Cyber Division

C. Department of Homeland Security National Cybersecurity and Communications Integration Center

D. Federal Trade Commission Consumer Protection Network

8. Which OSI layer is typically associated with MAC addressing and Ethernet frames?

A. Physical Layer (Layer 1)

B. Network Layer (Layer 3)

C. Application Layer (Layer 7)

D. Data Link Layer (Layer 2)

9. Which of the following is another typical digital evidence artifact encountered in investigations?

A. System/application logs and event timestamps

B. Printed manuals

C. Employee vacation schedules

D. Hardware warranty papers

10. How is a geographically compact crime scene under the administrative control of a single entity classified?

A. Multi-scene

B. Hybrid-scene

C. Single-scene

D. Network-scene

SAMPLE

Answers

SAMPLE

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

SAMPLE

Explanations

SAMPLE

1. The CSSS arrests and prosecutes the sale and distribution of counterfeit pharmaceuticals and controlled substances over the Internet through which operation?

A. Operation Pillwise

B. Operation Apothecary

C. Operation NetRx

D. Operation Counterfeit

This question hinges on recognizing an operation name that aligns with online pharmaceutical crimes. The best fit is the one that evokes medicine and drug handling, since the activity involves counterfeit pharmaceuticals and controlled substances sold over the Internet. An operation named Apothecary fits this theme perfectly because an apothecary is a historical term for a person who dispenses medicines. It creates an immediate connection to drugs and dispensing, which is exactly what the CSSS target in this context. The other names feel less precise for this scenario. Pillwise sounds like a casual reference to pills but doesn't clearly signal an official undercover operation. NetRx hints at online pharmacies but is more of a descriptor than a formal operation name. Counterfeit is too generic and doesn't convey the specific pharmacy/drug focus or the investigative branding typical of law enforcement campaigns.

2. Which center is the primary channel for submitting Internet crime complaints to federal authorities?

A. Internet Crime Complaint Center

B. National Security Agency

C. Federal Bureau of Investigation Cyber Division

D. Department of Homeland Security

The main concept here is where you report internet crime to federal authorities. The primary channel is the Internet Crime Complaint Center, a joint effort by the FBI and the National White Collar Crime Center. This site is specifically designed as the public intake point for internet-enabled crimes, such as scams, fraud, hacking, and other online offenses. Submitting your complaint there helps collect and categorize information so investigators can analyze trends and push leads to the right federal agencies for action. The other options serve related roles—NSA focuses on intelligence and security, the FBI Cyber Division handles investigations but generally relies on the IC3 page as the initial report channel, and DHS coordinates broader national cybersecurity efforts rather than acting as the single public complaint portal.

3. The claim that the NSA has provided code-breaking capabilities since the Civil War is historically accurate.

A. False

B. True

C. Not Mentioned

D. Always True

This question tests your ability to line up historical timelines with organizational roles. The NSA did not exist during the Civil War; it was created in 1952 (originating from earlier U.S. signals intelligence efforts, but not as a present-day agency in the 1860s). While cryptography and code-breaking have a long history, attributing NSA-level capabilities to the Civil War era misplaces the organization in time. Because of that, the claim is not historically accurate. The best answer is that this statement is false.

SAMPLE

4. Which of the following is NOT a form of telecommunications fraud?

A. Phone phreaking

B. Theft of telephone credit card numbers

C. Hacking into telecommunications 'switches'

D. Wireless phone theft and fraud

Understanding what counts as telecommunications fraud helps distinguish acts that manipulate the phone system for illicit gain from activities that don't fit that category by themselves. Phone phreaking describes historical experimentation with how the telephone network signals and routes calls, often to understand or socialize the system. While it can cross into illegal territory, it's not regarded as a specific fraud category in the same way as the other options. The other choices clearly involve illicit financial or operational exploitation: theft of telephone credit card numbers is direct financial fraud, hacking into telecommunications switches is unauthorized intrusion to alter or intercept service, and wireless phone theft and fraud involves stealing devices to commit or enable fraudulent use. Because phreaking centers on exploring the network rather than a defined fraudulent scheme, it isn't considered a form of telecommunications fraud in the same sense as the others.

5. Which agency leads investigations into access device fraud?

A. FBI

B. Secret Service

C. DEA

D. ATF

The main concept is which agency leads investigations into access device fraud, meaning crimes involving payment cards and other electronic credentials used to obtain goods or services. Access device fraud covers counterfeit or stolen card data, skimmed card numbers, and other fraud tied to payment systems. The agency with the primary responsibility for protecting and investigating these financial-payment system crimes is the Secret Service. Its mandate includes safeguarding the nation's payment networks and leading investigations into card fraud, ATM skimming, and related data breaches that target cardholder data. While the FBI handles many cyber and financial crimes, the Secret Service is the designated lead for this specific area of fraud. The other agencies listed focus on different domains (drugs, weapons, broader federal crimes) and aren't the primary leads for access device investigations.

6. Which statement best describes ransomware?

A. It encrypts data and demands payment

B. It self-replicates by attaching to files

C. It hides inside legitimate software

D. It steals user credentials

Ransomware works by encrypting files to make them unreadable and then demanding payment in exchange for a decryption key. That combination of denying access to data and extorting the victim is the defining behavior of this malware type. Other descriptions point to different threats: self-replication by attaching to files is characteristic of viruses or worms, hiding inside legitimate software describes a trojan, and stealing user credentials aligns with spyware or credential-theft malware. So the statement about encryption and a ransom demand captures what ransomware does and why it's distinguished from other malware.

SAMPLE

7. The entity that provides victims of Internet fraud with a mechanism to report suspicious online activities is known as which?

A. Internet Crime Complaint Center

B. FBI Cyber Division

C. Department of Homeland Security National Cybersecurity and Communications Integration Center

D. Federal Trade Commission Consumer Protection Network

Centralized reporting of internet crimes to law enforcement is the key idea here. The Internet Crime Complaint Center provides a formal, federally supported channel for victims of online fraud to file complaints about suspicious activity. It collects details, categorizes the incident, and forwards the information to the appropriate law enforcement agencies to investigate. This makes it the go-to mechanism for reporting internet crimes by the public. The other options are real agencies or centers, but they don't serve as the public-facing, centralized reporting hub in the same way: the FBI Cyber Division handles investigations and cyber matters but not the standard consumer report portal; the Department of Homeland Security's NCCIC coordinates cybersecurity activities rather than serving as the primary public reporting channel; and the Federal Trade Commission focuses on consumer protection and may take complaints, but IC3 is specifically designed to route internet crime reports to law enforcement.

8. Which OSI layer is typically associated with MAC addressing and Ethernet frames?

A. Physical Layer (Layer 1)

B. Network Layer (Layer 3)

C. Application Layer (Layer 7)

D. Data Link Layer (Layer 2)

MAC addressing and Ethernet frames live at the Data Link Layer because this layer defines how devices on the same local network are identified and how data is packaged for delivery over the physical link. Ethernet frames carry a destination MAC address and a source MAC address in their header, and switches use these addresses to forward frames within a LAN. The Data Link Layer also handles frame delimitation and error detection via mechanisms like the Frame Check Sequence. The Network Layer handles IP addresses and routing between networks, so MAC addresses aren't used for end-to-end routing. The Physical Layer is about the actual signaling and bits on the wire, while the Application Layer deals with software processes and user-facing data. For these reasons, MAC addressing and Ethernet frame structure are best associated with the Data Link Layer.

SAMPLE

9. Which of the following is another typical digital evidence artifact encountered in investigations?

A. System/application logs and event timestamps

B. Printed manuals

C. Employee vacation schedules

D. Hardware warranty papers

System and application logs with their event timestamps are digital traces that capture actions, access attempts, and system states as they happen. These logs come from operating systems, applications, and network devices, recording who did what, when, and from where. The timestamps are critical because they let investigators build an accurate timeline of events, correlate actions across multiple systems, and identify anomalies such as logins at odd times, unusual file access, or strange network activity. Because logs are generated automatically and stored in digital form, they are a go-to source of evidence in most investigations. Printed manuals, employee vacation schedules, and hardware warranty papers are primarily physical or HR records, not digital traces of activity. They don't automatically reflect system or user activity and typically don't provide the time-ordered actions investigators need to reconstruct events.

10. How is a geographically compact crime scene under the administrative control of a single entity classified?

A. Multi-scene

B. Hybrid-scene

C. Single-scene

D. Network-scene

When a crime scene is confined to one physical location and managed by a single entity, it is treated as a single-scene crime scene. This classification matters because the investigation can be organized around one locus of evidence, with a single command structure, streamlined evidence handling, and consistent procedures for preservation and documentation. It reduces the need for cross-jurisdiction coordination and simplifies chain-of-custody considerations since everything occurs in one place under one administrative authority. If the scene were spread across multiple locations, you'd be dealing with a multi-scene scenario that requires coordination among different teams or agencies. A hybrid-scene would involve both single and multiple locations under possibly different authorities. A network-scene implies scenes spread across interconnected sites tied by networks rather than a single geographic site.

SAMPLE

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://cybercrime.examzify.com

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

SAMPLE