Cybersecurity Essentials

The Beginner’s Guide

Ojula Technology Innovations

Cybersecurity Essentials

The Beginner’s Guide

ISBN: 9798840919057

Published in the United States

Limit of Liability/Disclaimer of Warranty

This book contains information obtained from authentic and highly regarded sources. Reasonable efforts have been made to publish reliable data and information, but the author and publisher cannot assume responsibility for the validity of all materials or the consequences of their use. All information given in this book is based on the author’s own knowledge and research, and does not constitute technical, financial or professional advice. The author and publisher have attempted to trace the copyright holders of all material reproduced in this publication, and apologize to copyright holders if permission to publish in this form has not been obtained. If any copyright material has not been acknowledged please write and let us know so we may rectify in any future reprint.

Table of Contents

Contents of This Sample

Contents of Rest of Book

How this Book can Help You

If you need to read only one book to acquire a strong foundation in cybersecurity fundamentals, make it this one. This is not just another book on cybersecurity. It is a well-illustrated *practical* guide designed for beginners to familiarize them with the latest cyber security landscape and provide the knowledge of relevant tools to assess and manage security protocols in information processing systems. It is a self-paced book that is excellent for beginners, practitioners and scholars alike.

After completing this book, you will be able to:

- Explain basic security risks, security of data and information, types of security breaches, and how to manage security threats
- Demonstrate how to configure browsers and safe browsing practices
- Identify security threats and explain how to address them in applications and shared networks

Whether you're skilling up to become a Help Desk Support Specialist, Security Specialist, Virtual Customer Service Agent, or just want to learn the basics of working in and managing security and security systems, you need a strong foundation in security fundamentals.

This course is divided into three modules:

- Common Security Threats and Risks
- Security Best Practices
- Safe Browsing Practices

You'll learn about common security risks and the importance of information privacy. You'll also learn various ways to identify and protect your organization against different types of security breaches and malware threats, and you'll discover more about confidentiality, integrity, and availability.

You’ll learn about security best practices, creating effective passwords, and securing devices. You will learn about authentication, authorization, and accounting, and how these concepts help secure devices, validate devices and servers, encrypt devices, and manage email and spam.

You’ll learn about safety concerns with applications and public browsing, including managing plug-ins, extensions, and toolbars. You will learn about web browser security configurations, cookies, and computer caches.

To successfully complete this guide, you should be familiar with:

- Basic computer operating skills
- Basic knowledge of computer terminology
- Knowledge of switching applications
- Familiarity with MS Windows OS

1. What is Cybersecurity?

Cybersecurity is the practice of protecting systems, networks, and programs from digital attacks. These attacks typically include business interruptions or the theft, tampering, or destruction of sensitive information.

Ransomware attacks are on the rise and are predicted to cost victims more than $265 billion (USD) annually by 2031. That is just one type of threat we all need to protect against. The need for organizations to implement effective security practices has never been more important or urgent.

This module will teach you the skills you need to identify basic security threats and choose the best security practices to address those threats. In this chapter, you'll learn the difference between data, information, and insights and how companies leverage all three to help guide their business decisions. You'll learn how to maintain data integrity and keep data confidential. You'll also learn about the different types of attacks and breaches that threaten today's organizations and their data.

1.1. Learning Objectives

- Explain how to keep data safe, confidential, and tamper-resistant
- Define what data is, how it drives business decisions, and how companies manage it
- Identify security threats like hacking, data theft, malware, and data leaks
- List other types of attack vectors used by cybercriminals

1.2. Security Threats: Confidentiality, Integrity, and Availability

After studying this section, you will be able to:

- Explain what the CIA Triad is
- list concerns related to the CIA Triad
- define common regulatory standards and penalties

1.2.1. The CIA Triad

A comprehensive security program must include confidentiality, integrity, and availability. These are known as the CIA Triad.

Confidentiality means that data is protected from unauthorized access. Integrity means that data is protected from unauthorized changes. Availability means that you have access to your data whenever you need it.

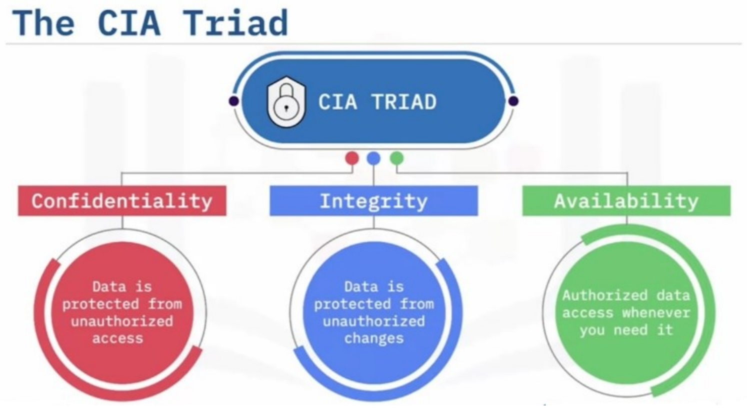
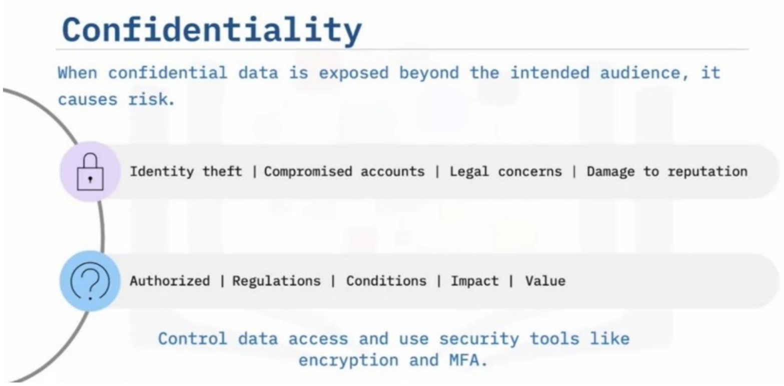

The CIA Triad
CIA TRIAD
Confidentiality
Integrity
Availability
Data is protected from unauthorized access
Data is protected from unauthorized changes
Authorized data access whenever you need it

Figure 1.1: Components of the CIA Triad

Confidentiality

When confidential data is exposed beyond the intended audience, it causes risk. Confidential information is kept secret to prevent: identity theft, compromised accounts and systems, legal concerns, damage to reputation, and other severe consequences.



Confidentiality

When confidential data is exposed beyond the intended audience, it causes risk.

Identity theft | Compromised accounts | Legal concerns | Damage to reputation

Authorized | Regulations | Conditions | Impact | Value

Control data access and use security tools like encryption and MFA.

Figure 1.2: Facts about Confidentiality

To determine if data should be confidential, ask: Who is authorized? Do confidentiality regulations apply? Are there conditions for when data can be accessed? What would the impact of disclosure be? Is the data valuable?

Cybercriminals are always after sensitive information or personal data. To keep confidential data secure, control data access and use security tools like encryption and multifactor authentication (MFA).