

9

Program name	Duration:	Trainee entry level
Cybersecurity and Protection from Cybercrimes Course	18 days 30 training hours	Primary school certificate at least

Design of this program:

The Cybersecurity course focuses on equipping participants with the knowledge and skills necessary to understand digital threats and secure data and systems from increasing cyberattacks. This course provides an essential introduction to the principles of information security, network protection, encryption, threat detection, and digital defense methods, with a focus on global practices and security standards. The course is suitable for those entering the field of information security or developing their careers in this growing field

Overall Program Objective:

Understand the concept of cybersecurity and its importance in the digital age.
Identify types of cyberattacks and how to protect against them.
Learn the basic principles of securing networks and systems.
Acquire encryption skills and protect sensitive data.
Identify cybersecurity tools and platforms in the digital age.
Become familiar with security policies.

Detailed Program Objectives:

By the end of the course, graduates will be able to competently understand:

- Introduction to Cybersecurity:
Basic concepts.
The difference between information security and cybersecurity.
The importance of cybersecurity at the individual, institutional, and national levels.
- Types of cyberthreats:
Viruses, malware, phishing, denial-of-service attacks, and social engineering.
- Network and infrastructure security:
Firewalls.
Cryptography and key management:
Symmetric and asymmetric encryption.
Digital signatures and security certificates (SSL).
- Cybersecurity tools:
Introduction to tools such as Wireshark, Kali Linux, Nessus, and others.
- Compliance and policies:
Develop security policies within organizations.
- Incident response and breach analysis:
Steps to take when a breach occurs.
Documenting incidents and learning from them.

By the end of the course, the trainee will receive:

- A certificate of attendance accredited by the training institute.
- Comprehensive knowledge of the fundamentals of systems and information security.
- The ability to analyze and respond to cyber threats.