Foundations of Cybersecurity – Course Outline

Course Description

This foundational cybersecurity course is designed for beginners who want to understand the core concepts of cybersecurity. It introduces essential security principles, basic tools, and a few hands-on labs to build practical awareness.

Course Objectives

1 Understand basic cybersecurity concepts and terminology

2 Identify common cyber threats and vulnerabilities

3 Learn basic network and system security principles

4 Gain introductory hands-on experience through guided labs

5 Build a strong foundation for advanced cybersecurity studies

Course Modules

Module 1: Introduction to Cybersecurity
Overview of cybersecurity, importance, career paths

Module 2: Cyber Threats & Attacks
Malware, phishing, social engineering, basic attack methods

Module 3: Networking Basics for Security
IP addressing, ports, protocols, network devices

Module 4: System & Endpoint Security
Operating system security, antivirus, patching basics

Module 5: Introduction to Cyber Defense
Firewalls, access control, authentication fundamentals

Module 6: Basic Cybersecurity Labs
Password security lab, phishing awareness lab, basic network scan

Module 7: Ethics & Best Practices
Cyber ethics, policies, safe online behavior

Module 8: Course Review & Next Steps
Recap, learning paths, certification awareness

Assessment & Completion

Course completion is based on participation, quizzes, and successful completion of introductory labs. A certificate of completion may be awarded.