

## Cybersecurity Fundamentals Course Outline

This course is a beginner-friendly introduction to cybersecurity. It is designed for students, career starters, non-IT professionals, and anyone who wants to understand how to stay safe online. The course also introduces basic digital forensics concepts and cybersecurity awareness for both personal and workplace environments.

Duration: 8 Weeks

Study Time: 4–6 hours per week

Format: Lectures, short readings, quizzes, practical exercises, and a final project

### Course Objectives

- Understand the basic concepts and importance of cybersecurity.
- Identify common cyber threats and how they affect individuals and organizations.
- Develop good cybersecurity habits and awareness for daily digital activities.
- Learn the basics of digital forensics and how cyber incidents are investigated.
- Apply cybersecurity knowledge ethically and responsibly.

### Prerequisites

Basic computer knowledge (using a computer, internet browsing, email).

No prior experience in cybersecurity is required.

### Course Structure

#### Course 1: Basics of Cybersecurity

Key Topics:

- What cybersecurity is and why it is important
- The CIA Triad: Confidentiality, Integrity, and Availability
- Common cyber threats such as viruses, ransomware, and phishing
- Basic security tools including antivirus software, firewalls, and encryption
- Introduction to computer networks and the internet

Learning Outcomes:

- Explain basic cybersecurity concepts
- Recognize common cyber threats
- Understand how basic security tools protect systems

Activities & Assessments:

- Short quizzes
- Discussion of real-world cyber incidents

- Simple threat-identification exercises

## Course 2: Cybersecurity Awareness

### Key Topics:

- Human behavior and cybersecurity risks
- Social engineering and online scams
- Password safety and multi-factor authentication
- Safe internet and email usage
- Introduction to data privacy and protection

### Learning Outcomes:

- Identify and avoid online scams
- Create and manage strong passwords
- Practice safe online behavior

### Activities & Assessments:

- Phishing simulation examples
- Personal cybersecurity checklist
- Group discussions

## Course 3: Basic Digital Forensics

### Key Topics:

- What digital forensics is and why it matters
- Steps in a digital forensic investigation
- Handling and protecting digital evidence
- Basic understanding of file systems
- Introduction to incident response
- Ethical and legal considerations

### Learning Outcomes:

- Describe the digital forensics process
- Understand evidence handling
- Apply ethical guidelines

### Activities & Assessments:

- Basic lab exercises
- Mock investigation scenario
- Short written reflection

#### Course 4: Integration and Final Project

##### Key Topics:

- How cybersecurity awareness helps prevent attacks
- How digital forensics supports investigations
- Basic cloud security concepts
- Cybersecurity career paths and future trends
- Course review

##### Learning Outcomes:

- Combine cybersecurity knowledge into real-world scenarios
- Explain prevention and response strategies

##### Activities & Assessments:

- Final project
- Final assessment or exam
- Optional guest session