1. Understanding the Importance of Data Security

- **Definition**: Data Security protects sensitive information from unauthorized access and ensures data privacy.
- **Importance**:
  - Prevents data breaches and financial losses.
  - Builds trust with customers and stakeholders.
  - Complies with legal regulations (e.g., GDPR, HIPAA).
- **Applications**: Key areas include securing customer information, intellectual property, and business operations.

2. Data Security Concepts

- **Confidentiality, Integrity, Availability (CIA Triad)**:
  - **Confidentiality**: Ensuring only authorized users can access data.
  - **Integrity**: Maintaining accuracy and trustworthiness of data.
  - **Availability**: Ensuring data is accessible when needed.
- **Encryption**: Encoding data so only authorized users can read it.
- **Authentication & Authorization**: Verifying identity and controlling access.
- **Risk Management**: Identifying, evaluating, and mitigating security risks.
- **Common Threats**: Phishing, malware, ransomware, insider threats.