2. Basic Principles of Data Security Concepts

- **Confidentiality**: Ensuring sensitive information is accessed only by authorized users.
- **Integrity**: Keeping data accurate and unaltered during storage, transmission, and handling.
- **Availability**: Making sure data is accessible to authorized users when needed.

Other Key Concepts:

- **Authentication**: Verifying the identity of users.
- **Authorization**: Granting permission to access data or systems.
- **Risk Assessment**: Analyzing potential threats and vulnerabilities to data security.

---

3. Types of Threats

- **Phishing**: Deceptive attempts to steal personal information by pretending to be a trustworthy entity.
- **Malware**: Software designed to harm or exploit any programmable device, service, or network.
- **Ransomware**: A type of malware that threatens to publish or block access to data unless a ransom is paid.
- **Insider Threats**: Risks originating from within the organization, often involving employees or associates.
- **Social Engineering**: Manipulating individuals to reveal confidential information.

---

4. Protection Methods

- **Encryption**: Converting data into code to prevent unauthorized access.
- **Access Control**: Restricting access to sensitive data based on user roles and responsibilities.
- **Firewalls**: Network security devices that monitor and control incoming and outgoing network traffic.
- **Antivirus Software**: Programs designed to detect and remove malicious software.

- **Regular Security Audits**: Routine checks to identify and fix security vulnerabilities.
- **Employee Training**: Educating staff about security risks and safe practices, reducing the risk of human error.