# Cyber Security

Cyber security refers to the practice of protecting systems, networks, and programs from digital attacks.

These attacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money;

or interrupting normal business processes.

### Key Areas of Cyber Security

1. **Network Security** – Protecting network infrastructure from unauthorized access.

2. **Application Security** – Ensuring applications are free of threats and vulnerabilities.

3. **Information Security** – Safeguarding data integrity and privacy.

4. **Operational Security** – Handling and protecting data assets.

5. **Disaster Recovery and Business Continuity** – Ensuring quick recovery after incidents.

### Emerging Trends

- **AI in Cyber Security** – Detecting threats in real-time using machine learning.

- **Zero Trust Security Models** – Eliminating implicit trust in networks.

- **Quantum Cryptography** – Next-generation encryption mechanisms.

Cyber security continues to evolve as attackers become more sophisticated, requiring continuous innovation

and awareness across organizations worldwide.

# Cyber Security

Cyber security refers to the practice of protecting systems, networks, and programs from digital attacks.

These attacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money;

or interrupting normal business processes.

### Key Areas of Cyber Security

1. **Network Security** – Protecting network infrastructure from unauthorized access.

2. **Application Security** – Ensuring applications are free of threats and vulnerabilities.

3. **Information Security** – Safeguarding data integrity and privacy.

4. **Operational Security** – Handling and protecting data assets.

5. **Disaster Recovery and Business Continuity** – Ensuring quick recovery after incidents.

### Emerging Trends

- **AI in Cyber Security** – Detecting threats in real-time using machine learning.

- **Zero Trust Security Models** – Eliminating implicit trust in networks.

- **Quantum Cryptography** – Next-generation encryption mechanisms.

Cyber security continues to evolve as attackers become more sophisticated, requiring continuous innovation

and awareness across organizations worldwide.

# Cyber Security

Cyber security refers to the practice of protecting systems, networks, and programs from digital attacks.

These attacks are usually aimed at accessing, changing, or destroying sensitive information; extorting money;

or interrupting normal business processes.

### Key Areas of Cyber Security

1. **Network Security** – Protecting network infrastructure from unauthorized access.

2. **Application Security** – Ensuring applications are free of threats and vulnerabilities.

3. **Information Security** – Safeguarding data integrity and privacy.

4. **Operational Security** – Handling and protecting data assets.

5. **Disaster Recovery and Business Continuity** – Ensuring quick recovery after incidents.

### Emerging Trends

- **AI in Cyber Security** – Detecting threats in real-time using machine learning.

- **Zero Trust Security Models** – Eliminating implicit trust in networks.

- **Quantum Cryptography** – Next-generation encryption mechanisms.

Cyber security continues to evolve as attackers become more sophisticated, requiring continuous innovation and awareness across organizations worldwide.