Cybersecurity refers to the practice of protecting systems,networks,devices and data from digital threats ,unauthorized access and damages.it involves a combination of technologies ,process and strategies designed to safeguard digital assets,ensuring the confidentiality, integrity and availability of information .

Components of cybersecurity

1. Threat Prevention : Threat prevention refers to strategies and measures put in place to proactively protect systems, networks, and data from potential cyber threats, attacks, or vulnerabilities.
2. Data Protection : Data protection safeguards sensitive information from unauthorized access, loss, or corruption. It involves encryption, access controls, backups, and compliance with regulations to ensure confidentiality, integrity, and availability of data.
3. Network Security : Network security protects networks and data from breaches, intrusions, and threats. It uses firewalls, intrusion detection systems, encryption, and access controls to ensure safe and reliable communication and data transfer.
4. Endpoint Security : Endpoint security protects devices like computers, smartphones, and tablets from cyber threats. It uses antivirus, firewalls, and encryption to secure endpoints and prevent unauthorized access or malware attacks.

5. Cloud Security : Cloud security refers to practices, technologies, and policies designed to protect data, applications, and services hosted in cloud environments from cyber threats, ensuring privacy, integrity, and availability.

6 Risk Management :involves identifying, assessing, and prioritizing risks to minimize the impact of potential threats on an organization. It includes strategies to prevent, mitigate, or accept risks while ensuring business continuity.