



Cyber Security



Cyber Security is the practice of protecting computer systems, networks, and data from unauthorized access, theft, or damage. Cyber security involves various methods, such as encryption, authentication, firewalls, antivirus software, and backup systems.



Ransomware is a type of malware that encrypts a victim's files and demands a ransom in exchange for the decryption key. It is often spread through malicious email attachments, compromised websites, or software vulnerabilities.

Strong Passwords

- Use a combination of upper and lowercase letters, numbers, and special characters.
- Avoid using easily guessable information like birthdays or names.

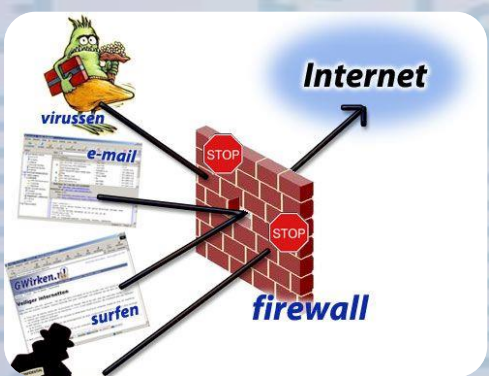


Encryption

- Encrypt sensitive data to protect it from unauthorized access.
- Use strong encryption algorithms and keep encryption keys secure.

Maintaining Backups

- Regularly backing up critical data and systems is essential for efficient recovery in the event of a cybersecurity incident. Backups should be stored securely and tested regularly to ensure their integrity.



Firewalls

- Firewalls act as a barrier between a trusted internal network and an untrusted external network, preventing unauthorized access and protecting against malicious activity.

Secure Wi-Fi Networks

- Using secure Wi-Fi networks with encryption protocols such as WPA2 or WPA3 helps protect sensitive data from interception and unauthorized access.



Prepared by

Huda Abubaker Nahla Muhamma joshken Falah

Supervised by : Omar Nabeel