

Cybersecurity :




Cybersecurity threats are acts performed with harmful intent to steal data, disrupt systems, or cause damage. Common threats include malware, phishing, DDoS attacks, and insider threats. To prevent these, individuals and organizations should implement measures like strong passwords, antivirus software, regular updates, email security, and employee training.




Common Cybersecurity Threats:

Common Cybersecurity Threats:

- **Malware:** Malicious software designed to damage or disable computers and networks.
- **Phishing:** Deceptive attempts to obtain sensitive information like passwords or credit card details.
- **DDoS Attacks:** Disrupting online services by overwhelming them with traffic.
- **Insider Threats:** Unauthorized access or actions from individuals within an organization.

- 
- **Man-in-the-Middle (MITM) Attacks:** Intercepting communication between two parties to steal data.
 -
 - **Social Engineering:** Manipulating people to disclose sensitive information or perform actions.
 -
 - **SQL Injection:** Exploiting vulnerabilities in web applications to access databases.
 -
 - **Ransomware:** Encrypting data and demanding a ransom for its release.
 -
 - **Data Breaches:** Unauthorized access to sensitive data.

- 
- **trong Passwords:** Use unique, strong passwords for each account and consider using a password manager.
 -
 - **Antivirus/Antimalware Software:** Install and keep reputable software updated.
 -
 - **Regular Updates:** Update operating systems, browsers, and other software to patch vulnerabilities.
 -
 - **Secure Networks:** Avoid using public Wi-Fi for sensitive transactions and use a VPN when necessary.
 -

PASSWORD :



- **trong Passwords:** Use unique, strong passwords for each account and consider using a password manager.
-
- **Antivirus/Antimalware Software:** Install and keep reputable software updated.
-
- **Regular Updates:** Update operating systems, browsers, and other software to patch vulnerabilities.
-
- **Secure Networks:** Avoid using public Wi-Fi for sensitive transactions and use a VPN when necessary.
-
-



Prevention technique :

- **Strong Passwords:** Use unique, strong passwords for each account and consider using a password manager.
- **Antivirus/Antimalware Software:** Install and keep reputable software updated.
- **Regular Updates:** Update operating systems, browsers, and other software to patch vulnerabilities.
- **Secure Networks:** Avoid using public Wi-Fi for sensitive transactions and use a VPN when necessary.



SECURITY :

- **Email Security:** Be cautious of unsolicited emails, especially those with links or attachments.
-
- **Employee Training:** Educate employees on cyber threats, phishing, and safe internet practices.
-
- **Multi-Factor Authentication (MFA):** Enable MFA for accounts and services to add an extra layer of security



DATAS :

- **Data Backups:** Implement regular system backups to recover from ransomware or data loss events.
- **Firewalls:** Use firewalls to control network traffic and limit incoming connections.
- **Security Assessments:** Conduct regular security assessments to identify and address vulnerabilities.

RESPONSE :



- **Zero Trust Security:**
Implement a zero-trust security model to minimize lateral movement and restrict access.
-
- **Incident Response Plan:**
Develop a plan for responding to security incidents, including data breaches.



WHAT CYBERSECURITY ?

Cybersecurity threats are acts performed with harmful intent to steal data, disrupt systems, or cause damage. Common threats include malware, phishing, DDoS attacks, and insider threats. To prevent these, individuals and organizations should implement measures like strong passwords, antivirus software, regular updates, email security, and employee training







