Cyber Security

Network Threats

Types of Network Threats

- Social engineering
- Denial of service
- Back door
- IP Spoofing
- SQL Injection
- Man-in-the-middle
  - Definition
    - Man In The Middle refers to when an attacker positions himself in a conversation between a user and an application
    - The Attacker intends to steal personal information (i.e. login credentials, account details, credit card numbers)
  - Examples
    - IP Spoofing
      - This is when the attacker alters a website's IP address and imitates the website. Users would think they're interacting with a trusted website when they are passing information to a malicious user
    - DNS Spoofing
      - This is when a cybercriminal creates and operates a fake website based on a website a user is familiar, and redirects them to the fake website for the cybercriminal to acquire the user's information
    - Wi-Fi Eavesdropping
      - Cybercriminals create public Wi-Fi networks or hotspots that appear to be a nearby business or trusted source.
    - Session Hijacking
      - This is when an attacker steals information stored in a web browser (browser cookies) such as saved passwords.
- Cross-site scripting

Types of malware

- Ransomware
- Viruses
- Rootkits
- Spyware
- Backdoors
- Phishing