

What is Cyber Attacks?

- A cyber attack is a deliberate attempt by hackers to steal, damage, or disrupt computer systems, networks, or data.
- It's like a thief trying different tricks to break into your digital house.
- Example: Sending fake bank emails to steal your login info.

Types of Cyber Attacks



- Phishing 
- Malware 
- Ransomware 
- DDoS Attack 
- Man-in-the-Middle Attack 
- SQL Injection 
- Password Attacks 

Phishing

- Fake emails, messages, or websites trick you into giving personal info (passwords, bank details).
- Example: You get an email “Your bank account will be closed, click here to verify” that link steals your credentials.

Malware

- Malicious software (virus, worm, trojan) installed secretly to harm your system or steal data.
- Example: Downloading a free cracked game that secretly installs a keylogger.

Ransomware

- Hackers lock your files and demand money (ransom) to unlock them.
- Example: A hospital's patient data is encrypted and hackers ask millions to restore it.

DDoS Attack (Distributed Denial of Service)

- Flooding a website/server with huge traffic until it crashes.
- Example: An e-commerce site attacked during a big sale, making it unavailable to customers.

Man-in-the-Middle Attack

- Hacker secretly intercepts communication between two parties.
- Example: Using free public Wi-Fi at a café, a hacker spies on your banking session.

SQL Injection

- Injecting malicious code into a website's database through forms or inputs.
- Example: A hacker types malicious commands in a login box and directly accesses all stored user data.

Password Attacks

- Guessing, stealing, or cracking weak passwords.
- Example: Someone tries “123456” or “password” to break into your account.

Why Understanding These is Important?

- Awareness helps you recognize threats early.
- Prevention measures (strong passwords, antivirus, 2FA, not clicking suspicious links) reduce risks.
- Cyber security careers demand strong knowledge of these attack types.