Types of cyber attacks

Malware

is a term used to describe malicious software, including spyware, ransomware, viruses, and worms. Malware breaches a network through a vulnerability, typically when a user clicks a dangerous link or email attachment that then installs risky software

Phishing

Phishing is the practice of sending fraudulent communications that appear to come from a reputable source, usually through email. The goal is to steal sensitive data like credit card and login information or to install malware on the victim's machine.

Password Attack

It is a form of attack wherein a hacker cracks your password with various programs and password cracking tools like Aircrack, Cain, Abel, John the Ripper.

Man-in-the-middle attack

Man-in-the-middle (MitM) attacks, also known as eaves dropping attacks, occur when attackers insert themselves into a two-party transaction. Once the attackers interrupt the traffic, they can filter and steal data.

Denial-of-service attack

A denial-of-service attack floods systems, servers, or networks with traffic to exhaust resources and bandwidth. As a result, the system is unable to fulfill legitimate requests. Attackers can also use multiple compromised devices to launch this attack

SQL Injection Attack

A Structured Query Language sql injection attack occurs on a database-driven website when the hacker manipulates a standard SQL query. It is carried by injecting a malicious code into a vulnerable website search box, thereby making the server reveal crucial information.

This results in the attacker being able to view, edit, and delete tables in the databases. Attackers can also get administrative rights through this.