Common types of cyber attacks

htlp.com.au

Malware

Malware refers to software that is unknowingly installed onto a device, typically by clicking a dangerous link or email attachment. This can include viruses, ransomware, spyware and other harmful bugs that may allow the hacker to collect and send confidential information and damage the device.

Phishing

Phishing is the practice of sending fraudulent communications (often emails) that come from a seemingly reliable source. Once clicking on the link, malicious malware will be installed onto the device, giving the hacker access to sensitive information...

SQL Injection Attack

A Structured Query Language (SQL) injection attack is where an attacker inserts malicious code into a SQL server, forcing the server to reveal information that would otherwise be unauthorised. If the attack is successful, the hacker can access, delete, steal, recover and modify sensitive information stored on the server.

Cross-Site Scripting (XXS)

Like a SQL attack, this also involves injecting malicious code into a website but it only runs in the user's browser when they visit the attacked website, and it goes after the visitor directly. Hackers use third-party web resources to execute scripts in a person's scriptable program or web browser.

Denial-of-Service (DDoS)

In this type of attack, hackers overload systems, servers, or networks with enough traffic to exhaust resources, rendering them unresponsive to service requests from website users.

Man-in-the-Middle (MITM)

MITM attacks occur when attackers insert themselves in a two party transaction so that they can interrupt the traffic, and filter and steal data. This type of attack is particularly vulnerable when using unsecured wifi networks or devices that already have malware installed on them.