Man in the middle

This method only requires the attacker to stand between the two parties trying to communicate; intercepting the messages sent and imitating at least one of them. The attacker stands between the target and the source; going totally unnoticed in order to successfully reach the goal.

Ramsomware

Ransomware, or also Encryption Trojan or Blackmail Trojan, is a malicious program for computers, which ensures that the device is locked for the user and can only be unlocked again with a ransom.

Adware

Adware is unwanted software designed to display advertisements on your screen, usually in a browser. Some security professionals see it as a precursor to today's PUPs (Potentially Unwanted Programs).

Phishing

Phishing is the crime of tricking people into sharing sensitive information like passwords and credit card numbers. Victims receive an email or text message that impersonates (or “spoofs”) a trusted person or organization, such as a co-worker, a bank, or a government office. When the victim opens the email or text message, she finds a message designed to scare her, with the intention of impairing her judgment by instilling fear. The message demands that the victim go to a website and act immediately or face consequences.

Doxing

Doxing is revealing identifying information about a person online, such as their real name, home address, place of work, phone number, financial data, and other personal information. This information is then released to the public without the victim's permission.

DDos

This type of attack takes advantage of specific capacity limits that apply to any network resource, such as the infrastructure that enables the company's website. The DDoS attack sends multiple requests to the attacked web resource, with the intention of overwhelming the website's ability to handle multiple requests and preventing the website from working properly.

Whaling

Pretend to hold senior positions in an organization and thus directly attack senior executives or other important people within it, in order to steal money, obtain confidential information or gain access to their computer systems for criminal purposes.

SQLinjection

Vulnerability that allows the attacker to send or "inject" SQL instructions in a malicious and malicious way within the SQL code programmed for the manipulation of databases, in this way all the stored data would be in danger.

XSS

Cyberattack by which vulnerabilities are searched for in a web application to introduce a harmful script and attack its own system, starting from a trusted context for the user. Scripts are scripts or programs written in programming languages such as JavaScript that are executed in the web browser. In its most innocuous version, pop-up windows are executed and, in the worst cases, they are used by attackers to access sensitive information or the user's computer.