# DNS spoofing

It is the process of altering entries in a DNS server to redirect a specific user to a malicious website that is under the attacker's control. It usually occurs in a public Wi-Fi network environment, but it can also occur in any situation and the attacker can alter the ARP tables and force the user's devices to use the attacker-controlled equipment as a server for a specific web page.

## What does it consist of?

Cybercriminals can use tools to perform DNS spoofing. Generally, public Wi-Fi networks tend to be the main points of attack, since they are not well configured and often have deficiencies in protection. Therefore, it gives cybercriminals more opportunities to carry out the desired action. That is why it is always recommended to think about the security of Wi-Fi networks, both private and public. But it is important to understand that it is not only limited exclusively to public networks and this can occur in other network environments if the attacker manages to position himself in the path of DNS communication.

## Why is this a problem?

Since users are often targeted by DNS spoofing attacks, they pose a threat to data privacy. The page to spoof depends on the attacker's goals. For example, if an attacker wants to steal banking information, the first step would be to find a popular banking website, download the code and style files, and upload them to the malicious computer used to hijack connections. Most attackers test and verify that the spoofed page is well done, but occasionally there are small errors that give away that the page is being spoofed.