CYBER CURE⁺
cyber security starts with us

July 25 2023

Spoofing: Unveiling the deceptive world of digital impersonation

Spoofing is a dishonest method used by people or cybercriminals where information is manipulated to look legitimate or come from a trustworthy source, but it's fake. There are various types of spoofing, each targeting different areas of technology and communication. Here are some common types of spoofing

Email Spoofing

You receive a deceptive email to make it appear as if it's from a trustworthy source, this is often used in phishing attacks to trick you or your kaimahi into revealing sensitive information or clicking on malicious links.

Caller ID spoofing

You receive a call on your mobile from a local or trusted number, but the attacker has changed the information that shows up on your phone's caller ID to hide their identity and trick you or your kaimahi into answering. This method is used for Robocalling and Social engineering.

Website Spoofing

An attacker creates a fake website that imitates a legitimate site to deceive you or your kaimahi into entering sensitive or confidential information, such as login credentials or payment details.

IP Spoofing

An attacker alters the source IP address in a data packet to make it appear as if the data is coming from a trusted source. This technique is commonly used in denial-of-service (DoS) attacks and other network-based attacks to hide the attacker's identity and location.