Spoofing Definition

Spoofing is the act of disguising a communication from an unknown source as being from a known, trusted source. Spoofing can apply to emails, phone calls, and websites, or can be more technical, such as a computer spoofing an IP address, Address Resolution Protocol (ARP), or Domain Name System (DNS) server.

Spoofing can be used to gain access to a target’s personal information, spread malware through infected links or attachments, bypass network access controls, or redistribute traffic to conduct a denial-of-service attack. Spoofing is often the way a bad actor gains access in order to execute a larger cyber attack such as an [**advanced persistent threat**](https://www.forcepoint.com/cyber-edu/advanced-persistent-threat-apt) or a [**man-in-the-middle attack**](https://www.forcepoint.com/cyber-edu/man-in-the-middle-attack).

Successful attacks on organizations can lead to infected computer systems and networks, data breaches, and/or loss of revenue—all liable to affect the organization’s public reputation. In addition, spoofing that leads to the rerouting of internet traffic can overwhelm networks or lead customers/clients to malicious sites aimed at stealing information or distributing malware.

How Spoofing Works

Spoofing can be applied to a number of communication methods and employ various levels of technical know-how. Spoofing can be used carry out [**phishing attacks**](https://www.forcepoint.com/cyber-edu/phishing-attack), which are scams to gain sensitive information from individuals or organizations.

Email Spoofing

Email spoofing occurs when an attacker uses an email message to trick a recipient into thinking it came from a known and/or trusted source. These emails may include links to malicious websites or attachments infected with malware, or they may use [**social engineering**](https://www.forcepoint.com/cyber-edu/social-engineering) to convince the recipient to freely disclose sensitive information.

Sender information is easy to spoof and can be done in one of two ways:

* Mimicking a trusted email address or domain by using alternate letters or numbers to appear only slightly different than the original
* Disguising the ‘From’ field to be the exact email address of a known and/or trusted source

Caller ID Spoofing

With caller ID spoofing, attackers can make it appear as if their phone calls are coming from a specific number—either one that is known and/or trusted to the recipient, or one that indicates a specific geographic location. Attackers can then use social engineering—often posing as someone from a bank or customer support—to convince their targets to, over the phone, provide sensitive information such as passwords, account information, social security numbers, and more.

Website Spoofing

Website spoofing refers to when a website is designed to mimic an existing site known and/or trusted by the user. Attackers use these sites to gain login and other personal information from users.

IP Spoofing

Attackers may use IP (Internet Protocol) spoofing to disguise a computer IP address, thereby hiding the identity of the sender or impersonating another computer system. One purpose of IP address spoofing is to gain access to a networks that authenticate users based on IP addresses.

More often, however, attackers will spoof a target’s IP address in a denial-of-service attack to overwhelm the victim with traffic. The attacker will send packets to multiple network recipients, and when packet recipients transmit a response, they will be routed to the target’s spoofed IP address.

ARP Spoofing

Address Resolution Protocol (ARP) is a protocol that resolves IP addresses to Media Access Control (MAC) addresses for transmitting data. ARP spoofing is used to link an attacker’s MAC to a legitimate network IP address so the attacker can receive data meant for the owner associated with that IP address. ARP spoofing is commonly used to steal or modify data but can also be used in denial-of-service and man-in-the-middle attacks or in session hijacking.

DNS Server Spoofing

DNS (Domain Name System) servers resolve URLs and email addresses to corresponding IP addresses. DNS spoofing allows attackers to divert traffic to a different IP address, leading victims to sites that spread malware.