What is spoofing?

Spoofing is faking the source of a communication so it appears to come from a trusted party: a forged email sender, a lookalike domain, a faked caller ID, or a spoofed IP or website. It is the enabler behind phishing and fraud. The defenses are authenticating the source (email SPF, DKIM, and DMARC; HTTPS; DNSSEC) and verifying unexpected requests on a channel you already trust.

HOW IT WORKS

01 How spoofing enables attacks

Spoofing is rarely the whole attack; it is the part that makes the rest believable. Phishing works because the sender looks real. Business email compromise works because the request appears to come from your CEO. Fraudulent sites harvest credentials because the address looks right.

In other words, spoofing supplies the trust that social engineering spends. Break the spoofing, and most of these attacks lose their disguise.

02 How to spot spoofing

The signs are usually small mismatches:

- The display name looks right but the actual email address or domain is off by a character.
- Email authentication (SPF, DKIM, DMARC) is missing or failing, which your mail provider can flag.
- A website's certificate warning, or a URL that is a lmost, but not quite, the real one.
- A call or message asking for something unusual from a number you cannot independently confirm.

When in doubt, do not trust the channel that contacted you; reach the person or company through details you already have.

HOW TO DEFEND

- Email authentication: publish SPF, DKIM, and DMARC so receivers can reject mail that forges your domain, and enforce DMARC over time.
- Register lookalike domains and monitor Certificate Transparency logs for new certificates that impersonate you.
- HTTPS and HSTS so users reach the real you and browsers refuse downgrades.
- DNSSEC and network anti-spoofing where applicable.
- A second-channel rule for any request that moves money or changes access.

SOURCES

[1] Phishing and Spoofing

[2] Impersonation (Technique T1656)

[3] Computer Security Resource Center Glossary

Find out whether an attacker can send mail as you.

securelayer7.net/learn/threats/spoofing

Open online