SPF Records

What are they

Sender Policy Framework or SPF records are used to prevent cybercriminals from pretending to send emails from your domain name (known as spoofing).

Recipient email servers can use the SPF record you publish in your DNS to determine whether an email they have received has come from an authorised or trusted place. Email filters will often use this as a method of determining whether an email is spam or not.

Why they are important

Not having an SPF record leaves you vulnerable to spoofing attacks. It also presents the risk of your emails being marked as spam by the recipients' email filter, and the recipient not receiving your email.

What is the risk of not having them

Email spoofing is when a cybercriminal sends emails with false sender addresses, which typically forms part of a phishing scam.

These types of attacks are designed to steal your information, infect your computer with malware, or ransomware. These emails may also use social engineering to convince the victim to freely disclose sensitive information.

How to set them up

An SPF record is a simple entry in your DNS records, your IT team will be able to add one in for you.