DMARC, SPF, DKIM

What is DMARC?
DMARC stands for Domain-based Message Authentication, Reporting & Conformance. It's an email authentication protocol that helps protect your domain from being used to send unauthorised emails, a practice known as email spoofing. Think of it like a three-pronged approach to email security:

- **Authentication:** DMARC relies on two other email authentication protocols, SPF (Sender Policy Framework) and DKIM (DomainKeys Identified Mail). SPF verifies that the email is coming from an authorised server, while DKIM adds a digital signature to the email to ensure it hasn't been tampered with.
- **Policy:** Once DMARC has determined whether an email is authenticated, it tells receiving mail servers what to do with it, if it fails authentication. The policy can range from simply rejecting the email to quarantining it or marking it as spam.
- **Reporting:** DMARC also provides reporting so you can see which emails are being sent from your domain and whether they are authenticated. This can help identify any unauthorised use of your domain and take steps to prevent it.

What is SPF and DKIM?
SPF and DKIM are two other email authentication protocols that work alongside DMARC to prevent email spoofing and protect your domain from unauthorised use. Here's a breakdown of each:

SPF (Sender Policy Framework)

- Imagine a whitelist for email senders. SPF allows you to specify which servers are authorised to send email on behalf of your domain. This is achieved by publishing a TXT record in your DNS zone file. The record lists all the IP addresses or domains that are allowed to send emails for your domain.
- When an email is received, the receiving server checks the SPF record for the domain in the email address. If the IP address of the sending server is listed in the SPF record, the email is considered to be authenticated. If the IP address is not listed, the email may be rejected or flagged as spam.

DKIM (DomainKeys Identified Mail):

- Think of it like a digital signature for your emails. DKIM adds a cryptographic signature to the header of your emails. This signature is generated using a private key that is only known to you. The public key is published in a DNS record for your domain.
- When an email is received, the receiving server verifies the signature using the public key. If the signature is valid, it means that the email was signed with the private key and therefore came from your domain. If the signature is invalid, the email may be rejected or flagged as spam.