**SPF, DKIM, and DMARC – Simple Explanation**

These are security measures used to **prevent email spoofing** (fake emails pretending to be from a trusted source).

**1. SPF (Sender Policy Framework) – Who Can Send Emails?**

* SPF tells email providers **which servers are allowed** to send emails on behalf of a domain (e.g., Gmail, Yahoo).
* If an email comes from an **unauthorized server**, it might be marked as **spam or rejected**.

🔍 **How to check SPF?**

* Run this command in your terminal:
* nslookup -type=TXT example.com
* Look for a record starting with **"v=spf1"**.

**2. DKIM (DomainKeys Identified Mail) – Is the Email Genuine?**

* DKIM adds a **digital signature** to emails.
* This signature allows the receiver to check if the email was **tampered with** during transmission.

🔍 **How to check DKIM?**

* Run this command (replace "default" with the selector if needed):
* nslookup -type=TXT default.\_domainkey.example.com
* If DKIM is set up correctly, you’ll see a long key in the response.

**3. DMARC (Domain-based Message Authentication, Reporting, and Conformance) – What to Do with Fake Emails?**

* DMARC tells email providers **what to do** if SPF and DKIM fail.
* It can **allow, quarantine, or reject** emails that don’t pass SPF/DKIM.

🔍 **How to check DMARC?**

* Run this command:
* nslookup -type=TXT \_dmarc.example.com
* Look for a record starting with **"v=DMARC1"**.

**Why Are These Important?**

✔ Protects your domain from being used for phishing.  
✔ Increases email deliverability (your emails won’t go to spam).  
✔ Helps email providers identify and block fake emails.

**How Do They Help?**

**SPF** – Checks if the email was sent from an allowed server.

* **If SPF fails**, the email might be fake.

**DKIM** – Ensures the email wasn’t modified after being sent.

* **If DKIM fails**, the email might be altered or forged.

**DMARC** – Tells email providers what to do if SPF or DKIM fail.

* **If both SPF & DKIM fail**, the email can be rejected or marked as spam.