📧 The Basics: Why These Exist

When you receive an email, you want to know:

"Is this really from who it says it's from?"

"Has the message been tampered with?"

"Should I trust it?"

To help answer those questions, email systems use:

✅ SPF – Who is allowed to send emails from this domain?

✅ DKIM – Has this email been altered in transit?

✅ DMARC – What should we do if SPF or DKIM fails?

1. SPF – Sender Policy Framework

What it does:

SPF checks if the server that sent the email is authorized to send email for that domain.

Think of SPF like a bouncer checking the guest list for who’s allowed to send mail as example.com.

🚫 SPF Failure:

Means the sender was not on the list of approved servers.

Why this matters:

If a phishing attacker sends an email from a random server pretending to be paypal.com, SPF can catch it — if configured properly.

2. DKIM – DomainKeys Identified Mail

What it does:

DKIM adds a digital signature to the email, signed with the sender's private key.

Think of DKIM like a wax seal on a letter. If it's missing or broken, the message might’ve been tampered with or forged.

What DKIM Actually Does:

DomainKeys Identified Mail (DKIM) adds a digital signature to an email. This signature is:

* Generated using a private key owned by the sending domain (not necessarily the individual sender).
* Verified by retrieving the corresponding public key from the sending domain's DNS records (\_domainkey.example.com).

***🚫 DKIM Failure:***

***Means the signature is missing or doesn’t match — maybe someone altered the message, or it wasn’t signed properly.***

3. DMARC – Domain-based Message Authentication, Reporting, and Conformance

What it does:

DMARC tells the receiver:

“If SPF or DKIM fails, here’s what you should do — reject, quarantine, or accept.”

It also allows domain owners to get reports of who is sending mail on their behalf.

🚫 DMARC Failure:

Means both SPF and DKIM failed, and the email didn't pass alignment rules.

Why this matters:

A failed DMARC is a red flag — it often signals a spoofed or phishing email.

**SUMMARY: WHAT TO WATCH FOR**

**Protocol Checks Failure Means Real-World Risk**

**SPF IP of sender Not allowed to send Possible spoof**

**DKIM Signature Message tampered or forged Integrity risk**

**DMARC Policy & alignment SPF + DKIM failed High phishing risk**

**Real-Life Application:**

**Say someone spoofs** [**bank.com**](bank.com) **by sending from a random mail server:**

* **SPF fails (server not authorized)**
* **DKIM fails (no valid signature from bank.com)**
* **DMARC = reject → The message is dropped or marked as spam.**

**But if a scammer registers** [**bank-secure.com**](bank-secure.com) **and signs using that domain’s DKIM, the message might pass DKIM—but not pass DMARC if the From: is still** [**bank.com**](bank.com)**, because there's no alignment.**