* **Domain Name System (DNS):** This system is essentially the phone book of the Web that organizes and identifies domains.

While a phone book translates a name like "Acme Pizza" into the correct phone number to call, the DNS translates a web address like "www.google.com" into the physical IP address—such as"74.125.19.147"—of the computer hosting that site (in this case, the Google homepage).

When using Google Cloud services, you periodically need to modify your DNS settings to set up various tools and services. You do this by changing various types of DNS records.

* **Sender Policy Framework (SPF)**: SPF is an email authentication standard that helps protect senders and recipients from spam, spoofing, and phishing.

By adding an SPF record to your Domain Name System (DNS), you can provide a public list of senders that are approved to send email from your domain. Receiving servers can then cross-check that email originated from a server with permission to send on your domains’ behalf.

**SPF record works:** At a high level, here is the workflow of how a mail server checks SPF:

1. The server with the IP address of 1.2.3.4 sends an email, and that email is using bounces@example.com as the Return-Path.
2. The receiving mail server grabs the Return-Path domain and checks out the domain’s DNS records for example.com, looking for the SPF record.
3. The receiving server found the SPF record for example.com! Now, it checks if any of the IP addresses listed as valid senders for the domain match the address that was used to send the email.
4. In this example, it’s a match! The sending IP 1.2.3.4 is listed as an approved sender, so SPF passes. If the IP addresses don’t match, that would cause SPF to fail. This would likely make the receiving server suspicious, and they might reject the mail.

**To implement an SPF record on my domain**

1. Understand your Return-Path

2. Create your SPF record

3. Update your domain’s DNS settings

* **DomainKeys Identified Mail (DKIM):** DKIM is an email security standard that helps detect whether messages are altered in transit between sending and receiving mail servers.

DKIM authentication uses public-key cryptography to sign email with a responsible party’s private key as it leaves a sending server; recipient servers then use a public key published to the DKIM’s domain to verify the source of the message, and that the parts of the message included in the DKIM signature haven’t changed since the message was signed. Once the signature is verified with the public key by the recipient server, the message passes DKIM and is considered authentic.

**DKIM works:** Uses two actions to verify your messages:

* The first action takes place on a server sending DKIM signed emails
* The second happens on a recipient server checking DKIM signatures on incoming messages.

The entire process is made possible by a private/public key pair. Your private key is kept secret and safe, either on your own server or with your ESP, and the public key is added to the DNS records for your domain to broadcast it to the world to help verify your messages.

* **Domain-based Message Authentication, Reporting & Conformance (DMARC):** DMARC is a standard that prevents spammers from using your domain to send email without your permission — also known as spoofing.

Spammers can forge the “From” address on messages, so the spam appears to come from a user in your domain. A good example of this is PayPal spoofing, where a spammer sends a fraudulent email to you pretending to be PayPal in an effort to obtain your account information. DMARC ensures these fraudulent emails get blocked before you even see them in your inbox.

In addition, DMARC gives you great visibility and reports into who is sending email on behalf of your domain, ensuring only legitimate email is received. DMARC is open and free for anyone to use, allowing you to secure your domain’s emails and gain control of your email delivery.

With SPF and DKIM, it is up to the ISP to decide what to do with the results. DMARC takes it a step further and gives you full control to set a policy to reject or quarantine emails from sources you do not know or trust, all based on the results of DKIM and SPF.

For instance, since PayPal is a huge target for email fraud, they publish a DMARC record that says if DKIM or SPF fails, reject the message. Participating ISPs will look at this policy and discard the emails that fail. In the 2013 holiday season, DMARC helped PayPal stop an estimated 25 million attacks according to a report by Agari.

**DMARC is a key component of a brand ‘s email security and deliverability strategy as it enables:**

1. **Visibility** - Monitor emails sent using your domain to ensure they are properly authenticated using SPF and/or DKIM.
2. **Brand Protection** - Block spoofed messages that might damage your brand ‘s reputation with customers.
3. **Security** - Prevent users from falling victim to phishing scams that could compromise your organization ‘s security.

**Diagram

Description automatically generated Diagram

Description automatically generated Diagram

Description automatically generated**