**Understanding SPF record and how to use it**

A sender policy framework or SPF record is a particular kind of DNS txt record that makes a list of all the servers that are approved to send emails from a particular domain. A DNS txt record permits a domain administrator to put any random text into the Domain Name System or DNS. The primary concern behind introducing text records was to include significant notices about the domain, but with each passing day, it has developed for other purposes as well. These records were primarily created since the standard protocol which was used for email, known as the Simple Mail Transfer Protocol (SMTP) does not essentially authenticate the “from” address in an email which means that without SPF or any other authentication records, a cyber attacker can very fondly and easily imitate a sender and bluff the recipient into taking different actions or share confidential and sensitive information they otherwise would not.

SPF records are one kind of DNS-based mechanism that helps email servers to confirm if an email comes from a trusted source or a fraud party. Domain-based Message Authentication Reporting and Conformance or DMARC and DomainKeys Identified Mail or DKIM are two other mechanisms that are used for email authentication and verification.

**Why are they used?**

There are different reasons why SPF records are used. These are enlisted as follows.

**1)Prevention of attack**

If any of the emails are not authenticated and validated, companies and email recipients stand at risk for various types of phishing attacks, spam emails, email spoofing, etc. With the help of SPF records, it is comparatively difficult for attackers to copy a domain, thereby reducing the chances of occurrence of these attacks.

**2)Improvement of email deliverability**

Domains that are without a published SPF record have a chance of their emails getting bounced or marked as spam. With time, these bounced emails or emails which are marked as spam can disappoint a domain’s ability to reach its target audience’s inboxes, compromising efforts to communicate with all the customers, employees, and other entities.

**3)DMARC compliance**

DMARC is a kind of email validation system that helps to make sure that all emails are sent only by authorized users. DMARC policies dictate what servers should do with emails that do not surpass SPF and DKIM checks and what they should not do. Based on the instructions of the DMARC policy, those emails will either be marked as spam, rejected, or delivered as normal. Administrators get reports about their email activity that help them make necessary adjustments to their policy.

**How to use SPF record by setting it up**

To use SPF records properly and efficiently, the foremost important thing is to set them up. SPF records can be set up in a few steps. These are enlisted as follows.

**1. Gathering of IP addresses for sending email**

The first and primary step to using SPF is to recognize all the mail servers which are used to send email from the user’s domain. Many organizations send mail from a wide variety of locations. All those mail servers and IP addresses have to be taken care of and noted down.

**2. Making a list of sending domains**

A list of all the domains which are used for sending emails has to be noted down.

﻿

**3. Creating of SPF record**

After noting down all the domains, an SPF record needs to be created.

**4. Publishing to SPF**

After the SPF is created, it needs to be published in the DNS server so that all the mailbox providers can reference the SPF record which will be beneficial.

**5. Testing**

In the last step, the created SPF record should be checked with an SPF check tool.

**References**

1)<https://www.validity.com/blog/how-to-build-your-spf-record-in-5-simple-steps/>

2)<https://www.dmarcanalyzer.com/spf/>

3)<https://www.cloudflare.com/en-in/learning/dns/dns-records/dns-spf-record/>

4)<https://dmarcian.com/what-is-spf/>

5)<https://postmarkapp.com/guides/spf>

6)<https://www.sparkpost.com/resources/email-explained/spf-sender-policy-framework/>

7)<https://mailtrap.io/blog/spf-records-explained/>