

SPF

Sender Policy Framework



What does a SPF record do?

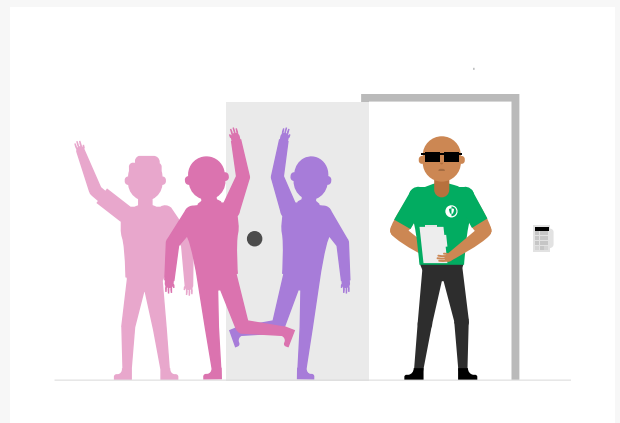
SPF stands for Sender Policy Framework and was developed to help fight sender address forgery by comparing the sending server's IP address to a list of authorized senders.

How does a SPF record work?

The authorized senders are the IP addresses which are allowed to send on behalf of the sending domain. They are specified in a TXT record which is published in the domain owner's DNS.

In other words...

Think of SPF record like a guest list at an email "party" - the IP address of the email sender has to be on the guestlist issued by the domain owner to pass.



What does a SPF record look like?

When you add an SPF record, you're simply adding it as a TXT record to your domain's DNS, it'll look something like this:

```
TXT @ "v=spf1 a include:_spf.google.com ~all"
```

The "include" part of the record will vary depending on the email sending services you use.

Why might your SPF record break?

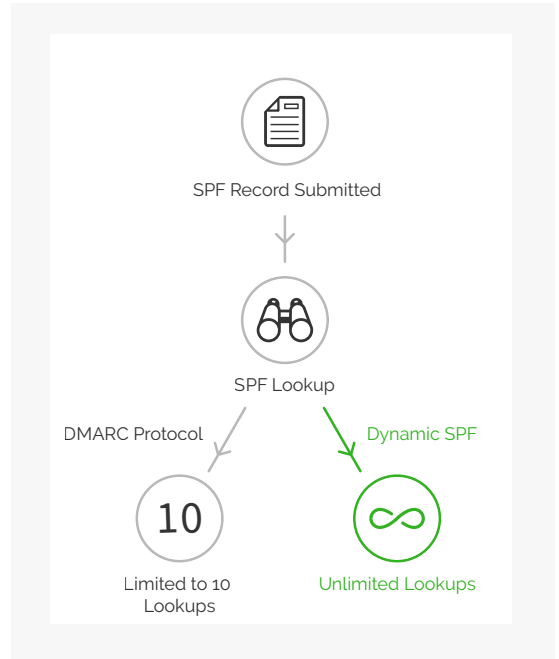
One of the main reasons the SPF record might be failing for your email traffic is the “too many DNS lookups” error.

The SPF specification limits the number of DNS lookups to 10. If your SPF record results to more than 10 DNS lookups then SPF will fail. The SPF mechanisms counted towards DNS lookups are: a, ptr, mx, include, redirect and exists. “ip4”, “ip6” and “all” do not count towards the lookup limit.

In other words...

If that all sounds a bit too technical, think about it this way. G Suite alone takes up 4 DNS lookups, add in Hubspot for marketing which uses 7 lookups then you'll already be over the 10 lookup limit!

As soon as you go over 10 SPF lookups, your email traffic will begin to randomly fail validation. This is where OnDMARC's “Dynamic SPF” feature is invaluable as it gives you an almost limitless number of SPF lookups.



Download the Dynamic SPF datasheet

Learn about the problems people often encounter when deploying SPF and how OnDMARC's Dynamic SPF can solve them for you.

[Find out more](#)



RED SIFT

The Red Sift Open Cloud is a data analysis platform that is purpose-built for the challenges of cybersecurity. By harnessing the power of AI we can securely collate, compute & visualize data from thousands of individual signals to help organizations to optimize their cybersecurity.

Products on the platform include OnDMARC and OnINBOX, SaaS applications that work together to close the net on the phishing problem by blocking outbound phishing attacks and analyzing the security of inbound communications for company-wide email threat intelligence.

- www.ondmarc.redsift.com
- contact@redsift.com
- [@redsift](https://twitter.com/redsift)