ONDMARC by RED SIFT

Dynamic SPF

An innovative solution that delivers simplified SPF management for flawless DMARC validation.

What's the problem?

DMARC works by telling inboxes what to do with an email it receives - deliver, quarantine or reject - based on the outcome of 2 authentication protocols: DKIM and SPF. For some organizations their SPF, Sender Policy Framework, can fail to work properly, which in turn means DMARC doesn't work properly and genuine email traffic can be rejected.

In fact, even if you're not looking to deploy DMARC you should! This limit can result in sporadic and hard to investigate SPF failures that significantly affect the deliverability of your email. Regardless of the size of your company, you want people to read your emails and you certainly don't want to be labeled as a spammer!

How does this happen?

SPF is the mechanism by which a receiving server checks the email has been sent from authorized IP addresses and domains. The protocol looks at your public SPF record to see what those IP addresses are and compares them to the one from which the email originated.

However, the problem is that the SPF protocol has a DNS lookup limit of 10. This was built in to reduce the potential for highly amplified Denial of Service (DoS) attacks against the internet's DNS infrastructure.

If you have more than 10 SPF entries then you run the risk of the receiving mailbox missing an associated IP address and recording the SPF check as failed - either rejecting or quarantining your email.

Dynamic SPF is a OnDMARC feature that allows you to have more than 10 DNS lookups and simplifies SPF management.

How common is this problem?

Most organizations use a number of different mail service providers - G Suite for business email, MailChimp for marketing emails, Salesforce for customer emails - and each one needs to be added to the organization's DNS in order to authenticate the emails as genuine using SPF.

However, this can easily breach the 10 DNS lookup limit imposed by SPF as each mail service is added as a domain which results in 1 or more lookups. This is because SPF resolves domains into multiple IP addresses, for example G Suite alone takes 4 DNS lookups.

Once your SPF record exceeds the 10 lookup limit, your email SPF validation will start to fail affecting the deliverability of your authorized emails.

This is when some people turn to something called "SPF flattening".

Key Benefits

Clicks not code

- Dynamic SPF removes the need for you to have the technical knowledge required to write complex SPF records and manually edit your DNS.
- Simply configure your required services from within the OnDMARC app.

SPF that's always correct

- The clue is in the name, Dynamic SPF automatically ensures every record for all 3rd party services is up to date at point of query, there's no static code to become outdated or obsolete.
- Dynamic SPF works with any existing mail service or ISP.

www.ondmarc.com
contact@redsift.com
@redsift

Why isn't static SPF flattening the answer?

Put simply, static SPF flattening isn't a reliable solution.

To understand why, we need to look at "include" statements. An "include" is an SPF mechanism that points to a domain to be queried when the receiver checks if the sending IP is allowed or not. If the sending IP is part of the "include" then it results in a match and SPF passes.

What SPF flattening does is instead of using "include" statements to refer to the domains, the IP addresses behind them are put as part of the SPF record itself.

This is problematic because:

1. IP addresses often change and by not using "include" statements (which take care of IP address changes), your SPF record is likely to quickly become outdated leading to email deliverability failures.
2. Simple SPF flattening can expand the size of the SPF records due to necessary duplications in the code, this in turn causes new problems.

Why is Dynamic SPF the solution?

Dynamic SPF is a OnDMARC feature that allows you to have more than the normally available number of authorized services using the SPF authentication mechanism. We give you a record that replaces all your mechanisms with a single include that dynamically combines all your authorized services correctly at the point of query. This prevents your authorized traffic from failing SPF validation.

How easy is it to set up Dynamic SPF with OnDMARC?

Super simple. Once your OnDMARC account is set up you simply add your SPF records (also known as 'includes') directly from your dashboard in the Dynamic SPF feature. Once added, just click to copy the string provided by us and paste it into your own SPF record. OnDMARC will automatically detect that you've included this in your DNS and shows you a green light to verify - nice work!

Dynamic SPF automatically ensures every record for all third party services is up to date at point of query, there's no static code to become outdated or obsolete.

Get in touch today to find out more about how you can use OnDMARC to combat phishing and boost email deliverability.

IS 672913

IS 672913

ONDMARC

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.

Our first product on the Red Sift platform is OnDMARC, a SaaS product that helps to implement and maintain DMARC. This email authentication protocol effectively blocks phishing attacks and increases the deliverability of genuine emails.

www.ondmarc.com
contact@redsift.com
@redsift