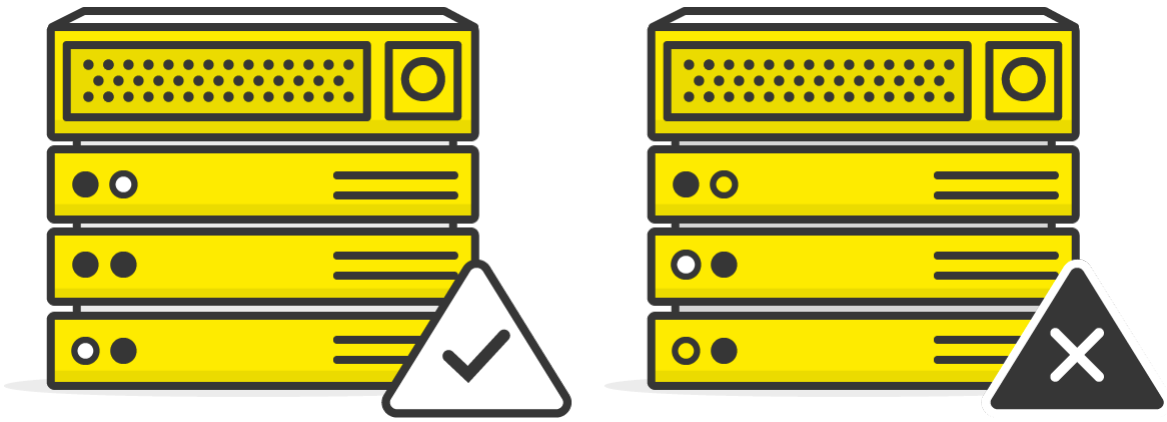
LOG IN

SPF Record: Protect your domain reputation and email delivery



Garrett Dimon
November 10th 2020

The battle against spam and email scams is never-ending. As a result, several standards have evolved to help stem the tide. An SPF record, or “Sender Policy Framework” is one of those standards. It enables a domain to publicly state which servers may send emails on its behalf. You don't have to understand every detail of SPF records to use it, but a deeper knowledge can help you see the bigger picture. Let’s see how you can protect your domain’s reputation and improve your email deliverability.

Jump to

Help

What is an SPF record?

SPF is an open standard that enables the owner of a domain to provide a public list of approved senders. For instance, if you use an email API like Postmark to send your transactional email and then use Campaign Monitor to send your marketing emails, you will include both of those services as approved senders. This way, receiving mail servers can cross-check that the email originated from a server that has permission to send on your behalf. If the message originates from a server that's not on your list, then the receiving server can consider it fake and treat it accordingly.

An important aspect to understand about SPF is that it does not validate against the `From` domain. Instead, SPF looks at the `Return-Path` value to validate the originating server. `Return-Path` is the email address that receiving servers use to notify the sending mail server of delivery problems, like bounces. So an email can pass SPF regardless of whether the `From` address is fake. The problem with this limitation is that the `From` address is what recipients see in their email clients. Furthermore, even if a message fails SPF, there's no guarantee it won't be delivered. That final decision about delivery is up to the receiving ISP.

SPF is just one of many factors that ISPs use to determine whether an email should be delivered. When it comes to verifying the `From` address, DMARC is a relatively new standard designed to address this shortcoming in SPF.

Why should I add an SPF record to my domain?

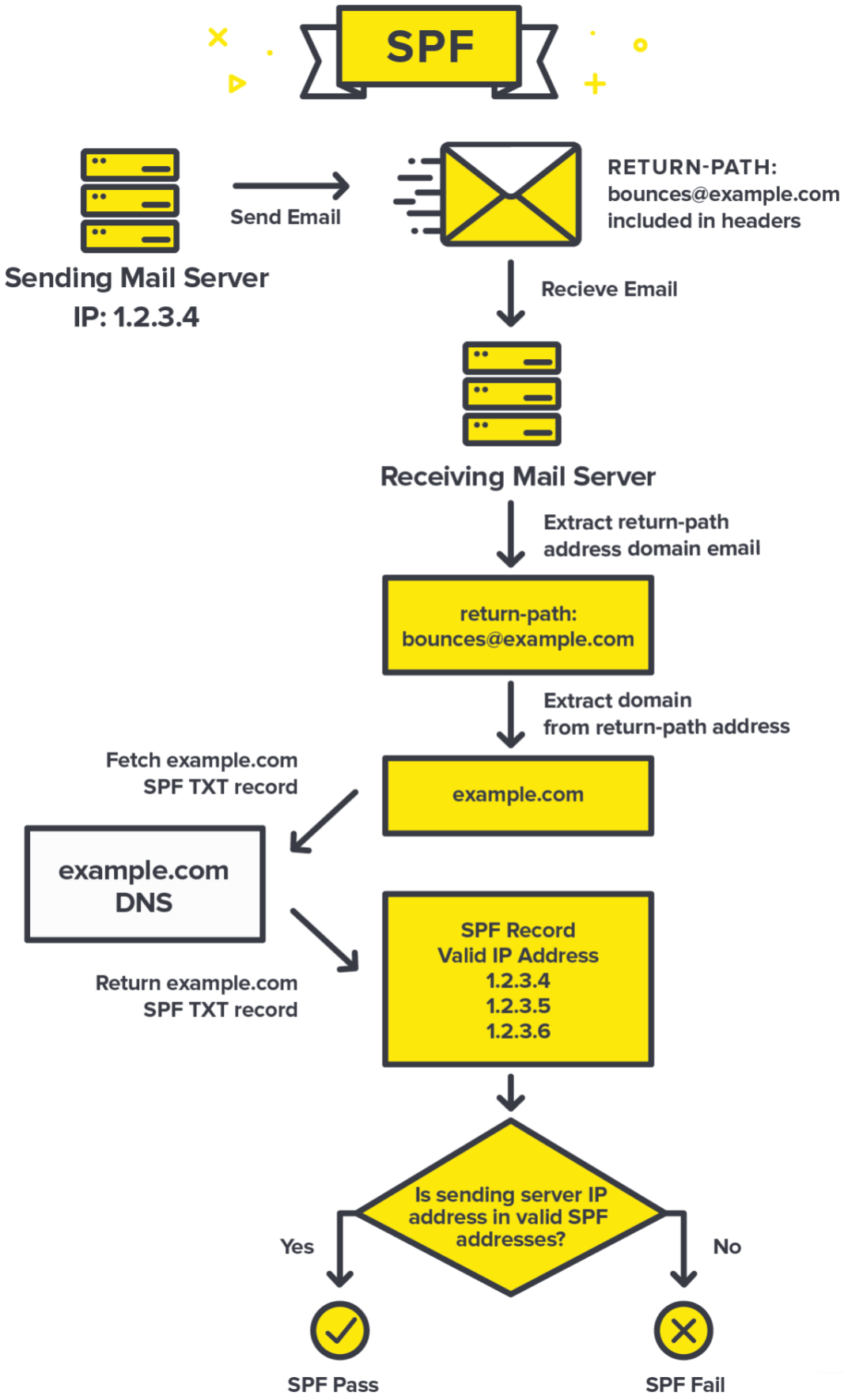
SPF may not be perfect, but you're still much better off using it than not using it. Emails can still be delivered without setting up SPF, but doing so improves your cha
Having an SPF policy provides an additional trust signal to ISPs so you can
likelihood that your emails arrive in the inbox. The SPF policy can also help mitigate the

backscatter of bounce and error notifications when spammers try to abuse your domain. Ultimately, SPF won't solve all of your delivery problems, but it's an additional layer that, combined with DKIM and DMARC, can improve your delivery rates and prevent abuse.

How do SPF records work?

Now that you have the big picture behind SPF, let's dive into the technical details a bit more. Most email services provide simple SPF record configuration instructions and then handle the hard part for you. Some providers, like Postmark, do not require that you add any DNS records to start passing SPF. So thankfully, you don't have to understand the inner-workings of SPF to benefit from it. But knowing a little more about it can come in handy.

Let's take a look at an SPF policy in action and see how the process unfolds:


SPF
Send Email
RETURN-PATH:
bounces@example.com
included in headers
Sending Mail Server
IP: 1.2.3.4
Recieve Email
Receiving Mail Server
Extract return-path
address domain email
return-path:
bounces@example.com
Extract domain
from return-path address
Fetch example.com
SPF TXT record
example.com
example.com
DNS
SPF Record
Valid IP Address
1.2.3.4
1.2.3.5
1.2.3.6
Return example.com
SPF TXT record
Is sending server IP
address in valid SPF
addresses?
Yes
No
SPF Pass
SPF Fail

As mentioned earlier, the key technical detail with SPF is that it works by looking at the domain of the `Return-Path` value included in the email's headers. The receiving server extracts the domain's SPF record and then checks if the source email server IP is approved to send emails for that domain.

Receiving servers verify SPF by checking a specific TXT DNS entry in your domain, which includes a list of approved IP addresses. This is one of the key aspects of SPF. By using DNS, it's able to build on something that every website or application already has. That DNS entry includes several parts that each provide different information to the server.

How do I implement an SPF record on my domain?

You do not need to do anything to pass SPF on emails sent through Postmark, but for most services, implementing SPF only requires a TXT entry in DNS. That entry consolidates multiple values in a short line of text. If a provider needs you to add them to your SPF entry, they'll provide the full text that you need to copy into your SPF entry. However, as you accumulate providers and need to add more, it's important to know that you only need to take the `include:` portion from their instructions and insert that into your existing SPF entry.

The most common mistake when setting up SPF is having multiple SPF TXT entries in your DNS. If you do, the receiving server won't know which SPF TXT entry is the definitive entry. This can result in valid servers failing SPF. So whenever you need to add an SPF record for a new service, always make sure that you don't have an existing SPF TXT entry first. If you already have an entry, just add the service to that entry.

How does the SPF record syntax work?

SPF record syntax might look complicated and confusing at first, but it is fairly easy to understand once you know the basics. Let's look at a breakdown of the key elements (also called "mechanisms") in an example SPF record entry of `v=spf1 a mx include:spf.mtasv.net include:_spf.createsend.com ~all`.

- `v=spf1` This states which version of SPF is being used.
- `a` This states that if the domain includes an address record (A or AAAA) for the

sender's address, it will match. So, if the IP address of your A record is used to send email, it will pass.

- `mx` The short version is that as long as the email originates from an IP address of the domain's incoming mail servers, then it's a match. The recipient server will check the MX record with the highest priority first.
- `include:` The include statements essentially tell receiving servers to include the values for the SPF records at the specified domain. These records generally specify a set of IP addresses for the service. In this case `spf.mtasv.net` contains the SPF entry for Postmark and `_spf.creatsend.com` represents Campaign Monitor's SPF entry. To double-check that everything works as it should, you can look at these using the `dig` command in your terminal. Just type `dig txt spf.mtasv.net` and you'll see the Postmark SPF record and the specified IP addresses.
- `~all` This specifies that everything else should be a "Soft" fail. That means that the message should be accepted but tagged as a soft fail, and the receiving ISP can use that as an additional factor in scoring the message's likeliness of being spam. You could replace the `~` with a `-` and that would indicate that the message should be rejected. However, this is more aggressive and is known to create more issues than it solves (we don't recommend it).

Each one of these values gives recipient servers important information they can use to make sure a message is sent from one of your trusted sources. As one of the earliest attempts to secure email, SPF created a path for future email security protocols like DKIM and DMARC.

The very best approach to securing your domain's email is to layer SPF with DKIM and DMARC. Don't miss our other guides on these protocols to learn more about how they work together to protect your domain.

Resources

Postmark guides on email authentication

- DMARC
- DKIM

Dive deeper into SPF

- Open-SPF.org
- How to Explain SPF in Plain English
- SPF Testing Tools

FAQ

Why doesn't SPF focus on the `From` address? It seems like that's what spammers would want to impersonate.

SPF was designed to protect the envelope sender and it stops spammers from abusing mail systems with backscatter and other irrelevant traffic. DKIM protects the `From` address by cryptographically signing messages to verify the author.

If I add an SPF record to our DNS, will I be able to see which emails have been blocked?

Not always. If you'd like a report on how email from your domain performs against SPF checks, you can setup DMARC to get weekly reports.

Will the sender of the email get a bounce message or does the email ju disappear if it fails SPF?

It's really up to the recipient server to decide how they handle messages that don't align with SPF. Sometimes postmasters choose to bounce these failed messages, and other servers choose to discard messages that fail SPF.

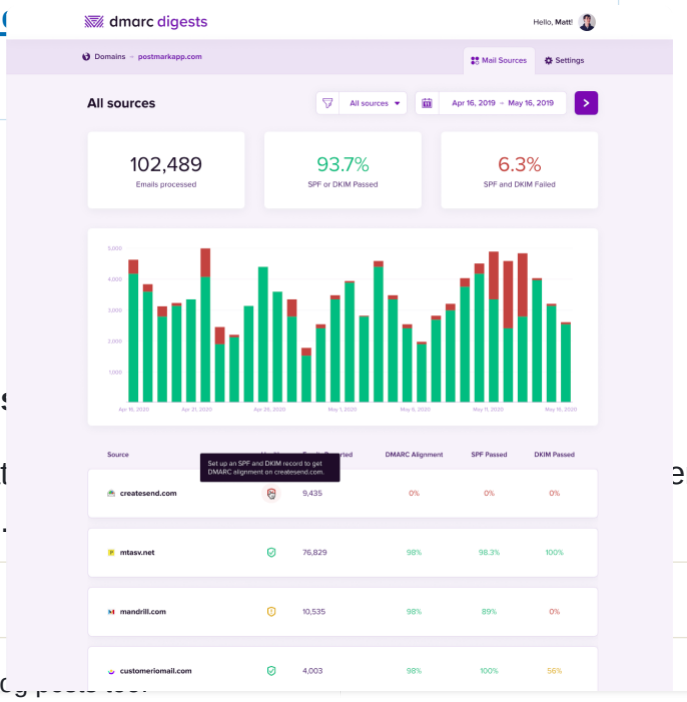
This post was originally published Feb 08, 2016

DKIM: What is it and why is it important?

By Shane Rice

Troubleshooting

By Shane Rice



Alternatively, use our free tool to receive weekly DMARC reports by email.

Follow @postmarkapp RSS feed

Still have questions?

Brian

Schedule a call

PRODUCT

Pricing
Customers
Reviews
Meetup Sponsorship
Dedicated IPs
iOS App
Latest Updates

FEATURES

Email API
SMTP Service
Message Streams
Transactional Email
Email Delivery
Templates
Inbound Email
Analytics
Webhooks
Security
Email Experts
Rebound

POSTMARK FOR

Agencies
Startups
Enterprise
Bootstrapped Startups
Side Projects
Developers

POSTMARK VS.

SendGrid
SparkPost
Mailgun
Amazon SES
Mandrill

RESOURCES

Blog
API Documentation
Getting Started
Email Guides
Videos
Podcast
DMARC Digests
Webinars
Labs
Migration Guides
Newsletter

HELP

Support Center
Contact Support
Status: Up!

Made with ♥ at We're hiring!