How to Set up SPF Record for Your Domain

https://orbisius.com/blog/set-up-spf-record-domain-p6946

What is SPF?

SPF (Sender Policy Framework) is an email authentication process that site owners can whitelist certain servers to send email on their behalf.

It’s a TXT record added to the main domain (@) that lists the authorized services.

Defining this is very important so your emails you send to reach their (final) destination.

When sending transactional emails it’s good to allow your customers to just hit reply and then receive the email.

Also if you don’t have SPF (and DKIM) records your emails will most likely land in spam.

The bare minimum is spf which is a simple TXT record that you add at your registrar.

It’s good to use client emails and a dedicated email delivery system such as mailgun and mailchimp. They take care of their infrastructure so the emails are delivered properly and catching bad people as soon as possible.

So for our SaaS apps we have these settings

- emails are allowed from the email provider (MX records e.g. Google Workspace or Zoho Mail etc),
- the server that hosts the website and mailgun.
- transactional email providers e.g. mailgun, mandrill, mailjet
- Sometimes we also add an extra IP address to the list.

You can use this tool to check the current setting. You need to either enter spf:EXAMPLE.COM or find SPF from the dropdown

https://mxtoolbox.com/SuperTool.aspx

Your registrar has put a default value for the SPF field in case you have an email forwarding service activated for your domain name. If that’s the case you will need to keep the existing list and add the extra info to the existing value.

The spf record is usually added to the main domain which is usually marked as @.

SPF failure occurs when the sender's IP address is not authorized to send that email.
The email is then sent to a spam folder or rejected.
This is when somebody is pretending to send emails on your behalf.

At the end there’s a modifier which determines how the email should be treated.

SoftFail ~all

A soft fail instructs the mail servers to forward it to the spam folder.

HardFail -all

A hard fail means that emails from unauthorized senders should be deleted

The value of the whole SPF record consists of fields separated by a space.

Example of SPF value.

v=spf1 a mx include:mailgun.org include:zoho.com include:spf.mandrillapp.com include:spf.r

If you’re using outlook you may need to add include:spf.protection.outlook.com

For the full list of Outlook servers go to the following address:

> https://docs.microsoft.com/en-us/microsoft-365/security/office-365-security/set-up-spf-in-office-365-to-help-prevent-spoofing?view=o365-worldwide

You can also add a specific IP that may send emails on your behalf.

ip4:111.222.333.444

How to add a record with GoDaddy

https://dcc.godaddy.com/manage/dns

Then select your domain name and then update results per page (bottom of the page) and then search for SPF.

There should be a record. It could be on a first or other pages.

If there's one you need to update it while keeping the values there or you may lose emails.

How Add an SPF Record for NameCheap

You need to login and then in domain list > Manage > Advanced DNS

Check again for an existing record. It may show as locked. If there isn't one then add a TXT record.

Image credit: Erica Steeves (@ecees) on unsplash, image: G_lwAp0TF38

If you need any help implementing any of the steps, **contact us** (free estimate)

Disclaimer: The content in this post is for educational purposes only. Always remember to take a backup before doing any of the suggested steps just to be on the safe side. Referral Note: When you purchase through an referral link (if any) on this page, we may earn a commission.