proofpoint

HOW TO IMPLEMENT SPF

WHAT IS SPF?

SPF (Sender Policy Framework) allows the owner of a domain to specify which mail servers they use to send mail from that domain. A company sending email publishes an SPF record (TXT RR) in the Domain Name System (DNS). The record lists which IP addresses are authorized to send email on behalf of their domain.

Receivers of email verify the SPF record by looking up the "envelope from" (aka Mail From, Mfrom or return-path) domain name in the DNS. If the IP address sending email on behalf of this domain is not listed in the SPF record, the message fails SPF authentication.

An SPF-protected domain is less attractive to fraudsters and is therefore less likely to be blacklisted by spam filters, ensuring that legitimate email from that domain is delivered.

HOW TO IMPLEMENT SPF

STEP 1: Gather IP addresses that are used to send email

Identify which mail servers you use to send email from your domain (e.g. web servers, in-office mail servers, your ISP's mail server, third-party mail servers, etc.) This can be a difficult task in its own right. We recommend using DMARC (Domain-based Message Authentication Reporting and Conformance) reporting to help. See the DMARC template in this kit to learn more.

STEP 2: Make a list of your sending domains

Chances are, your company owns many domains. Some of these domains are used to send email. Others are not.

It's important to create SPF records for all the domains you control, even non-sending domains. Why? Because the first thing cybercriminals will do once they realize all of your sending domains are protected with SPF is try to spoof your non-sending domains.

STEP 3: Create Your SPF Record

To authorize legitimate senders, follow a v=spf1 (version 1) tag and follow it with your designated IPs.

For example: v=spf 1ip4:1.2.3.4 ip4:2.3.4.5

If you want to authorize a third party to send email on behalf of your domain, you must add your IP address, A records or "include" statement within your SPF record (such as include:thirdparty.com).

After adding all authorized IPs, end your record with an –all tag to indicate a hard SPF fail or an ~all tag to indicate a soft SPF fail. Proofpoint recommends an –all tag as it is the most secure.

SPF records cannot be over 255 characters in length and cannot contain more than ten additional DNS lookups, so make sure anything contained therein does not generate more than that. Here's an example of what your record might look like:

v=spf1 ip4:1.2.3.4 ip4:2.3.4.5 include:thirdparty.com –all

For your domains that do not send email, the SPF record will exclude any modifier with the exception of -all. Here's an example record for a non-sending domain:

v=spf1-all

STEP 4: Publish your SPF to DNS

Work with your DNS server administrator to publish your SPF record to DNS for your envelope from domain, so mailbox providers can reference it. If you're using a hosting provider such as 123-reg or GoDaddy, then this process is fairly simple.

If your DNS records are administered by your ISP or if you aren't sure, then contact your IT department for support. Email service providers typically publish SPF records for sending domains on your behalf if control of a particular DNS location has been delegated to them.