SPF Setup Guide

Welcome to another Global Cyber Alliance setup guide. Today we will be looking at SPF or Sender Policy Framework. SPF is an email authentication protocol that allows the owner of a domain to specify which mail servers are allowed to send mail using the organizations domain name. Once SPF is created on your DNS server as a TXT file, receiving mail servers will check to see if the server that sent the email was authorized by the sender's domain to do so. Let's first take a look at a sample SPF record and break down the different parts. An example for an SPF record would look something like this

v=spf1 mx include: _spf.authorizedmailservers.com -all

- v=spf1 – Sets the SPF version that is being used
- mx – Allows the domain's MX details to send email
    - If the domain name has an MX record resolving to the sender's address it will match (an example would be if the mail comes from one of the domain's incoming mail servers)
- include: _spf.authorizedmailservers.com – The mail server you have authorized for your domain goes here.
- -all – This flag indicates that servers that are not listed previously are not authorized to send email. If an unauthorized server does send email, action is taken according to the receivers mailer server policy.
    - The all flag is an important aspect of the SPF record
        - -all – Fail, any server that is not previously listed is not authorized to send email.
        - ~all – SoftFail, if mail is received from a server that is not previously listed, it is marked as a soft fail, which allows the email to be checked further.
        - ?all – Neutral, an IP that matched a mechanism with this qualifier will neither pass or fail SPF
        - +all – Pass, an IP that matches a mechanism with this qualifier will pass SPF, also this is the default setting for SPF records

Gather IP addresses that are used to send email

- We need to identify which mail servers your organization is using to send mail. While working on this list we need to consider if any of the following are used by your organization to send emails
    - In-Office mail server (Microsoft Exchange)
    - Your ISP's mail server
    - The mail server of your end user's mailbox provider
    - **Any other third-party mail server used to send email on behalf of your organization**

Make a list of your sending domains

It is highly likely that your organization owns multiple domains. Some of these are used to send mail while others are not. It is vital that you create SPF records for all the domains that your organization owns even the ones you're not mailing from. By doing this you can protect both your domains you send mail from and the domains you don't from criminals.

Create your SPF record

SPF authenticates a sender's identity by comparing the sending mail servers IP address to the authorized list of IP addresses published by the sender in the DNS record. And here is how we create your SPF record:

- You can only have one SPF record per domain
- SPF records cannot be more than 255 characters in length, also no more than ten include statements sometimes known as "lookups" can be used.
- Always start with v=spf1 tag. All other tags will follow after this.
    - Any IP addresses that are authorized to send mail. These will start with either ip4 or ip6 for example, v=spf1 ip4:1.2.3.4 ip4:2.3.4.5
- If you also are using a third party to send emails on behalf of your organization, you must add an "include" statement in your SPF record (include:thirdparty.com) to authorize that specific third party as an authorized sender
- Alright now that we have added all authorized IP addresses and include statements, our SPF record will end with and ~all or -all tag
    - An ~all tag indicates a soft SPF fail while the -all tag indicates a hard SPF fail. While both ~all and -all will kickback a failure it is recommended to use the -all tag as it is more secure.

Now let's take a quick look at the domains that are not used for email. The SPF record for these are simple and will exclude any include statements or modifiers with the exception of -all. Here is an example of what that would look like….

```
v=spf1 -all
```

And with that we have created the SPF records needed to protect your organization's domains. These records along with the DMARC and DKIM records will work to solidify email security for your servers.