M^{3}AAWG Technology Summaries

Sender Policy Framework (SPF)

September 2023

The reference URL for this document is https://www.m3aawg.org/ts_SPF

What SPF is:

SPF is an email authentication protocol that checks which IP addresses are authorized to send mail on behalf of the originating domain.

What SPF does:

- Domain owners use SPF to publish a list of IP addresses and domains from which authorized email can be sent.
- Receiving servers check the IP address of the sending server against the published list of addresses authorized by the domain being authenticated.
- If the IP address is included in the authorized list, the result is “SPF pass.” If the sending server is not authorized, the verification query returned is “SPF fail.” The verification query can also return a range of results, from “neutral” to “soft fail.”

What SPF does not do:

- SPF does not attest to the authenticity or quality of the message’s content and does not ensure that the message is “good” or “legitimate.”
- As SPF uses the IP address of a directly connected server, “SPF pass” does not survive simple relaying or re-posting through mailing list distribution or alumni-address forwarding.
- “SPF fail” does not equate to malicious or bad activity, because a variety of benign reasons can cause an SPF failure.

References:

RFC 7208, “Sender Policy Framework (SPF) for Authorizing Use of Domains in Email, V1”
RFC 5321, “Simple Mail Transfer Protocol” (SMTP)
“M3AAWG Email Authentication Recommended Best Practices”
“M3AAWG Best Practices for Managing SPF Records”

As with all documents that we publish, please check the M^{3}AAWG website (www.m3aawg.org) for updates.