What is SPF?

SPF (Sender Policy Framework) Explained

Sender Policy Framework (SPF) is a crucial component of email authentication protocols designed to combat email spoofing and phishing attacks.

It works by allowing domain owners to specify which mail servers are authorized to send emails on behalf of their domain. When an email is sent, the recipient's mail server checks the SPF record of the sender's domain to verify if the sending server is allowed to send emails for that domain. If the sending server is listed in the SPF record, the email is considered legitimate; otherwise, it may be flagged as suspicious, quarantined, or rejected altogether.

The primary benefit of SPF is its ability to prevent email spoofing, where malicious actors forge the sender's email address to deceive recipients into believing that the email is from a trusted source. By implementing SPF records, domain owners can significantly reduce the likelihood of their domains being used for fraudulent activities. Additionally, SPF helps in maintaining the reputation of legitimate senders by reducing the chances of their emails being marked as spam or phishing attempts.

SPF plays a vital role in enhancing email deliverability. By authenticating the sender's identity through SPF, email servers can make more informed decisions about the legitimacy of incoming emails, thereby improving the overall deliverability rates and reducing the likelihood of false positives or false negatives in spam detection mechanisms.

SPF is a widely accepted and expected component for reliable email delivery and should be enabled on your web site now. If it is not, make sure SPF is enabled in your DNS records as soon as possible. SPF Tools are available by default on all **GlowHost Web Hosting** packages and SPF records can be set up with a few clicks within your web site's control panel. In many cases is already setup for you by default, or our technicians can help you set it up if you are still unsure on how to do it on your own.

Here is how SPF works:

1. **DNS record**: The owner of a domain publishes an SPF DNS record in the domain's DNS settings. This record specifies a list of authorized mail servers that are allowed to send emails on behalf of that domain.
2. **Email transmission**: When an email is sent from a domain that has SPF enabled, the receiving mail server checks the SPF DNS record of the sender's domain to verify if the sending mail server is authorized to send emails on behalf of that domain.
3. **SPF verification**: The receiving mail server compares the IP address of the sending mail server against the list of authorized IP addresses specified in the SPF DNS record. If the sending mail server's IP address matches one of the authorized IP addresses, the email passes SPF authentication. Otherwise, it fails SPF authentication.
4. **SPF action**: Depending on the SPF authentication result, the recipient's mail server may take various actions:
    - If the email passes SPF authentication, it is accepted and will likely be delivered to the recipient's inbox.
    - If the email fails SPF authentication, the receiving mail server may choose to mark the email as spam, reject it outright, or apply other filtering actions based on its configured SPF policy.

SPF helps prevent email spoofing by allowing domain owners to specify which mail servers are authorized to send emails on behalf of their domain. It provides a mechanism for receivers to verify the authenticity of the sender's domain, reducing the likelihood of fraudulent emails reaching users' inboxes.

SPF is also one of the essential building blocks along with **DKIM (DomainKeys Identified mail)** for those seeking to deploy a full-blown **DMARC** (Domain-based Message Authentication, Reporting, and Conformance) policy for their sending domains. While DMARC is not necessarily required to send emails reliably, DMARC is starting to become widely adopted to increase email security and brand trust across the Internet. Larger organizations are encouraged to implement a DMARC as soon as possible, and the DMARC compliance process does take some time and technical knowledge to achieve.

You can **learn more about how DMARC, SPF and DKIM** work together as we have created an entire section that tackles DMARC from start to finish within this knowledge base. GlowHost also offers **Managed DMARC Services** for those that would prefer a "done for you" hands-off DMARC approach, or for those organizations that prefer to outsource or supplement their own IT department's management of their DMARC policy. GlowHost's Managed DMARC Services combine experienced DMARC email technicians with a Software as a Service DMARC dashboard complete with graphs and robust reporting options.

Related Topics:

- DMARC, DKIM, SPF and BIMI Info
- DMARC SPF Alignment (aspf)
