iCorps TECHNOLOGIES

Email Security: SPF, DKIM, DMARC Explained

SPF, DMARC and DKIM are **three standards that help to prevent email spoofing, phishing and spamming** by verifying the sender's identity and domain.

These standards work together to ensure that only authorized senders can use a specific domain name in their email messages, and that the recipients can trust that the messages are authentic and unaltered.

Email security is a vital aspect of protecting the **integrity and confidentiality** OF ELECTRONIC COMMUNICATIONS

Benefits of SPF, DKIM & DMARC

- Enhanced email security posture
- Improves overall deliverability of the sending mail server
- Combats phishing and spoofing as IP address of sender is verified
- Keeps your domain off global blacklists
- Elevates domain reputation

SPF, DKIM & DMARC Defined

If the recipient knows who sent the email, they are more likely to open it.

SPF: Sender Policy Framework

Sender Policy Framework (SPF) works by strictly determining the number of allowed IP addresses that can send emails from your domain.

Three Major Elements of SPF:

1. Policy frame as the name implies
2. Authentication method
3. Specialized headers within the email that conveys data

DKIM: DomainKeys Identified Mail

DomainKeys Identified Mail (DKIM) authentication ensures that the content of the email is trusted and has not been compromised or tampered with during the delivery.

DKIM adds trust between the receiver and sender server in a similar way as sending Certified Mail.

DMARC: Domain-Based Message Authentication, Reporting and Conformance

Also known as "email signing", DMARC ties SPF and DKIM email security protocols together with a more consistent set of policies.

Three Purposes of DMARC:

1. Verify that the sender's email message is protected by DKIM and SPF protocols.
2. Inform the receiving mail server what to do if neither DKIM or SPF protocols pass.
3. Provide a way for the receiving mail server to report to the sender about the email message(s) that fail or pass DMARC evaluation.

How do they work?

SPF

Adding an SPF record to your DNS / DNStxt records specifies all the approved servers that email is allowed to come from.

`v= spll a ip4:12.34.56.78/28 include:marketingemailserver.com -all`

The SPF authentication record allows email sent from 12.34.56.78/28 and marketingemailserver.com. If an email comes from other addresses, then it will be considered an SPF soft fail.

DKIM

DKIM works by adding a digitial signature to the email message header.

DKIM also uses an encryption algorithm that creates a private key and a public key.

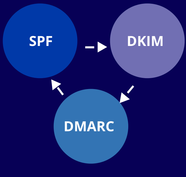
DMARC

DMARC relies on the established standards of SPF and DKIM for email authentication. DMARC validation works by deciding whether to reject, accept or flag an email message.

To deploy DMARC, you need to publish a DMARC record (text entry within the DNS record).

What comes next?

iCorps Technologies' team of experts is here to help your business align SPF, DKIM and DMARC to boost your email security standards and maximize your email security.



iCorps TECHNOLOGIES