What are DMARC, DKIM, and SPF?

Archived: 2026-04-06 02:50:40 UTC

What are DMARC, DKIM, and SPF?

DMARC, DKIM, and SPF are three email authentication methods. Together, they help prevent spammers, phishers, and other unauthorized parties from sending emails on behalf of a domain* they do not own.

DKIM and SPF can be compared to a business license or a doctor's medical degree displayed on the wall of an office — they help demonstrate legitimacy.

Meanwhile, DMARC tells mail servers what to do when DKIM or SPF fail, whether that is marking the failing emails as "spam," delivering the emails anyway, or dropping the emails altogether.

Domains that have not set up SPF, DKIM, and DMARC correctly may find that their emails get quarantined as spam, or are not delivered to their recipients. They are also in danger of having spammers impersonate them.

**A domain, roughly speaking, is a website address like "example.com". Domains form the second half of an email address: alice@example.com, for instance.*

How does SPF work?

Sender Policy Framework (SPF) is a way for a domain to list all the servers they send emails from. Think of it like a publicly available employee directory that helps someone to confirm if an employee works for an organization.

SPF records list all the IP addresses of all the servers that are allowed to send emails from the domain, just as an employee directory lists the names of all employees for an organization. Mail servers that receive an email message can check it against the SPF record before passing it on to the recipient's inbox.

How does DKIM work?

DomainKeys Identified Mail (DKIM) enables domain owners to automatically "sign" emails from their domain, just as the signature on a check helps confirm who wrote the check. The DKIM "signature" is a digital signature that uses cryptography to mathematically verify that the email came from the domain.

Specifically, DKIM uses public key cryptography:

- A DKIM record stores the domain's *public key*, and mail servers receiving emails from the domain can check this record to obtain the public key
- The *private key* is kept secret by the sender, who signs the email's header with this key
- Mail servers receiving the email can verify that the sender's private key was used by applying the public key

How does DMARC work?

Domain-based Message Authentication Reporting and Conformance (DMARC) tells a receiving email server what to do given the results after checking SPF and DKIM. A domain's DMARC policy can be set in a variety of ways — it can instruct mail servers to quarantine emails that fail SPF or DKIM (or both), to reject such emails, or to deliver them.

DMARC policies are stored in DMARC records. A DMARC record can also contain instructions to send reports to domain administrators about which emails are passing and failing these checks. DMARC reports give administrators the information they need to decide how to adjust their DMARC policies (for example, what to do if legitimate emails are erroneously getting marked as spam).

Where are SPF, DKIM, and DMARC records stored?

SPF, DKIM, and DMARC records are stored in the Domain Name System (DNS), which is publicly available. The DNS's main use is matching web addresses to IP addresses, so that computers can find the correct servers for loading content over the Internet without human users having to memorize long alphanumeric addresses. The DNS can also store a variety of records associated with a domain, including alternate names for that domain (CNAME records), IPv6 addresses (AAAA records), and reverse DNS records for domain lookups (PTR records).

DKIM, SPF, and DMARC records are all stored as DNS TXT records. A DNS TXT record stores text that a domain owner wants to associate with the domain. This record can be used in a variety of ways, since it can contain any arbitrary text. DKIM, SPF, and DMARC are three of several applications for DNS TXT records.

How to check if an email has passed SPF, DKIM, and DMARC

Most email clients provide an option labeled "Show details" or "Show original" that displays the full version of an email, including its header. The header — typically a long block of text above the body of the email — is where mail servers append the results of SPF, DKIM, and DMARC.

Reading through the dense header can be tricky. Users viewing it on a browser can click "Ctrl+F" or "Command+F" and type "spf," "dkim," or "dmarc" to find these results.

The relevant text might look like:

```
arc=pass (i=1 spf=pass spfdomain=example.com dkim=pass
dkdomain=example.com dmarc=pass fromdomain=example.com);
```

The appearance of the word "pass" in the text above indicates that the email has passed an authentication check. "spf=pass," for example, means the email did not fail SPF; it came from an authorized server with an IP address that is listed in the domain's SPF record.

In this example, the email passed all three of SPF, DKIM, and DMARC, and the mail server was able to confirm it really came from example.com and not an impostor.

It is important to note that these records themselves do not enforce the domain's policies or authenticate the emails. The mail servers have to check them and apply them correctly for the records to have any effect.

It is also important to note that domain owners need to configure their SPF, DKIM, and DMARC records properly themselves — both in order to prevent spam from their domain, and to make sure that legitimate emails from their domain are not marked as spam. Web hosting services do not necessarily do this automatically. Even domains that do not send emails should at least have DMARC records so that spammers cannot pretend to send emails from that domain.

How to set up DMARC, DKIM, and SPF for a domain

DMARC, DKIM, and SPF have to be set up in the domain's DNS settings. Administrators can contact their DNS provider — or, their web hosting platform may provide a tool that enables them to upload and edit DNS records. For more details on how these records work, see our articles about them:

- SPF DNS records
- DKIM DNS records
- DMARC DNS records

How to easily set up these records in Cloudflare

To set up these records in Cloudflare, use the Email Security DNS Wizard.
