

[← All articles](#)

INSIGHT

What DMARC Actually Protects You From, and What It Does Not

3 Aug 2026 · 8 min read

Ask five people what DMARC does and you will get five answers: it stops phishing, it kills spam, it proves an email is safe. None of that is quite right. DMARC (the current spec is [RFC 9989](#)) checks one narrow thing: did the owner of the domain shown in the From line actually authorise this message, provable through SPF or DKIM?

It is a good question to answer. It is also a lot smaller than the reputation DMARC has built up. Reach p=reject thinking you are now phishing-proof and you will quietly drop the controls that handle everything DMARC never touched in the first place.

How email proves who sent it

Two building blocks sit underneath DMARC. **SPF** is a list a domain publishes of the servers allowed to send mail on its behalf; the receiver checks whether the mail actually arrived from one of them. **DKIM** adds a cryptographic signature to the message, which lets the receiver confirm it came from the signing domain and was not altered along the way. DMARC then pins both of those to the address you see in the From line.

Here is the part that trips people up. An email actually has two "from" addresses. There is the **envelope address**, which works like the address on a posted parcel: mail servers use it to route the message and then throw it away, so you never see it. And there is the **visible From** your mail app displays, the "Your Bank <alerts@your-bank.com>" you read at the top of the message. Nothing forces those two to match.

That gap is the whole game: an attacker can show your bank in the visible From while the envelope quietly points at their own server.

SPF looks at the envelope address. DKIM's signature carries a domain of its own. DMARC's job is to take whichever of those actually authenticated and check it against the From line you can see, because that is the address a human trusts.

What these actually look like

All three live as text records in your domain's DNS, the same place your website's address is configured. You do not need to memorise the syntax; it helps to recognise the shape.

An **SPF** record lists who is allowed to send. This one authorises Google Workspace and a marketing tool, and says anything else should be treated as suspicious:

```
example.com.  TXT  "v=spf1 include:_spf.google.com include:sendgrid.net -all"
```

The `include:` entries pull in each provider's own list of servers, and `-all` means "if it is not on those lists, it is not us".

A **DKIM** record publishes the public half of the signing key, so receivers can check the signature on your mail. The long string is the key itself:

```
selector1._domainkey.example.com.  TXT  "v=DKIM1; k=rsa; p=MIGfMA0GCSqGSIb3DQEBAQ...AB"
```

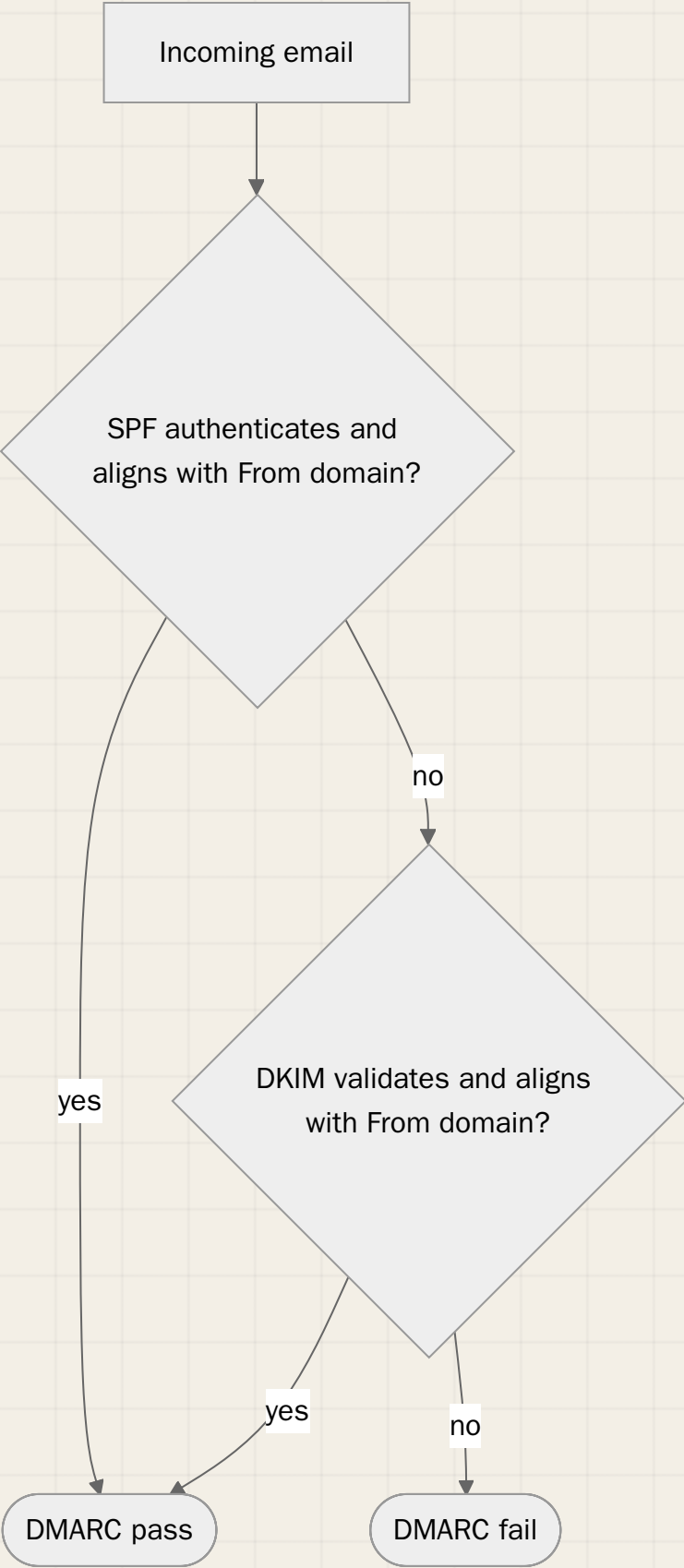
Finally the **DMARC** record ties it together and tells receivers what to do when a message fails. This one asks them to reject failures and to send you reports:

```
_dmarc.example.com.  TXT  "v=DMARC1; p=reject; rua=mailto:reports@example.com"
```

`p=reject` is the strict setting: fail authentication and the mail gets turned away. `rua=` is simply where your aggregate reports land.

How a pass is actually decided

DMARC sits on top of SPF and DKIM, and it evaluates them independently. There are two separate ways a message can pass: SPF passes for the hidden envelope domain and that domain aligns with the visible From domain, or a DKIM signature validates and its signing domain aligns with the visible From domain. If either aligned path succeeds, DMARC passes. If neither does, it fails. "Aligns" simply means the two domains match closely enough to count as the same organisation.



DMARC passes if either SPF or DKIM both authenticates and aligns with the visible From domain. It fails only when neither does.

A quick word on what "align" means, because it catches people out. DMARC has two modes. In **relaxed** mode (the default) the two domains only need to share the same organisational domain, so a DKIM signature from mail.example.com aligns with a From of example.com. In **strict** mode they must be identical, and that same signature would fail. If you have seen "SPF pass, DMARC fail" and wondered how both can be true at once, it normally means SPF confirmed the hidden envelope domain successfully, but that domain did not match the visible From address closely enough to align. Strict versus relaxed mode then decides whether closely related domains count as the same.

Notice what the test never looks at: the words in the message, the links, the attachments, whether the sender means you harm. It only asks where the mail came from.

Where DMARC helps

The case DMARC was built for is exact-domain spoofing. If someone places your-bank.com in the From address without producing an aligned SPF or DKIM result, a policy of p=reject asks participating receivers to reject the message, although the receiver retains final control over its disposition and may apply local policy or exceptions. This is real protection, and for this specific attack it is strong. It also gives you something you did not have before: aggregate reports (defined in [RFC 9990](#)) revealing many of the systems participating receivers have observed sending as your domain, which is how you find the forgotten marketing tool or misconfigured relay before an attacker does.

Where it falls short

Lookalike domains. An attacker registers your-bank-support.com, sets up valid SPF and DKIM, and passes DMARC on their own domain. Your policy has no reach over a domain you do not own. To every receiver, that mail is fully authenticated.

Display-name impersonation. The name shows "Your Bank Security"; the actual address behind it is alerts@some-unrelated-domain.com. DMARC only ever checks the domain. It has nothing to say about the friendly name, which is the bit most people actually read, so this sails straight through a passing check.

Compromised mailboxes. When an attacker signs into a real account through phished credentials and sends through the legitimate provider, the message will usually pass SPF, DKIM and DMARC because, in

the protocol's terms, it was sent through authorised infrastructure. Authentication cannot tell a real user apart from an attacker controlling that user's account.

Authenticated but malicious domains. Anyone can register a domain and configure flawless authentication; senders of unwanted mail do this routinely. A pass on totally-legit-invoices.com confirms the owner authorised the mail. It says nothing about whether the owner is honest.

Spam and inbox placement. DMARC is not a spam filter and does not decide whether mail reaches the inbox. Filters may weigh it as one input, but authenticated spam is still spam, and placement is a separate system with its own logic.

Forwarding and mailing lists. Legitimate intermediaries can break authentication. Forwarding commonly breaks SPF because the forwarding server is not authorised by the original sender's domain, while mailing lists may modify the subject or body and invalidate DKIM. A legitimate message can therefore fail DMARC even though nobody is impersonating the sender. This is one reason enforcement should follow careful monitoring and remediation rather than a blind switch to p=reject.

Authentication is not trust

So a DMARC pass tells you one thing and one thing only: the domain in the From line authorised the mail, and SPF or DKIM proves it. Useful. It shuts down exact-domain spoofing and shows you who is sending as you. But whether the message is honest, whether it is safe to click, whether the account behind it has been hijacked, DMARC has no opinion on any of that. When a vendor tells you DMARC "stops phishing", that is the gap they are papering over.

We take a narrower line at SenderLedger. We get you to enforcement without knocking out your legitimate mail, show you which senders are really yours, and lock the door on exact-domain spoofing. The rest, watching for lookalike domains, spotting hijacked accounts, using human judgement, is a different job, and a domain that reaches p=reject thinking it is now covered has been sold a false sense of security.

See who is really sending as your domain.

SenderLedger maps every sender, tracks remediation, and tells you when reaching p=reject is actually safe.

Request access

DMARC

EMAIL-AUTHENTICATION

PHISHING

DB

SenderLedger

EU-first DMARC remediation for teams that need to discover senders, repair authentication and reach enforcement without breaking legitimate email.

Product

How it works

For MSPs

Pricing

Access

Request access

Request demo

MSP demo