

COLD EMAIL

What Is DMARC?

SPF, DKIM and DMARC Explained for Cold Email

B2BXclusive · b2bxclusive.com/blog



FREE CHEAT SHEET · B2BXCLUSIVE

What Is DMARC? SPF, DKIM and DMARC Explained for Cold Email

Short answer: DMARC (Domain-based Message Authentication, Reporting and Conformance) is a DNS record that tells receiving mail servers how to handle email that claims to come from your domain but fails authentication. A message passes DMARC when SPF or DKIM passes and that passing domain aligns with the visible From domain. Gmail requires it for bulk senders.

Key takeaways

- DMARC passes when **SPF or DKIM passes and is aligned** with the From domain. Passing alone is not enough.
- Google requires **SPF, DKIM and DMARC** for anyone sending 5,000+ messages a day to Gmail; p=none is the minimum policy.
- The most common cold email failure is **alignment**: the sending tool signs or bounces with its own domain, not yours.
- Roll out in steps: **p=none with reports**, fix every source, then quarantine, then reject.

SPF, DKIM and DMARC in one sentence each

Standard	What it proves	Where it lives	What it checks against
SPF	This server is allowed to send for this domain	TXT record on the domain	The hidden envelope sender (Return-Path), not the visible From
DKIM	This message was signed by this domain and not altered	TXT record at selector._domainkey	The d= domain in the signature, which can be any domain
DMARC	SPF or DKIM passed for the same domain the reader sees	TXT record at _dmarc.domain	The visible From domain

Example DMARC record (TXT at `_dmarc.yourdomain.com`) (template: copy and adapt)

```
v=DMARC1; p=quarantine; sp=quarantine; rua=mailto:dmarc@yourdomain.com; adkim=r; aspf=r
```

The DMARC pass rule (template: copy and adapt)

```
DMARC pass = (SPF pass AND SPF domain aligned with From)
              OR
              (DKIM pass AND DKIM d= domain aligned with From)
```

Quick answers

What is the difference between SPF, DKIM and DMARC?

SPF lists the servers allowed to send mail for a domain. DKIM adds a cryptographic signature that proves a message was not changed and names the signing domain. DMARC sits on top: it checks that SPF or DKIM passed for a domain that matches the visible From address, and tells receivers whether to deliver, quarantine or reject mail that fails.

Do I need DMARC for cold email?

Yes. Gmail requires SPF, DKIM and DMARC from bulk senders, Yahoo and Outlook.com have similar rules for high-volume senders, and an unauthenticated domain looks suspicious to every spam filter. Even if each inbox sends far below 5,000 a day, a DMARC record with aligned DKIM is the baseline for reaching the primary inbox.

What DMARC policy should a cold email domain use?

Start with `p=none` and a `rua` address so you receive reports for two to four weeks. Once every legitimate source passes aligned SPF or DKIM, move to `p=quarantine` and later `p=reject`. A secondary outreach domain with only one or two sending tools can usually reach enforcement faster than your main company domain.

Does DMARC `p=none` do anything?

It does not change delivery: receivers treat failing mail as they would without DMARC. But it publishes that you have a policy, which Gmail, Yahoo and Outlook.com require from bulk senders, and the `rua` tag gets you daily aggregate reports showing every server sending as your domain. That visibility is what makes enforcement safe later.

Why does DMARC fail when SPF and DKIM pass?

Because of alignment. SPF may pass for your sending tool's bounce domain and DKIM may pass for the tool's own signing domain, while the From address shows your domain. Neither passing domain matches yours, so DMARC fails. The fix is a custom return-path and custom DKIM key on your own domain in the sending tool.

What changed with RFC 9989 (DMARCBis)?

In 2026 the IETF published RFC 9989, which obsoletes the original DMARC specification, RFC 7489, and moves DMARC onto the standards track. Industry summaries say the `pct` tag is replaced by a simple test flag, and reporting moved into separate documents. Existing `v=DMARC1` records keep working, so nobody needs to rush a change.

Book a free strategy call

<https://bookshawn.b2bxclusive.com/>

Full guide with sources: <https://b2bxclusive.com/blog/what-is-dmarc-spf-dkim/> · By Subhendu J Shawn, founder of B2BXclusive.