

Email DNS posture of 100 ecommerce brands active in France

A reproducible snapshot of SPF, DMARC, MX, MTA-STS and TLS-RPT across the brands' public domains, conducted on August 21, 2026.

100/100

domains analyzed

67.0%

with enforced DMARC

21.0%

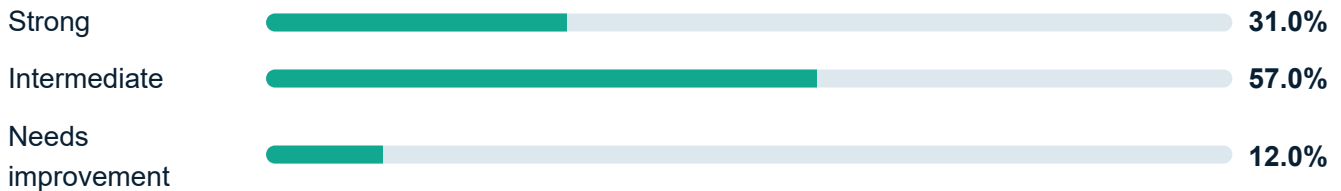
with a public SPF risk

4.0%

with MTA-STS detected

Key finding. 7.0% of the analyzed domains have no detectable DMARC policy, while 26.0% remain in monitoring mode only (p=none).

Public DNS score distribution



The median score is **76.5/100**. It measures public DNS signals only and is neither an inbox-placement test nor a Gmail or Outlook compliance certification.

What the data shows

- 79.0% have SPF with no issue detected by the scanner.
- 67.0% enforce DMARC with p=quarantine or p=reject.
- 4.0% publish MTA-STS and 4.0% publish TLS-RPT.

Results by category

Category	Domains	Median score	DMARC absent	Strong rating
Beauty	10	78.0	20.0%	30.0%
Culture and pets	8	65.0	0.0%	12.5%
Electronics	10	78.0	0.0%	20.0%
Fashion	25	78	8.0%	44.0%
Grocery	12	76.5	0.0%	33.3%
Home and DIY	15	75	0.0%	40.0%
Marketplaces	10	76.5	0.0%	30.0%
Sports	10	60.0	30.0%	10.0%

Methodology

Purposive sample of 100 brands with an ecommerce website accessible to the French market. Queries are performed on each brand's public domain. The score assigns 30 points to SPF, 45 to DMARC, 10 to MX, 10 to MTA-STS and 5 to TLS-RPT.

DKIM is deliberately excluded from the score. Reliable verification requires the selector used by the sender or the headers of a real message. The absence of a key for a few common selectors does not prove the absence of DKIM.

Limitations: the website domain may differ from the marketing sending domain; DNS records change; valid SPF does not prove message alignment; DMARC p=none meets some minimum requirements but does not enforce protection. The results should be described as a public DNS snapshot.

Provider context

Google requires SPF, DKIM and DMARC, among other measures, for senders delivering more than 5,000 messages per day to Gmail. Microsoft also requires these mechanisms for high-volume senders to Outlook.

Official sources: <https://support.google.com/mail/answer/81126> · <https://techcommunity.microsoft.com/blog/microsoftdefenderforoffice365blog/4399730>

About AuditLabHQ

AuditLabHQ analyzes a domain's main email authentication and security signals, then provides a summary and a PDF action plan.