

FREE CHEAT SHEET · B2BXCLUSIVE

We Checked 7,601 US SaaS Domains: 40% Don't Tell Inboxes to Block Fake Emails

Short answer: 40.2% of 7,601 US SaaS domains (21-200 employees) have no working DMARC protection: 31.6% are set to p=none, 7.9% have no DMARC record and 0.6% have duplicate records. 11.8%, about 1 in 8, have at least one hard error such as no SPF, two SPF records or no DMARC. Only 55.4% fully enforce DMARC.

Key takeaways

- **40.2%** of 7,601 US SaaS domains give inboxes no instruction to block fake email in their name.
- **11.8%, about 1 in 8,** have a hard error: no DMARC (7.9%), no SPF (4.4%), no MX (2.5%) or duplicate records.
- **Only 55.4%** fully enforce DMARC at quarantine or reject.
- **Teams using a sales email tool** have about half the hard-error rate (6.6% vs 12.7%), but just as many stop at p=none.
- **Most fixes take minutes:** merge duplicate records, publish DMARC with reports, then move to enforcement.

2. About 1 in 8 has a hard error that inboxes can see

Hard problem	Domains	Share
No DMARC record	603	7.9%
No SPF record	332	4.4%
No MX record	192	2.5%
Two or more SPF records	91	1.2%
Two or more DMARC records	49	0.6%

6. Companies that already use a sales email tool are cleaner, but not on DMARC

Group	Domains	Any hard problem	No DMARC	DMARC p=none	DMARC enforced
Uses a sales email tool	1,141	6.6%	2.9%	30.7%	60.2%
No tool detected	6,460	12.7%	8.8%	31.8%	54.5%

Quick answers

What are SPF, DKIM and DMARC, in one line each?
SPF lists the servers allowed to send for your domain. DKIM adds a signature that proves the message was not changed. DMARC tells inboxes what to do when a message fails those checks, and sends you reports.

Is DMARC p=none bad?
It is a starting point, not a finish line. It meets the minimum rule for high-volume senders, but it tells inboxes to deliver mail that fails authentication, so it does not stop impersonation.

Will fixing DNS get my cold emails into the inbox?
It removes a reason to be filtered. Inbox placement also depends on your sending volume, list quality, complaint rate and content. Authentication is the floor, not the whole house.

Why do two SPF or DMARC records matter so much?
The standards allow one of each. With two SPF records, SPF returns an error. With two DMARC records, receivers ignore DMARC for that domain.

Do these rules apply to small teams?
Gmail asks every sender to pass SPF or DKIM. The stricter SPF + DKIM + DMARC rule applies at roughly 5,000 messages a day to Gmail or Outlook.com addresses, counted across the whole domain, including marketing and product email.

How did you check DKIM without knowing each company's selector?
We tried 16 selectors that common mail providers and sending tools use. That finds most keys but not custom ones, so treat our missing-DKIM numbers as an upper bound.

Can I see the list of companies?
No. We publish aggregates only and do not name any company.

Can I use this data?
Yes, with a link to this page (see "Cite this study" on this page).

Book a free strategy call
https://bookshawn.b2bxclusive.com/

Full guide with sources: https://b2bxclusive.com/blog/saas-email-authentication-study/ · By Subhendu J Shawn, founder of B2BXclusive.