SNAPLEADS / LAB

SPF / DKIM / DMARC DNS Cheat Sheet

SPF: authorize sending hosts

RFC 7208

```
example.com. TXT "v=spf1 include:_spf.provider.example -all"
```

Question	Which infrastructure is authorized to use this MAIL FROM / HELO identity?
Common failure	Publishing multiple independent v=spf1 records instead of one coherent policy.
Check	Inspect the evaluated identity and DNS result; do not stop at what a vendor setup screen shows.

DKIM: sign message content with a domain key

RFC 6376

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

Question	Which signing domain and selector appear in the actual DKIM-Signature header?
Common failure	A correct-looking key exists, but the message signs with a different selector or old domain.
Check	Capture a fresh message and compare header values with authoritative DNS.

SNAPLEADS / LAB

SPF / DKIM / DMARC DNS Cheat Sheet

DMARC: align authenticated identity with visible From

RFC 9989

```
_dmarc.example.com. TXT "v=DMARC1; p=none; rua=mailto:dmarc@example.com"
```

A message can show SPF=pass or DKIM=pass and still fail DMARC if the authenticated domain does not align with the RFC5322.From domain. For direct bulk mail to personal Gmail accounts, Google requires alignment with at least one of SPF or DKIM.

Current RFC set

Base DMARC: RFC 9989 (May 2026). Aggregate reports: RFC 9990. Failure reports: RFC 9991. These documents collectively replace the older RFC 7489 reference.

Fast diagnostic order

MESSAGE -> DNS -> ALIGNMENT

01 Capture Authentication-Results from a fresh real message.

02 Identify SPF identity, DKIM d=/s= values, and visible From domain.

03 Query authoritative DNS for the records those values actually reference.

04 Check DMARC alignment, not just raw PASS labels.

05 Only then change policy, provider configuration, or sending behavior.