Email authentication checklist

SPF, DKIM, and DMARC | A practical review for business domains

Prepared by Subas Kandel, IT Consultant

1. Inventory the senders

[ ] List every service sending from the domain: staff mail, CRM, website forms, invoicing, and marketing.
[ ] Identify the DNS owner and record the existing settings before changes.

2. Check SPF

[ ] Confirm the SPF record includes the authorized sending services.
[ ] Check the DNS-lookup limit (10) and remove retired senders.
[ ] Verify outgoing messages pass SPF; allow for DNS propagation.

3. Enable DKIM

[ ] Follow each email provider's instructions to publish the signing key.
[ ] Enable signing in the sending service, then test an outgoing message.
[ ] Check DKIM passes for every legitimate sending service.

4. Review DMARC alignment

[ ] Confirm the visible From domain aligns with a passing SPF or DKIM domain.
[ ] Enable DMARC reporting and review legitimate and unrecognized sources.
[ ] Resolve legitimate failures before moving from monitoring to enforcement.

5. Keep checking

[ ] Repeat delivery tests after changes to DNS, mail providers, or third-party senders.
[ ] Assign an owner to review authentication reports and maintain the sender list.

Use provider-specific records. Authentication supports domain protection, but does not guarantee inbox placement.

Provider references

Google Workspace: Set up SPF | Troubleshoot SPF
Google Workspace: Set up DKIM
Gmail: Email sender guidelines and DMARC alignment