CICADA | RESOURCES

EMAIL | 120 MIN | WORKING KNOWLEDGE | UPDATED NOVEMBER 2026

Stop email impersonation with SPF, DKIM and DMARC

The three DNS records that make it much harder to send email pretending to be your business.

The short version

- ✓ SPF lists allowed senders; DKIM signs the message; DMARC sets the policy.
- ✓ Start DMARC at monitoring, read the reports, then tighten.
- ✓ Include legitimate senders before you enforce, or you'll block real mail.
- ✓ DMARC protects your domain's reputation, not your inbox from all phishing .

What each record does

- **SPF**: a DNS record listing the servers allowed to send email for your domain. Receivers check the sending server against it.
- **DKIM**: a cryptographic signature added to outgoing mail, verified with a public key in DNS.
- **DMARC**: a policy that tells receivers what to do when SPF or DKIM fails, and sends you aggregate reports.

Your email provider publishes the exact values. You add them at your domain registrar or DNS host.

The safe sequence

01 Turn on DKIM in your email platform and publish the record.

02 Publish an SPF record that includes every legitimate sender: Microsoft 365, Google, your website's contact form, the booking system, the newsletter tool.

Keep it under the lookup limit.

03 Publish DMARC with `p=none` and a reporting address.

04 Wait two to four weeks and read the reports. Identify anything legitimate that fails.

05 Fix those senders, then move to `p=quarantine`, and later `p=reject`.

Avoid the common mistakes

- Enforcing before you know which systems send mail as you is how quotes and password resets silently stop arriving.
- Using a `~all` SPF that soft-fails forever and never tightening DMARC.
- Forgetting subdomains and third-party senders.
- Assuming DMARC stops inbound phishing. It doesn't; it protects your domain from being impersonated.

> **NEED HELP?**
>
> Your email provider or IT supplier can publish these in an hour. Ask them to show you the DMARC reports and the policy value, not just say it's done.

Generated free at resources.cicadacs.com · General guidance, not an audit or legal advice.

Action checklist

- [ ] DKIM enabled and verified
- [ ] SPF includes every legitimate sender
- [ ] DMARC published at p=none
- [ ] Reports reviewed for four weeks
- [ ] Policy moved to quarantine or reject
- [ ] Subdomains and third-party senders covered

0 of 6 done