SPF policy

The question

Who can send for your domain?

SPF gives recipients a public list of authorised sending systems. Your email provider may be only one of them.

01 Understand

02 Observe

03 Verify

A practical briefing for the people who own your domain.

SPF policy

The mechanism

The recipient checks the server

It compares the connecting IP with the envelope domain's SPF policy. The visible From address is a separate identity.

01 Sending server IP

↓

02 Envelope domain's SPF policy

↓

03 Recipient's SPF result

SPF checks a server against the envelope identity. DMARC separately relates authenticated identity to the visible From domain.

SPF policy

The evidence

A record is one part of the evidence

> Our probe checks supported syntax and bounded dependencies. It does not test a real message. Sender-dependent rules can remain unknown.

PUT THE OBSERVATION IN CONTEXT

- **Public signal**
- **Service context**
- **Operational validation**

Use the finding to start an owned review.

SPF policy

The handoff

Start with the sender inventory

Ask your email owner to identify each sending service. Have your DNS owner review one policy before tightening its final rule.

BRING THE RIGHT OWNERS TOGETHER

01 Email service owner

02 DNS administrator with email providers

SPF policy

Your checklist

Keep a verifiable SPF checklist

- ✓ Record your sending services
- ✓ Check the lookup budget
- ✓ Test representative messages
- ✓ Assign an owner

> Read the SPF explainer for the full review.
>
> **/learn/spf**