



1. Home (<https://www.gov.uk/>)
2. Email security standards (<https://www.gov.uk/government/publications/email-security-standards>)
 - Government Digital Service (<https://www.gov.uk/government/organisations/government-digital-service>)

Guidance

Using Sender Policy Framework (SPF) in your organisation

Published 19 February 2016



© Crown copyright 2016

This publication is licensed under the terms of the Open Government Licence v3.0 except where otherwise stated. To view this licence, visit [nationalarchives.gov.uk/doc/open-government-licence/version/3](https://www.nationalarchives.gov.uk/doc/open-government-licence/version/3) (<https://www.nationalarchives.gov.uk/doc/open-government-licence/version/3>) or write to the Information Policy Team, The National Archives, Kew, London TW9 4DU, or email: psi@nationalarchives.gov.uk.

Where we have identified any third party copyright information you will need to obtain permission from the copyright holders concerned.

This publication is available at <https://www.gov.uk/government/publications/email-security-standards/sender-policy-framework-spf>

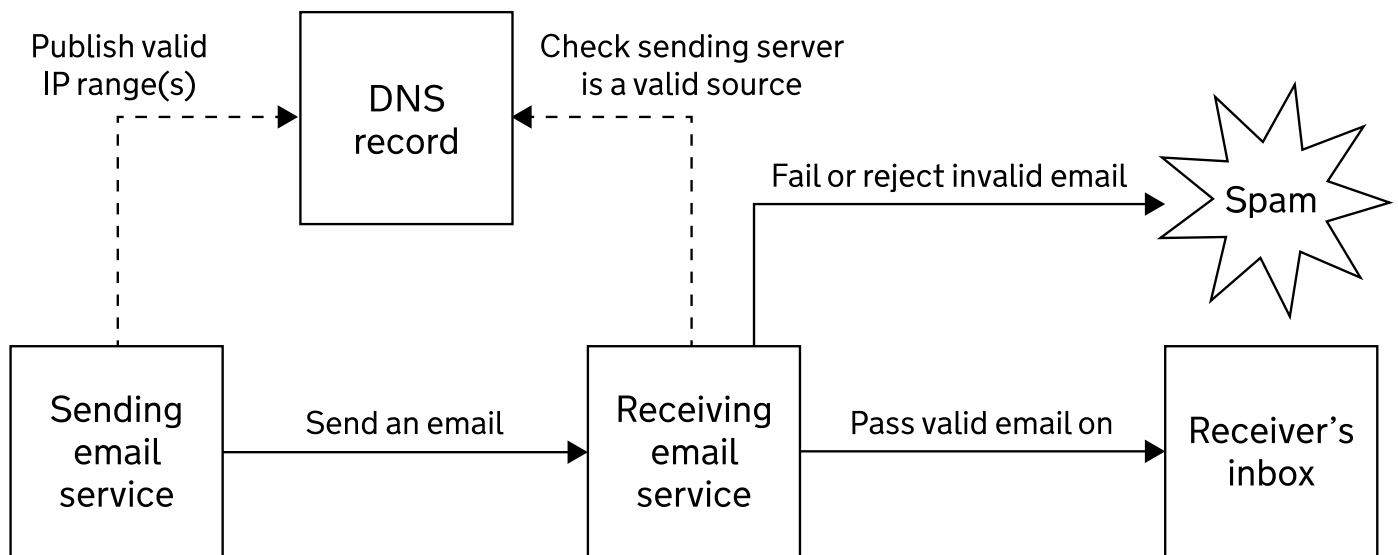
Sender Policy Framework (SPF) lets you publish a DNS record of all the domains or IP addresses you use to send email. Receiving email services check the record and know to treat email from anywhere else as spam.

You can include more than one sending service in your SPF record. For example, your corporate email service and an email marketing service.

Your SPF record also contains a qualifier option, which lets you:

- tell recipients to ignore your record while you test it
- mark, but not reject, email from an unknown source

How SPF works



An example SPF record looks like this:

```
v=spf1 include:spf.protection.outlook.com include:servers.mcsv.net ~all
```

In the example:

- `v=spf1` is an SPF record
- `include:` means email can only come from these sources
- `~all` considers any other email as a soft fail

Further email security guidance

All public sector organisations must follow guidance on how to set up email services securely (<https://www.gov.uk/guidance/set-up-government-email-services-securely>).

Openspf.org (<http://www.openspf.org/>) has detailed information on the SPF specification.

Print this page