Guidance

Using Sender Policy Framework (SPF) in your organisation

Published 19 February 2016

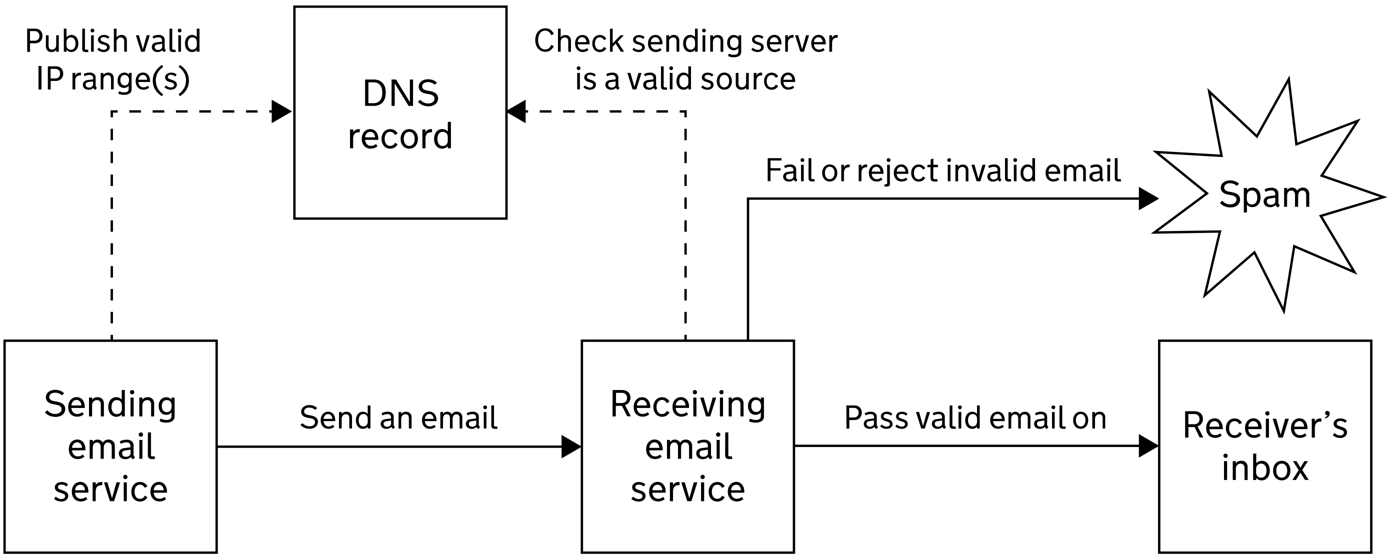
Sender Policy Framework (SPF) lets you publish a DNS record of all the domains or IP addresses you use to send email. Receiving email services check the record and know to treat email from anywhere else as spam.

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