GOV.UK

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 Domain-based Message Authentication, Reporting and Conformance (DMARC) in your organisation

Published 19 February 2016

## Contents



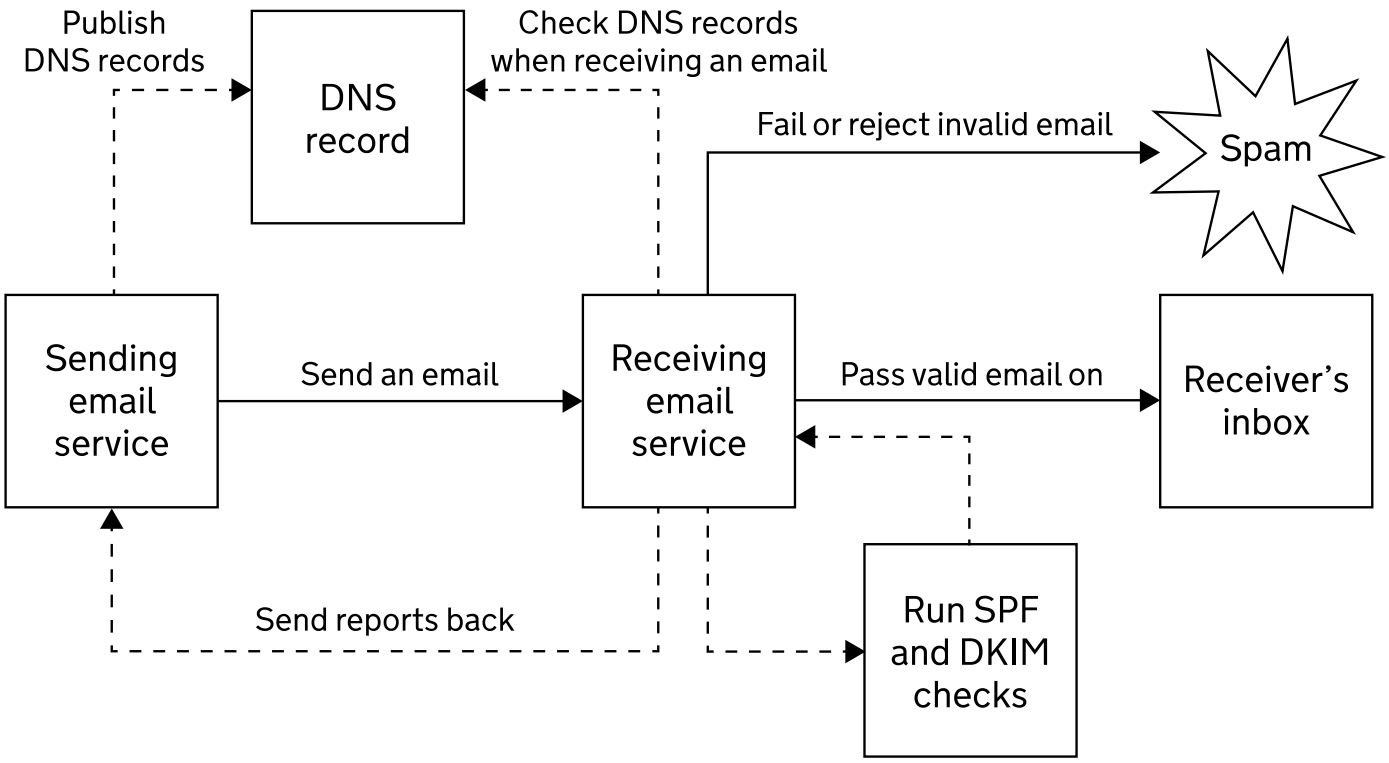
Print this page



This publication is available at https://www.gov.uk/government/publications/email-security-standards/domain-based-message-authentication-reporting-and-conformance-dmarc

Domain-based Message Authentication, Reporting and Conformance (DMARC) is an email standard that:

- confirms the sender's identity using Sender Policy Framework (SPF) (https://www.gov.uk/government/publications/email-security-standards/sender-policy-framework-spf) and DomainKeys Identified Mail (DKIM) (https://www.gov.uk/government/publications/email-security-standards/domainkeys-identified-mail-dkim)
- tells the recipient's email service what to do with emails that fail the check
- asks recipient email services to provide reports of where email comes from




The receiving email service uses SPF and DKIM to confirm the sender's identity. If the receiving email service confirms the sender's identity it will forward the email to the receiver's inbox. If the receiving email service cannot confirm the sender's identity it will mark the email as spam.

## Benefits of DMARC

By using DMARC, you can:

- help protect your users, employees and reputation from cybercrime
- reduce customer support costs relating to email fraud
- improve trust in the emails your organisation sends
- see the legitimate and fraudulent use of your domains via DMARC reports

## Setting up DMARC

Publish a text (TXT) record in your DNS like this one:

```
v=DMARC1; p=quarantine; pct=100; rua=mailto:dmarc@mydomain.gov.uk
```

This tells anyone receiving email from you that:

- you have a DMARC policy (`v=DMARC1`)
- any messages that fail DMARC checks should be treated as spam (`p=quarantine`)
- they should treat 100% of your messages this way (`pct=100`)
- they should send reports of email received back to you (`rua=mailto:dmarc@mydomain.gov.uk`)

## 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).

Dmarc.org has more information on DMARC (https://dmarc.org/). You can also read this guide to creating a DMARC record (https://www.dmarcanalyzer.com/how-to-create-a-dmarc-record/) and implementation guides for cloud-based email services like G Suite and Office 365.

Google uses DMARC to show when email is authenticated in Gmail (https://gmail.googleblog.com/2016/02/making-email-safer-for-you-posted-by.html).

Authenticated Receive Chain (http://arc-spec.org/) is a related standard that supports email authentication in indirect email flow.

Print this page