

GUIDE · TOMORIS TOOLBOX

Email Security: SPF, DKIM and DMARC in Five Steps

Rollout plan from the inventory to p=reject, based on RFC 7208, RFC 6376 and the DMARC standard RFC 9989

UPDATED

Oct 22, 2026

LENGTH

PDF, 7 pages

ONLINE

tomoris.com/en/downloads/e-mail-sicherheit-spf-dkim-dmarc

AT A GLANCE

5

Steps from the inventory to p=reject

10

DNS lookups at most for SPF (RFC 7208)

2048 bits

DKIM key recommended (RFC 8301)

1 month

at least per DMARC stage (RFC 9989)

WHO IT IS FOR

- IT managers and administrators of mail servers and Microsoft 365
- Companies whose domain is or could be misused for phishing
- Anyone who sends newsletters, invoices or tickets through external services

WHAT THIS COVERS

With SPF, DKIM and DMARC, you prove that emails using your domain really come from you and tell recipients how to handle forgeries. This plan takes you in five steps from the inventory to the p=reject policy, with sample DNS entries and the pitfalls described in the standards. It takes into account the DMARC standard RFC 9989 published in May 2026.

The DNS entries are examples using reserved example domains. Only adopt values after the inventory: a p=reject policy set too early can cause legitimate emails to be rejected.

CONTENTS

01	What checks what	2
02	Step 1: Record all senders	3
03	Step 2: Publish SPF	3
04	Step 3: DKIM for every sender	4
05	Step 4: DMARC in monitoring mode	4
06	Step 5: Via quarantine to reject	5
07	At a glance	6
08	Sources	6

01 —

What checks what

SPF, DKIM and DMARC in one table: what is checked, where the entry is located, which standard applies.

The three methods at a glance

METHOD	WHAT IT CHECKS	DNS ENTRY	STANDARD
SPF	whether the sending server is authorized to send for the domain in the envelope sender (MAIL FROM) or in the HELO, not the visible sender address	TXT at the domain, starts with v=spf1	RFC 7208
DKIM	whether the message is unchanged and comes from the signing domain (d=)	TXT under <selector>._domainkey.<domain>	RFC 6376, updated by RFC 8301
DMARC	whether the visible sender domain (From) matches a domain verified by SPF or DKIM (alignment); plus policy and reports	TXT under _dmarc.<domain>- , starts with v=DMARC1	RFC 9989 (obsoletes RFC 7489), reports RFC 9990

SPF alone says nothing about the visible sender address (RFC 7208, Section 11.2). Only DMARC links them: a message passes DMARC if at least one domain verified by SPF or DKIM aligns with the sender domain (RFC 9989, Section 5.3.5).

02 —

Step 1: Record all senders

Every service that sends with your domain needs matching SPF or DKIM, otherwise it will later fail DMARC.

Record every service that sends emails with your domain as the sender. Every legitimate sender will later need a passing SPF or DKIM result with an aligned domain; gaps must be closed before you publish a strict policy (RFC 9989, Section 5.1.6).

- ☐ Your own mail server or Microsoft 365 or Exchange Online
- ☐ Newsletter and marketing services
- ☐ CRM, ticket system, web shop and accounting (invoice delivery)
- ☐ Devices and applications that send via SMTP, such as scanners, monitoring and web forms
- ☐ Service providers that send on your behalf
- ☐ Domains and subdomains that do not send any email at all

03 —

Step 2: Publish SPF

One entry per domain, no more than ten DNS lookups, ending with -all or ~all.

DNS: SPF

```
; Microsoft 365 and your own server (192.0.2.25 is an example address)
example.com.      IN TXT "v=spf1 ip4:192.0.2.25 include:spf.protection.outlook.com -all"

; Name under which no email is sent
www.example.com.  IN TXT "v=spf1 -all"
```

- Exactly one SPF entry per domain: multiple entries with **v=spf1** result in a permanent error (permerror, RFC 7208, Section 4.5).
- No more than 10 DNS lookups caused by **include**, **a**, **mx**, **ptr**, **exists** and **redirect** during the entire evaluation, otherwise permerror (Section 4.6.4). The entries of included service providers count too.
- Do not use **ptr** (Section 5.5).
- **-all** (fail) explicitly declares servers not listed as unauthorized, **~all** (softfail) is only a weak statement; recipients should not reject on the basis of softfail alone (Sections 2.6.4, 2.6.5 and 8.5).

- Names that do not send email publish `v=spf1 -all` (Section 10.1.2).
- A TXT string holds no more than 255 characters. Longer entries are split into several strings, which the recipient concatenates without spaces (Section 3.3).

04 —

Step 3: DKIM for every sender

Sign with `rsa-sha256` and a 2048-bit key; the public key is in the DNS under the selector.

Each sender signs with its own key. You publish the public key as a TXT entry under `<selector>._domainkey.<domain>`; the selector (s=) and domain (d=) appear in the signature of every message (RFC 6376, Sections 3.5 and 3.6.2.1).

DNS: DKIM (key shortened)

```
mail2026._domainkey.example.com. IN TXT "v=DKIM1; k=rsa; p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA..."
```

- Sign only with `rsa-sha256`; `rsa-sha1` must not be used for signing or verifying (RFC 8301, Section 3.1).
- Keys of at least 1024 bits, 2048 bits recommended (RFC 8301, Section 3.2).
- Microsoft 365: DKIM is set up via two CNAME entries `selector1._domainkey` and `selector2._domainkey`; `Get-DkimSigningConfig` shows the exact targets. When created via PowerShell, 1024 bits is the default; `Rotate-DkimSigningConfig -KeySize 2048` switches to 2048 bits.
- DKIM signatures usually survive forwarding, SPF does not. Anyone who publishes `p=reject` therefore must not rely on SPF alone and must sign validly with DKIM (RFC 9989, Section 7.4).

05 —

Step 4: DMARC in monitoring mode

Publish `p=none` with a report address, evaluate reports automatically, close gaps.

DNS: DMARC in monitoring mode

```
_dmarc.example.com. IN TXT "v=DMARC1; p=none; rua=mailto:dmarc-berichte@example.com"
```

- `p=none` expresses no preference for handling failures (monitoring mode). With `rua`, you receive aggregate reports on all servers that send with your domain (RFC 9989, Sections 5.1.4 and 5.1.5).
- The reports are intended for automated processing; use an analysis tool or service (Section 5.1.5).
- If the report mailbox is in a different domain, that domain must consent, for example with a TXT entry `example.com._report._dmarc.example.net` containing `v=DMARC1` (RFC 9990).
- Failure reports (`ruf`) contain content from individual messages; most recipients do not send them for privacy reasons (RFC 9989, Section 10.2). Aggregate reports remain the recommended means (RFC 9991).
- Every legitimate sender without aligned SPF or DKIM is fixed before a strict policy applies (RFC 9989, Section 5.1.6).

06 —

Step 5: Via quarantine to reject

At least one month of `p=none`, just as long with `p=quarantine`, then `p=reject`, with an eye on mailing lists.

Stages up to `p=reject` (RFC 9989, Section 7.4)



p=none Monitor

`v=DMARC1; p=none; rua=mailto:...` – At least one month.



p=quarantine Quarantine

`v=DMARC1; p=quarantine; rua=mailto:...` – Just as long; compare the results with the monitoring phase.



p=reject Reject

`v=DMARC1; p=reject; rua=mailto:...` – Permanently, once all legitimate senders pass.

- `t=y` marks a policy in testing: recipients apply one level less, so for `p=reject` only quarantine (RFC 9989, tag `t`). The former `pct` tag no longer exists since RFC 9989; older guides, including Microsoft's, still mention it.
- Subdomains: `sp` applies to existing subdomains, `np` to non-existent ones; if both are missing, `p` applies (RFC 9989, tags `sp` and `np`).
- Mailing lists: according to RFC 9989, domains whose users post to mailing lists on the internet should not publish `p=reject`; anyone who does so anyway should inform users that participation in mailing lists may be impaired (Section 7.4).

DNS: domain with no email traffic at all

```
parked.example.com.      IN TXT "v=spf1 -all"
_dmarc.parked.example.com. IN TXT "v=DMARC1; p=reject;"
parked.example.com.      IN MX  0 .
```

The null MX entry `MX 0 .` states that the domain does not accept email; there must be no other MX entry alongside it, and domains used as senders should not publish it (RFC 7505). For unused domains, Microsoft recommends DMARC entries stating that no email may ever come from them, and no DKIM entries.

07 —

At a glance

The seven points to check off, from the sender inventory to the secured secondary domain.

- ☐ All senders are recorded, including external services and devices.
- ☐ Exactly one SPF entry, no more than 10 DNS lookups, ending with `-all` or `~all`.
- ☐ DKIM for every sender with `rsa-sha256` and a 2048-bit key.
- ☐ DMARC with `p=none` and `rua`; the reports are evaluated.
- ☐ All legitimate senders pass DMARC with an aligned domain.
- ☐ `p=quarantine`, then `p=reject`; mailing lists are taken into account.
- ☐ Domains without email traffic are secured with SPF, DMARC and null MX.

NEXT STEP

Check It Yourself or Put It into Practice Together

CHECK FOR FREE

Email security check (German)

tomoris.com/tools/email-security-check

DNS security check (German)

tomoris.com/tools/dns-security-check

DISCUSS IMPLEMENTATION

Get in Touch

tomoris.com/en/contact

contact@tomoris.com

08 —

Sources

All statements are supported by sources. Legislation applies in its current version.

- | | |
|---|---|
| <p>1 RFC 7208: Sender Policy Framework (SPF)
Sections 2.6, 3.3, 4.5, 4.6.4, 5.5, 8.5, 10.1.2, 11.2
www.rfc-editor.org/rfc/rfc7208</p> | <p>2 RFC 6376: DomainKeys Identified Mail (DKIM) Signatures
Sections 3.5, 3.6.1, 3.6.2.1
www.rfc-editor.org/rfc/rfc6376</p> |
| <p>3 RFC 8301: Cryptographic Algorithm and Key Usage Update to DKIM
Sections 3.1 and 3.2
www.rfc-editor.org/rfc/rfc8301</p> | <p>4 RFC 9989: Domain-Based Message Authentication, Reporting, and Conformance (DMARC)
Standards Track, May 2026, obsoletes RFC 7489
www.rfc-editor.org/rfc/rfc9989</p> |
| <p>5 RFC 9990: DMARC Aggregate Reporting
www.rfc-editor.org/rfc/rfc9990</p> | <p>6 RFC 9991: DMARC Failure Reporting
www.rfc-editor.org/rfc/rfc9991</p> |

- | | |
|--|--|
| <p>7 RFC 7489: DMARC (previous version, Informational, March 2015)
www.rfc-editor.org/rfc/rfc7489</p> <p>9 Microsoft Learn: Set up DKIM for Microsoft 365
learn.microsoft.com/defender-office-365/email-authentication-dk...</p> <p>11 Microsoft Learn: Set up SPF for Microsoft 365
learn.microsoft.com/defender-office-365/email-authentication-sp...</p> | <p>8 RFC 7505: A "Null MX" No Service Resource Record
www.rfc-editor.org/rfc/rfc7505</p> <p>10 Microsoft Learn: Set up DMARC for Microsoft 365
learn.microsoft.com/defender-office-365/email-authentication-dm...</p> |
|--|--|