# Email Security

## SPF (Sender Policy Framework)

SPF is an email authentication method that **specifies which mail servers are allowed to send emails on behalf of your domain**. This helps receiving servers detect and block **unauthorized senders**, reducing the risk of spam and phishing using your domain.

- **Joker.com mailboxes:** SPF records are automatically created, so no action is needed.
- **Other mail services:** You need to create an SPF TXT record yourself as described here. Instructions for adding SPF records can be found here

> If you create an **Email Forwarding** at Joker.com, an SPF record is **not** created automatically. It is strongly recommended to **create** and **set up an SPF record** for forwards - especially if you forward emails to providers such as Gmail - to ensure proper email delivery.

**How it works:**

1. When an email is sent, the receiving server checks your SPF record.
2. If the sending server is listed in your SPF record, the email passes authentication.
3. If it’s not listed, the email may be marked as spam or rejected.

## DKIM (DomainKeys Identified Mail)

DKIM adds a **digital signature to your outgoing emails**, ensuring that the message **hasn’t been tampered with** and that it really comes from your domain. This improves trust with email providers and recipients.

- **Joker.com mailboxes:** DKIM records are automatically set up.
- **Other mail services:** You need to create a DKIM TXT record yourself. Instructions for adding DKIM records can be found here

**How it works:**

1. Your mail server signs each outgoing email with a **private key**.
2. The receiving server uses the **public key in your DKIM record** to verify the signature.
3. If the signature matches, the email passes authentication; if not, it may be flagged as suspicious.

# DMARC (Domain-based Message Authentication, Reporting & Conformance)

**What is DMARC?**
DMARC (Domain-based Message Authentication, Reporting & Conformance) is an email authentication standard that helps protect your domain from email spoofing and phishing. It works with SPF and DKIM to tell receiving mail servers how to handle emails that fail authentication.

**What does a DMARC record help you with?**
A DMARC record helps you:

- Prevent attackers from sending fake emails using your domain
- Improve email deliverability
- Gain visibility into who is sending email on behalf of your domain
- Protect your brand and users from phishing

**What should I do before setting up DMARC?**
Before setting up DMARC, make sure that you have **SPF and DKIM** records in place for your domain.

> If you are using Joker Mailboxes, **SPF and DKIM** are set up automatically.

**How is a DMARC record added?**
A DMARC record is added as a DNS TXT record for your domain. The basic format of a DMARC record starts with `v=DMARC1; p=`, followed by your policy.

- In the DNS configuration section, choose "TXT" as record type.
- The Name field should be set to `_dmarc`.
- In the Content field, paste your DMARC policy (example below).

**What does a simple DMARC record look like?**
A simple DMARC record for monitoring only looks like:

v=DMARC1; p=none; rua=mailto:dmarc@example.com;

**Explanation:**

- `v=DMARC1` – DMARC version (required)
- `p=none` – Monitor only, no enforcement
- `rua=` – Email address where aggregate reports are sent

> Starting with `p=none` allows you to monitor email traffic without blocking anything. Once you review reports and confirm legitimate senders are properly authenticated, you can gradually move to a stricter policy (`quarantine` then `reject`) as you gain confidence in your email sending practices and ensure that legitimate emails are properly authenticated.

**What are the available DMARC policies?**

- `p=none` – Monitor only, no action taken on failed messages
- `p=quarantine` – Place failing messages in spam/junk folder
- `p=reject` – Block delivery of failing messages completely

**Example of a strict policy:**

v=DMARC1; p=reject; rua=mailto:dmarc@example.com;

**What information do DMARC reports show?**
DMARC reports show:

- Which servers send email for your domain
- Whether emails pass or fail SPF/DKIM
- Potential abuse or misconfiguration

Reports are sent in XML format to the email address specified in `rua`.

**How can I check if my DMARC record is working?**

- Use online DMARC lookup tools like DMARC Analyzer, MXToolbox, or Google Admin Toolbox
- Run a DNS TXT lookup for `_dmarc.example.com`
- Wait for DMARC reports to arrive at your reporting address

---

Revision #10
Created 2026-03-19 10:32:12 UTC by Admin
Updated 2026-07-03 13:31:12 UTC by Administrator