E-Mail-Sicherheit

SPF (Sender Policy Framework)

SPF ist eine E-Mail-Authentifizierungsmethode, die **festlegt, welche Mailserver berechtigt sind, E-Mails im Namen Ihrer Domain zu versenden**. Dies hilft empfangenden Servern dabei, **nicht autorisierte Absender** zu erkennen und zu blockieren, und reduziert das Risiko von Spam und Phishing über Ihre Domain.

- **Joker.com-Postfächer:** SPF-Einträge werden automatisch erstellt, es sind keine weiteren Schritte erforderlich.
- **Andere E-Mail-Dienste:** Sie müssen selbst einen SPF-TXT-Eintrag erstellen, wie hier beschrieben. Anleitungen zum Hinzufügen von SPF-Einträgen finden Sie hier

> Wenn Sie bei Joker.com eine **E-Mail-Weiterleitung** einrichten, wird **kein** SPF-Eintrag automatisch erstellt. Es wird jedoch dringend empfohlen, einen SPF-Eintrag für Weiterleitungen **zu erstellen** und **zu konfigurieren** – insbesondere, wenn Sie E-Mails an Anbieter wie Gmail weiterleiten –, um eine ordnungsgemäße Zustellung der E-Mails zu sicherstellen.

So funktioniert es:

1. Wenn eine E-Mail gesendet wird, prüft der empfangende Server Ihren SPF-Eintrag.
2. Ist der sendende Server im SPF-Eintrag aufgeführt, besteht die E-Mail die Authentifizierung.
3. Ist er nicht aufgeführt, kann die E-Mail als Spam markiert oder abgewiesen werden.

DKIM (DomainKeys Identified Mail)

DKIM versieht Ihre ausgehenden E-Mails mit einer **digitalen Signatur** und stellt so sicher, dass die Nachricht **nicht verändert wurde** und tatsächlich von Ihrer Domain stammt. Dies stärkt das Vertrauen bei E-Mail-Anbietern und Empfängern.

- **Joker.com-Postfächer:** DKIM-Einträge werden automatisch eingerichtet.

- **Andere E-Mail-Dienste:** Sie müssen selbst einen DKIM-TXT-Eintrag erstellen.

  Anleitungen zum Hinzufügen von DKIM-Einträgen finden Sie hier

So funktioniert es:

1. Ihr Mailserver signiert jede ausgehende E-Mail mit einem **privaten Schlüssel**.
2. Der empfangende Server nutzt den **öffentlichen Schlüssel in Ihrem DKIM-Eintrag**, um die Signatur zu verifizieren.
3. Stimmt die Signatur überein, besteht die E-Mail die Authentifizierung; andernfalls wird sie möglicherweise als verdächtig eingestuft.

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

Was ist DMARC?
DMARC (Domain-based Message Authentication, Reporting & Conformance) ist ein E-Mail-Authentifizierungsstandard, der Ihre Domain vor E-Mail-Spoofing und Phishing schützt. Er arbeitet zusammen mit SPF und DKIM und teilt empfangenden Mailservern mit, wie mit E-Mails umzugehen ist, die die Authentifizierung nicht bestehen.

Wozu dient ein DMARC-Eintrag?
Ein DMARC-Eintrag hilft Ihnen dabei:

- Angreifer daran zu hindern, gefälschte E-Mails unter Ihrer Domain zu versenden
- Die E-Mail-Zustellbarkeit zu verbessern
- Transparenz darüber zu gewinnen, wer E-Mails im Namen Ihrer Domain versendet
- Ihre Marke und Nutzer vor Phishing zu schützen

Was sollte ich vor der Einrichtung von DMARC tun?
Stellen Sie vor der Einrichtung von DMARC sicher, dass für Ihre Domain bereits **SPF- und DKIM**-Einträge vorhanden sind.

> Wenn Sie Joker-Postfächer verwenden, werden **SPF und DKIM** automatisch eingerichtet.

Wie wird ein DMARC-Eintrag hinzugefügt?
Ein DMARC-Eintrag wird als DNS-TXT-Eintrag für Ihre Domain angelegt. Das Grundformat eines DMARC-Eintrags beginnt mit `v=DMARC1; p=`, gefolgt von Ihrer Richtlinie.

- Wählen Sie im DNS-Konfigurationsbereich „TXT" als Eintragstyp.
- Das Feld „Name" sollte auf `_dmarc` gesetzt werden.
- Fügen Sie im Feld „Inhalt" Ihre DMARC-Richtlinie ein (Beispiel siehe unten).

Wie sieht ein einfacher DMARC-Eintrag aus?
Ein einfacher DMARC-Eintrag zur reinen Überwachung sieht so aus:

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

Erläuterung:

- `v=DMARC1` – DMARC-Version (erforderlich)
- `p=none` – Nur Überwachung, keine Durchsetzung
- `rua=` – E-Mail-Adresse, an die aggregierte Berichte gesendet werden

> Mit `p=none` zu beginnen ermöglicht es Ihnen, den E-Mail-Verkehr zu überwachen, ohne etwas zu blockieren. Sobald Sie die Berichte ausgewertet und bestätigt haben, dass legitime Absender ordnungsgemäß authentifiziert sind, können Sie schrittweise zu einer strengeren Richtlinie wechseln (`quarantine`, dann `reject`), wenn Sie ausreichend Vertrauen in Ihre E-Mail-Versandpraktiken gewonnen haben und sichergestellt ist, dass legitime E-Mails korrekt authentifiziert werden.

Welche DMARC-Richtlinien stehen zur Verfügung?

- `p=none` – Nur Überwachung, bei fehlgeschlagenen Nachrichten wird keine Maßnahme ergriffen
- `p=quarantine` – Fehlgeschlagene Nachrichten werden in den Spam-/Junk-Ordner verschoben
- `p=reject` – Zustellung fehlgeschlagener Nachrichten wird vollständig blockiert

Beispiel einer strengen Richtlinie:

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

Welche Informationen enthalten DMARC-Berichte?
DMARC-Berichte zeigen:

- Welche Server E-Mails für Ihre Domain versenden
- Ob E-Mails SPF/DKIM bestehen oder nicht
- Möglichen Missbrauch oder Fehlkonfigurationen

Berichte werden im XML-Format an die in `rua` angegebene E-Mail-Adresse gesendet.

Wie kann ich überprüfen, ob mein DMARC-Eintrag funktioniert?

- Verwenden Sie Online-DMARC-Überprüfungstools wie DMARC Analyzer, MXToolbox oder die Google Admin Toolbox

- Führen Sie eine DNS-TXT-Abfrage für `_dmarc.beispiel.de` durch
- Warten Sie, bis DMARC-Berichte an Ihre Berichtsadresse eintreffen

---

Revision #2
Created 2026-03-20 16:45:01 UTC by Admin
Updated 2026-03-20 16:59:29 UTC by Admin