

E-Mail-Zustellung

Damit Mails ankommen und nicht im Spam landen.

- [SPF, DKIM und DMARC einrichten](#)
- [Auf einer Blacklist gelandet: was tun?](#)

SPF, DKIM und DMARC einrichten

Ohne SPF, DKIM und DMARC landen Mails immer öfter im Spam oder werden abgewiesen. Gmail, Microsoft und Yahoo verlangen sie inzwischen von allen, die größere Mengen versenden. So richtest du sie Schritt für Schritt ein.

Prüfen kannst du jeden Schritt mit dem [Mail-Check](#).

1. SPF: Wer darf für die Domain senden?

SPF ist ein TXT-Eintrag auf der Domain selbst. Er listet die Server, die Mails im Namen der Domain verschicken dürfen.

```
example.de.  TXT  "v=spf1 mx include:_spf.google.com -all"
```

- `mx`: die eigenen Mailserver aus dem MX-Eintrag
- `include:...`: Server eines Dienstleisters (Microsoft 365: `include:spf.protection.outlook.com`, Google: `include:_spf.google.com`)
- `ip4:203.0.113.10`: eine einzelne IP, z. B. für einen Drucker oder ein Shopsystem
- `-all`: alles andere ist nicht erlaubt. `~all` (Softfail) ist die weichere Variante für die Umstellungsphase.

Fallstricke:

- Nur **ein** SPF-Eintrag pro Domain. Zwei Einträge machen beide ungültig.
- Höchstens **10 DNS-Lookups** (jedes `include`, `a`, `mx` zählt, auch verschachtelt). Der Mail-Check zählt sie für dich.

2. DKIM: Mails signieren

Der Mailserver signiert jede ausgehende Mail. Der öffentliche Schlüssel liegt im DNS unter `<selektor>._domainkey.<domain>.`

- **Microsoft 365:** im Defender-Portal unter E-Mail-Authentifizierung DKIM aktivieren, dann die zwei angezeigten CNAME-Einträge (`selector1`, `selector2`) anlegen.
- **Google Workspace:** Admin-Konsole → Apps → Gmail → E-Mails authentifizieren, Schlüssel erzeugen, TXT-Eintrag `google._domainkey` anlegen, dann „Authentifizierung starten“.
- **Eigener Server** (Postfix mit OpenDKIM, Stalwart, Mailcow ...): Schlüssel im Server erzeugen lassen und den angezeigten TXT-Eintrag übernehmen.

Den Selektor einer echten Mail findest du im Header `DKIM-Signature` hinter `s=`.

3. DMARC: Was passiert mit Fälschungen?

DMARC verbindet SPF und DKIM mit der Absenderadresse, die der Empfänger sieht, und legt fest, was mit Mails passiert, die durchfallen.

Fang beobachtend an:

```
_dmarc.example.de.  TXT  "v=DMARC1; p=none; rua=mailto:dmarc@example.de"
```

- `p=none`: nur beobachten, nichts blockieren
- `rua=`: Adresse für tägliche Sammelberichte der großen Anbieter

Nach zwei bis vier Wochen Berichte auswerten. Tauchen dort nur noch deine eigenen Dienste auf, verschärfst du schrittweise:

```
v=DMARC1; p=quarantine; pct=25; rua=mailto:dmarc@example.de  
v=DMARC1; p=reject; rua=mailto:dmarc@example.de
```

4. Prüfen

1. [Mail-Check](#) für die Domain laufen lassen, alles sollte grün sein.
2. Eine Testmail an ein Gmail-Konto schicken und dort „Original anzeigen“: SPF, DKIM und DMARC sollten `PASS` zeigen.
3. Die IP des Mailservers im [Blacklist-Check](#) prüfen.

Domains, die gar keine Mails senden

Auch die solltest du absichern, damit niemand sie fälscht:

example.de.	TXT	"v=spf1 -all"
_dmarc.example.de.	TXT	"v=DMARC1; p=reject"

Auf einer Blacklist gelandet: was tun?

Mails kommen zurück mit Meldungen wie „blocked using zen.spamhaus.org“ oder landen plötzlich überall im Spam? Dann steht deine IP oder Domain vermutlich auf einer Sperrliste (DNSBL).

1. Prüfen, wo du stehst

Im [Blacklist-Check](#) die IP deines Mailservers prüfen und zusätzlich die Domain. Bei der Domain prüft der Check auch die IPs der Mailserver aus dem MX-Eintrag.

Wichtig ist, **welche** Liste: Spamhaus (SBL, XBL, CSS, DBL), Barracuda und SpamCop werden von vielen Empfängern benutzt. Kleine Listen haben kaum Wirkung.

2. Die Ursache finden

Listen tragen nicht zufällig ein. Häufige Gründe:

- **gehacktes Postfach:** Ein Passwort wurde abgefischt und das Konto verschickt Spam. Prüfe im Mailserver, welche Konten auffällig viele Mails senden.
- **offenes Kontaktformular** oder Newsletter-Anmeldung ohne Bestätigung, die von Bots benutzt wird
- **infizierter Rechner** im Netz, der direkt über Port 25 nach außen sendet (typisch für Spamhaus XBL/CBL)
- **Mailserver ohne Reverse DNS** oder mit generischem Namen wie `ip-203-0-113-10.provider.net`

3. Ursache abstellen

- betroffene Passwörter ändern, 2FA einschalten
- Formulare mit Captcha bzw. Double-Opt-in absichern
- ausgehenden Port 25 in der Firewall für alles außer dem Mailserver sperren

- Reverse DNS beim Hoster setzen lassen: Der PTR der IP soll auf den Namen des Mailservers zeigen, und der Name zurück auf die IP

4. Austragen

Erst **nach** dem Abstellen der Ursache, sonst bist du gleich wieder drin. Im Blacklist-Check steht bei jeder Liste der Link zum Austragen. Viele Listen tragen auch nach einigen Tagen von selbst aus, wenn nichts mehr kommt.

Sonderfall: Spamhaus PBL

Auf der PBL stehen IPs von **privaten Internetanschlüssen**. Das ist kein Vorwurf, sondern bedeutet: Von hier sollen Mails nicht direkt verschickt werden, sondern über einen Mailserver (Smarthost). Betreibst du dort einen Mailserver, nutze für den Versand einen Relay-Dienst deines Providers.