

Mail-Check

tools.ngosu-corp.de/mail prüft, ob eine Domain sauber für E-Mail eingerichtet ist. Du kannst eine Domain oder eine ganze Mail-Adresse eingeben.

Was geprüft wird

Prüfung	Worum es geht
MX	Welche Server Mails annehmen, mit Reverse DNS ihrer IPs
SPF	Welche Server im Namen der Domain senden dürfen. Gezählt werden auch die DNS-Lookups, mehr als 10 machen den Eintrag ungültig
DKIM	Signaturschlüssel für ausgehende Mails
DMARC	Was Empfänger mit Mails tun sollen, die SPF/DKIM nicht bestehen, und wohin Berichte gehen
MTA-STS	Erzwingt verschlüsselte Zustellung an deine Mailserver
TLS-RPT	Adresse für Berichte über Verschlüsselungsprobleme

Zu jedem Fund gibt es einen Hinweis, was fehlt und wie man es behebt.

DKIM-Selektor

DKIM-Schlüssel liegen unter `<selektor>._domainkey.<domain>`. Gängige Selektoren (Google, Microsoft 365, Mailjet ...) probiert der Check automatisch. Deinen eigenen findest du im Header einer gesendeten Mail im Feld `DKIM-Signature` hinter `s=`. Trag ihn dann im Feld *DKIM-Selektor* ein.

Häufige Befunde

- **„SPF: zu viele Lookups“**: `include:` verschachtelt zu tief. Entferne Dienste, die du nicht mehr nutzt, oder fasse IPs direkt zusammen.
- **„DMARC fehlt“**: Fang mit `v=DMARC1; p=none; rua=mailto:dmarc@example.de` an, wertet die Berichte aus und stell später auf `quarantine` oder `reject`.

- „**MX ohne Reverse DNS**“: Der PTR-Eintrag der Mailserver-IP fehlt oder passt nicht. Den setzt dein Hoster.

Eine Schritt-für-Schritt-Anleitung kommt ins Regal „Wissen für IT-Admins“.

Im Terminal

```
curl tools.ngosu-corp.de/mail/example.de  
curl "tools.ngosu-corp.de/mail/example.de?selector=s1&json"
```

Erstellt: 2026-10-16 11:50:01 CEST von cherry

Zuletzt aktualisiert: 2026-10-17 22:53:47 CEST von cherry