

Wie vertrauenswürdig sind Mails von beispiel-gmbh.ch?

Geprüft wurden nur öffentliche DNS-Einträge, die jeder empfangende Mailserver auch sieht. Mail läuft über: Microsoft 365.



Dringender Handlungsbedarf

2 Punkte gefährden die Zustellung Ihrer Mails oder erlauben Fälschungen in Ihrem Namen. 2 weitere sollten verbessert werden. Die Korrektur ist klein und schnell gemacht.

Bereich	Ampel	Befund
Mails empfangen MX	● Grün	Eingetragen, 1 Server erreichbar (Microsoft 365).
Wer in Ihrem Namen senden darf SPF	● Rot	Es gibt keinen SPF-Eintrag, der festlegt, wer in Ihrem Namen Mails senden darf.
Digitale Unterschrift DKIM	● Gelb	Ihre Mails sind nicht digital unterschrieben (DKIM), obwohl Microsoft 365 das kann.
Schutzregel gegen Fälschungen DMARC	● Rot	Ihre Domain hat 2 DMARC-Einträge statt einem, deshalb ignorieren Empfänger alle.
Zusatzschutz MTA-STS, TLS-RPT, BIMI	● Neutral	Nicht eingerichtet; freiwillig, für kleine Firmen nicht nötig.

1 Was das für Sie bedeutet

- **Es gibt keinen SPF-Eintrag, der festlegt, wer in Ihrem Namen Mails senden darf.**
Empfänger können echte und gefälschte Mails von Ihnen nicht unterscheiden, und Ihre Mails landen öfter im Spam.
- **Ihre Domain hat 2 DMARC-Einträge statt einem, deshalb ignorieren Empfänger alle.**
Ihre Domain ist damit so ungeschützt, als gäbe es keine Regel.
- **Ihre Mails sind nicht digital unterschrieben (DKIM), obwohl Microsoft 365 das kann.**
Ohne Unterschrift gelten Ihre Mails bei den grossen Postfachanbietern als weniger vertrauenswürdig, und bei Weiterleitungen fällt der letzte Echtheitsnachweis weg.
- **Ihre DMARC-Regel beobachtet nur (p=none) und hält gefälschte Mails nicht auf.**
Gefälschte Mails mit Ihrer Adresse werden weiter zugestellt; p=none ist nur als Startstufe gedacht.

2 Mein Angebot

Leistung	Inhalt	CHF
Paket E-Mail-Schutz Empfohlen für Sie	SPF, DKIM und DMARC: jeder Eintrag fertig zum Einfügen, mit Anleitung für Ihre Informatik; DMARC mit Berichten schrittweise bis zur Quarantäne-Stufe begleitet	490.00
Einzelne Korrektur	Ein Bereich, etwa SPF zusammenführen, DKIM einschalten oder MX korrigieren: Eintrag und Anleitung für Ihre Informatik	150.00

Fixpreise, keine Mehrwertsteuer. Die Einträge setzt Ihre Informatik bei Ihrem DNS-Anbieter, genau nach meiner Anleitung im technischen Anhang. Ich prüfe jeden Schritt von aussen nach und brauche keinen Zugang zu Ihren Systemen; Ihr Mailbetrieb läuft ohne Unterbruch weiter. Auf Wunsch prüfe ich Ihre Einträge danach jeden Monat neu und schreibe Ihnen, was sich verändert hat (Monatskontrolle, CHF 29 pro Monat).

Korrekturen für Ihre Informatik

Einzutragen beim DNS-Anbieter der Domain beispiel-gmbh.ch. Stand der Abfrage: 20. Oktober 2026, 21.47 Uhr.

1 Es gibt keinen SPF-Eintrag, der festlegt, wer in Ihrem Namen Mails senden darf.

- Einen TXT-Eintrag an der Domain setzen. Alle weiteren Absender ergänzen (Website-Formular, Newsletter, Buchhaltung, Drucker), danach höchstens 10 DNS-Abfragen und genau ein SPF-Eintrag.

Name	Typ	Wert
beispiel-gmbh.ch	TXT	v=spf1 include:spf.protection.outlook.com ~all

2 Ihre Domain hat 2 DMARC-Einträge statt einem, deshalb ignorieren Empfänger alle.

v=DMARC1; p=none | v=DMARC1; p=none;

- Alle Einträge an _dmarc löschen bis auf einen; Ziel siehe unten.

Name	Typ	Wert
_dmarc.beispiel-gmbh.ch	TXT	v=DMARC1; p=none; rua=mailto:dmarc@beispiel-gmbh.ch; fo=1

3 Ihre Mails sind nicht digital unterschrieben (DKIM), obwohl Microsoft 365 das kann.

Geprüft: selector1, selector2

- Im Microsoft Defender-Portal unter E-Mail & Zusammenarbeit > Richtlinien > E-Mail-Authentifizierung > DKIM die Domain wählen.
- Die beiden angezeigten CNAME-Einträge selector1._domainkey und selector2._domainkey beim DNS-Anbieter setzen (Werte aus dem Portal übernehmen).
- Nach einigen Minuten im Portal «Mit DKIM-Signaturen signieren» einschalten.

Name	Typ	Wert
selector1._domainkey.beispiel-gmbh.ch	CNAME	Wert aus dem Defender-Portal
selector2._domainkey.beispiel-gmbh.ch	CNAME	Wert aus dem Defender-Portal

4 Ihre DMARC-Regel beobachtet nur (p=none) und hält gefälschte Mails nicht auf.

v=DMARC1; p=none

- Startwert setzen, danach den Stufenplan unten befolgen.

Name	Typ	Wert
_dmarc.beispiel-gmbh.ch	TXT	v=DMARC1; p=quarantine; pct=25; rua=mailto:dmarc@beispiel-gmbh.ch; fo=1

5 DMARC in Stufen (TXT an _dmarc.beispiel-gmbh.ch)

Zeitpunkt	Wert	Wirkung
Woche 0	v=DMARC1; p=none; rua=mailto:dmarc@beispiel-gmbh.ch; fo=1	Berichte sammeln, alle echten Absender finden
Woche 2–4	v=DMARC1; p=quarantine; pct=25; rua=mailto:dmarc@beispiel-gmbh.ch; fo=1	erst ein Viertel der Fälschungen in den Spam
danach	v=DMARC1; p=quarantine; rua=mailto:dmarc@beispiel-gmbh.ch; fo=1	alle Fälschungen in den Spam (Stufe 50 % nach Bedarf)
nach 2–4 sauberen Wochen	v=DMARC1; p=reject; rua=mailto:dmarc@beispiel-gmbh.ch; fo=1	Fälschungen werden abgewiesen

Gehen echte Mails verloren, eine Stufe zurück und den Absender in SPF/DKIM aufnehmen.

6 Heutige Einträge

MX	10 beispielgmbh-ch02e.mail.protection.outlook.com
SPF	-
DMARC	v=DMARC1; p=none v=DMARC1; p=none;
DKIM	keiner gefunden
MTA-STS	-
TLS-RPT	-
BIMI	-