

How trustworthy is mail from beispiel-gmbh.ch?

I checked only public DNS records, the same ones every receiving mail server sees. Mail runs through: Microsoft 365.



Urgent action needed

2 points put the delivery of your mail at risk or allow forgeries in your name. 2 more should be improved. The fix is small and quick to make.

Area	Status	Finding
Receiving mail MX	● Green	Set, 1 server reachable (Microsoft 365).
Who may send in your name SPF	● Red	There is no SPF record stating who may send mail in your name.
Digital signature DKIM	● Amber	No DKIM key found at the selectors checked, although Microsoft 365 can sign your mail digitally.
Policy against forgery DMARC	● Red	Your domain has 2 DMARC records instead of one, so receivers ignore all of them.
Extra protection MTA-STS, TLS-RPT, BIMI	● Neutral	Not set up; optional and not needed for small businesses.

1 What this means for you

- **There is no SPF record stating who may send mail in your name.**
Receivers cannot tell your real mail from forged mail, and your mail lands in spam more often.
- **Your domain has 2 DMARC records instead of one, so receivers ignore all of them.**
That leaves your domain as unprotected as if there were no policy at all.
- **No DKIM key found at the selectors checked, although Microsoft 365 can sign your mail digitally.**
Without a signature the big mailbox providers trust your mail less, and when mail is forwarded the last proof that it is genuine is lost.
- **Your DMARC policy only monitors (p=none) and does not stop forged mail.**
Forged mail with your address is still delivered; p=none is only meant as a starting stage.

2 My offer

Service	What it includes	EUR
Mail protection package Recommended for you	SPF, DKIM and DMARC: every record ready to paste, with instructions for your IT team; DMARC with reports, guided step by step up to the quarantine stage	490.00
Single fix	One area, such as merging SPF, switching on DKIM or correcting MX: the record and instructions for your IT team	150.00

Fixed prices, no VAT added. Your IT team enters every record at your DNS provider, exactly following my instructions in the technical appendix. I check each step from the outside and never access your systems; your mail keeps running without interruption. If you wish, I then check your records again every month and tell you what has changed (monthly re-check, EUR 29 a month).

Fixes for your IT team

For your IT team to enter at the DNS provider of beispiel-gmbh.ch, exactly as given here; I check every step from the outside and never access your systems. Lookup made on 20 October 2026, 21:47.

1 There is no SPF record stating who may send mail in your name.

- Set a TXT record on the domain. Add every other sender (website form, newsletter, accounting, printers); after that, no more than 10 DNS lookups and exactly one SPF record.

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

2 Your domain has 2 DMARC records instead of one, so receivers ignore all of them.

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

- Delete every record at _dmarc except one; the target value is below.

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

3 No DKIM key found at the selectors checked, although Microsoft 365 can sign your mail digitally.

Checked: selector1, selector2

- In the Microsoft Defender portal, under Email & collaboration > Policies & rules > Threat policies > Email authentication settings > DKIM, select the domain.
- Set the two CNAME records shown, selector1._domainkey and selector2._domainkey, at the DNS provider (copy the values from the portal).
- After a few minutes, switch on 'Sign messages for this domain with DKIM signatures' in the portal.

Name	Type	Value
selector1._domainkey.beispiel-gmbh.ch	CNAME	value from the Defender portal
selector2._domainkey.beispiel-gmbh.ch	CNAME	value from the Defender portal

4 Your DMARC policy only monitors (p=none) and does not stop forged mail.

v=DMARC1; p=none

- Set the starting value, then follow the staged plan below.

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

5 DMARC in stages (TXT at _dmarc.beispiel-gmbh.ch)

When	Value	Effect
week 0	v=DMARC1; p=none; rua=mailto:dmarc@beispiel-gmbh.ch; fo=1	collect reports, find every real sender
weeks 2 to 4	v=DMARC1; p=quarantine; pct=25; rua=mailto:dmarc@beispiel-gmbh.ch; fo=1	first a quarter of forgeries to spam
after that	v=DMARC1; p=quarantine; rua=mailto:dmarc@beispiel-gmbh.ch; fo=1	all forgeries to spam (50% stage if needed)
after 2 to 4 clean weeks	v=DMARC1; p=reject; rua=mailto:dmarc@beispiel-gmbh.ch; fo=1	forgeries are rejected

If real mail goes missing, go back one stage and add the sender to SPF/DKIM.

6 Current records

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