Email Desk

Email delivery, sorted properly.

EMAIL HEALTH CHECK

WillcoxMedia

willcoxmedia.net

Overall status

Needs attention

64

/ 100

PROVIDER
Microsoft 365

REPORT DATE
15 May 2026

PRODUCT
GBP 99 Email Health Check

PREPARED BY
Email Desk

This sample shows the intended paid deliverable: branded, downloadable and suitable to email automatically to the customer after the intake and test email have been received.

Executive summary

Your domain has working Microsoft 365 mail routing and SPF is present, but the setup needs attention before it can be considered properly healthy.

What looks good

MX records point to Microsoft 365. SPF exists and includes Microsoft 365. The test email produced useful real-world authentication evidence.

Needs attention

No public DMARC record was found. SPF contains a duplicated IP entry. Public DKIM selectors were not visible at the custom domain.

Plain-English conclusion

The setup is not broken, but it is unfinished. The highest-value fixes are to add a safe starter DMARC record, verify Microsoft 365 DKIM at the custom domain, tidy SPF, and run a separate QuickBooks invoice test because invoice emails may not use the same route as normal mailbox email.

Why this matters

Gmail, Outlook/Hotmail and other providers use SPF, DKIM, DMARC, reputation and message behaviour to decide whether to trust mail. Missing or inconsistent authentication does not guarantee spam placement, but it gives filters fewer positive trust signals.

DNS findings

MX records - Pass

Mail routes to Microsoft 365: willcoxmedia-net.mail.protection.outlook.com. No urgent MX change is recommended unless mail is intentionally routed elsewhere.

SPF - Review

Current SPF: v=spf1 ip4:185.41.10.120 ip4:185.41.10.120 include:spf.protection.outlook.com -all. This includes Microsoft 365, but the hosting IP appears twice. Confirm whether the IP still sends legitimate mail, then keep one copy or remove it if stale.

DMARC - Missing

Public lookup for _dmarc.willcoxmedia.net returned no answer. Add a starter monitoring record such as: v=DMARC1; p=none; rua=mailto:dmarc-reports@willcoxmedia.net; adkim=s; aspf=s. Move towards quarantine/reject only after all legitimate senders are known.

DKIM and real test email

DKIM public selectors - Needs confirmation

Public selector checks for selector1._domainkey.willcoxmedia.net and selector2._domainkey.willcoxmedia.net did not return expected Microsoft 365 selector records. Confirm DKIM is enabled for the custom domain in Microsoft 365 and publish the exact CNAME values Microsoft provides.

Received test email - Mixed evidence

The test email arrived and included Microsoft authentication evidence. Some upstream Microsoft ARC results showed SPF/DKIM/DMARC pass signals, while final receiving-side evidence included dkim=none and dmarc=none. This should be retested after DKIM/DMARC DNS corrections.

QuickBooks invoice path - Test separately

The reported problem mentions invoices from QuickBooks. Those messages may use a different sending path from normal Microsoft 365 mailbox emails. Send a real QuickBooks test invoice and inspect its SPF, DKIM, DMARC and Return-Path alignment.

Priority action plan

1

Add starter DMARC

Begin with p=none and reporting. Do not jump straight to reject until all legitimate senders are known.

2

Verify Microsoft 365 DKIM

Enable DKIM for willcoxmedia.net and publish the selector CNAME records Microsoft gives you.

3

Tidy SPF

Remove duplicate IP entries and verify whether the hosting server still sends legitimate mail.

4

Test QuickBooks

Send a real QuickBooks test invoice and analyse the headers separately from normal mailbox mail.

5

Retest and compare

Send fresh tests to Gmail, Outlook/Hotmail and Email Desk after changes. Confirm the visible authentication results improve.

Suggested order

Fix DMARC and DKIM first, then investigate QuickBooks invoice delivery. This avoids chasing symptoms before the domain authentication foundation is clean.

Want Email Desk to make the fixes?

The GBP 99 Email Health Check gives you the diagnosis and recommended fixes. If you would rather not edit DNS, Microsoft 365, QuickBooks or website settings yourself, the next step is a Delivery Fix.

Delivery Fix can include SPF/DKIM/DMARC implementation, Microsoft 365 checks, third-party sender testing, before/after evidence, and a short final change summary.

Delivery Fix: quoted separately, typically from GBP 350 depending on scope.

Important limits

This report cannot guarantee inbox placement. Gmail, Microsoft, Yahoo and other providers apply private filtering rules that change over time. The report identifies technical setup issues, authentication evidence and sensible next steps to reduce avoidable delivery problems.

Email Desk
Email delivery, sorted properly.