Email authentication audit for Sample client · 24 Nov 2026

# northwind-foods.com

Mail provider detected: Microsoft 365 · score 30/100 · live public DNS, nothing guessed

**F**

| 3 | 0 | 2 | 1 |
|---|---|---|---|
| High | Medium | Low | Passing |

## Fix plan, in order

1. 2 SPF records (only 1 allowed)
2. No DKIM signature found
3. No valid DMARC policy

## Findings

High

### 2 SPF records (only 1 allowed)

With two SPF records, SPF returns an error on every message, so it never passes. Usually left behind after switching mail providers.

```
Delete both and publish one merged record:
TXT  @  "v=spf1 a mx include:secureserver.net include:spf.protection.outlook.com
~all"
(ptr dropped: deprecated and slow. Remove any include for a provider you no longer
use.)
```

High

### No DKIM signature found

Without DKIM, DMARC can only pass through SPF, which breaks on forwarding. Bulk sender rules at Gmail, Yahoo and Microsoft require it.

```
Defender portal > Email authentication > DKIM > enable, then publish the two
selector1/selector2 CNAMEs it shows
```

High

### No valid DMARC policy

Nothing tells receivers what to do with mail that fails checks, so spoofed mail in your name gets delivered. Also required for bulk senders since 2024.

```
TXT  _dmarc  "v=DMARC1; p=none; rua=mailto:dmarc@northwind-foods.com; fo=1"
(start in monitor mode, move to quarantine after 2-4 weeks of clean reports)
```

Low

### No MTA-STS

Inbound mail can be downgraded to unencrypted in transit. Nice to have, not urgent.

```
Publish _mta-sts TXT plus a policy file at mta-sts.northwind-foods.com/.well-known/mta-sts.txt, start in testing mode.
```

Low

### No TLS reporting

You won't hear about failed encrypted deliveries.

```
TXT  _smtp._tls  "v=TLSRPTv1; rua=mailto:tls@northwind-foods.com"
```

Passing

### No blocklist listings found

Checked mail server IPs on SpamCop and Barracuda.

## Raw results

| | |
|---|---|
| MX | 1 MX records |
| SPF | 2 SPF records (only 1 allowed) |
| DKIM | none on common selectors |
| DMARC | no DMARC record |

DKIM checked on 49 common selector names; a custom selector can exist. DNS changes, so rerun after every fix.