

[Partner logo]

Scan date: 18 Oct 2026

# Email security and domain health report

Prepared for Example Retail Ltd by Example Web Agency

|                      |                   |                    |
|----------------------|-------------------|--------------------|
| 3<br>domains checked | 4<br>issues found | 2<br>high priority |
|----------------------|-------------------|--------------------|

## What we found

| Domain           | Check        | What we found                                                                                | Priority | Suggested fix                                                  |
|------------------|--------------|----------------------------------------------------------------------------------------------|----------|----------------------------------------------------------------|
| shop.example.com | DMARC policy | Policy is set to “none”, so spoofed emails are reported but not blocked.                     | High     | Move to quarantine, then reject, after reviewing the reports.  |
| example.org      | DMARC record | No DMARC record is published, so anyone can send mail that appears to come from this domain. | High     | Publish a DMARC record starting with monitoring, then enforce. |
| example.com      | SPF record   | The record needs 11 DNS lookups; the limit is 10, so SPF can fail for legitimate mail.       | Medium   | Remove unused includes or flatten the record.                  |
| example.net      | MTA-STS      | No policy is published, so encryption for email in transit is not required.                  | Low      | Publish an MTA-STS policy in testing mode first.               |

## What this means

When email authentication is not enforced, others can send messages that look like they come from your company. That can damage customer trust, send your real mail to spam, and make phishing against your customers easier. The two high-priority items are the quickest wins.

## Recommended next steps

1. Fix the high-priority items first; most are a single DNS change.
2. Turn on continuous monitoring so new problems are caught when they appear, not months later.
3. Re-scan after the changes to confirm everything is fixed. [Partner name] can do this for you.

## How this report was produced

This report uses only publicly visible information, such as public DNS records. No systems were accessed or tested beyond what any visitor could see. Findings reflect the settings at the scan date and may change. To have this report removed or to ask a question, contact [Partner name] at the details below.