



# Your Tidy Cyber check

Domain: example-bakery.co.uk    Checked: 2026-10-14 10:00 (UK time)    Scope: passive public checks only

## 2 high risks: scammers can send emails pretending to be you

2 high, 2 medium, 1 low and 4 optional item(s). Tidiness score: **18/100** (7 of 16 checks passed). Even large companies rarely score 100. What matters is fixing the high risks.

## In plain English

Things you are doing well: Mail servers (MX) published, TLS certificate valid, Modern TLS protocol, HTTP redirects to HTTPS. The most important thing to fix: SPF record - This domain receives email (MX found) but has no SPF record, so anyone can more easily send email pretending to be you; DMARC policy - v=DMARC1; p=none (policy: none) - monitoring only: fake emails using your name are still delivered. All fixes listed are configuration changes your web host, email provider or IT support can usually make quickly.

## Priority fixes

| # | Priority | Issue                                                                                                                                        | How to fix                                                                             | CE theme                   |
|---|----------|----------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------|----------------------------|
| 1 | High     | <b>SPF record</b><br>This domain receives email (MX found) but has no SPF record, so anyone can more easily send email pretending to be you. | Add a TXT record e.g. 'v=spf1 include: -all'.                                          | Secure configuration       |
| 2 | High     | <b>DMARC policy</b><br>v=DMARC1; p=none (policy: none) - monitoring only: fake emails using your name are still delivered.                   | Move DMARC policy from p=none to p=quarantine, then p=reject, once reports look clean. | Secure configuration       |
| 3 | Medium   | <b>Legacy TLS 1.0/1.1 disabled</b><br>Fail: server still accepts TLS 1.0/1.1                                                                 | Turn off TLS 1.0 and 1.1 in server/CDN settings.                                       | Security update management |
| 4 | Medium   | <b>Header: strict-transport-security</b><br>Missing. Forces browsers to always use HTTPS.                                                    | Add 'Strict-Transport-Security: max-age=31536000; includeSubDomains'.                  | Secure configuration       |
| 5 | Low      | <b>DNSSEC</b><br>DNSSEC not enabled/validated                                                                                                | Enable DNSSEC at your domain registrar/DNS host (often a single toggle).               | Secure configuration       |
| 6 | Low      | <b>Header: content-security-policy</b><br>Missing. Limits which scripts can run.                                                             | Add a Content-Security-Policy (start in Report-Only mode).                             | Secure configuration       |
| 7 | Low      | <b>Header: referrer-policy</b><br>Missing. Limits data leaked in links to other sites.                                                       | Add 'Referrer-Policy: strict-origin-when-cross-origin'.                                | Secure configuration       |
| 8 | Low      | <b>Header: permissions-policy</b><br>Missing. Restricts browser features like camera/mic.                                                    | Add a Permissions-Policy header disabling unused features.                             | Secure configuration       |
| 9 | Low      | <b>Software version not disclosed</b><br>Server: 'Apache/2.4.41 (Ubuntu)'<br>X-Powered-By: 'PHP/7.4.3'                                       | Hide version numbers in Server/X-Powered-By headers.                                   | Security update management |

## All checks

| Result | Check                       | Detail                                                                                                                  |
|--------|-----------------------------|-------------------------------------------------------------------------------------------------------------------------|
| PASS   | Mail servers (MX) published | mx1.example-mail.net, mx2.example-mail.net                                                                              |
| FIX    | SPF record                  | This domain receives email (MX found) but has no SPF record, so anyone can more easily send email pretending to be you. |

| Result | Check                               | Detail                                                                                              |
|--------|-------------------------------------|-----------------------------------------------------------------------------------------------------|
| FIX    | DMARC policy                        | v=DMARC1; p=none (policy: none) - monitoring only: fake emails using your name are still delivered. |
| PASS   | DKIM signing key (common selectors) | Found selector(s): default                                                                          |
| FIX    | DNSSEC                              | DNSSEC not enabled/validated                                                                        |
| PASS   | TLS certificate valid               | Valid, trusted chain, issuer Let's Encrypt, expires 12 Jan 2027 (90 days)                           |
| PASS   | Modern TLS protocol                 | Pass: Negotiated TLSv1.3 (checked via a normal HTTPS handshake to this hostname).                   |
| FIX    | Legacy TLS 1.0/1.1 disabled         | Fail: server still accepts TLS 1.0/1.1                                                              |
| PASS   | HTTP redirects to HTTPS             | http://example-bakery.co.uk ended at https://example-bakery.co.uk/                                  |
| FIX    | Header: strict-transport-security   | Missing. Forces browsers to always use HTTPS.                                                       |
| FIX    | Header: content-security-policy     | Missing. Limits which scripts can run.                                                              |
| PASS   | Header: x-content-type-options      | Present: nosniff. Stops browsers guessing file types.                                               |
| PASS   | Header: x-frame-options             | Present: SAMEORIGIN.                                                                                |
| FIX    | Header: referrer-policy             | Missing. Limits data leaked in links to other sites.                                                |
| FIX    | Header: permissions-policy          | Missing. Restricts browser features like camera/mic.                                                |
| FIX    | Software version not disclosed      | Server: 'Apache/2.4.41 (Ubuntu)' X-Powered-By: 'PHP/7.4.3'                                          |

## How this maps to Cyber Essentials

Cyber Essentials has five control themes: **Firewalls**, **Secure configuration**, **Security update management**, **User access control** and **Malware protection**. This external check can only see what is public, so it mainly informs Secure configuration and Security update management. Firewalls, user access control (e.g. MFA, admin accounts) and malware protection on your devices need the full self-assessment questionnaire, which Tidy Cyber can help you work through.

## Important: this report is not a certification

This is an automated, passive review of publicly visible configuration (DNS records, one TLS handshake and normal web requests). It did not scan ports, test for vulnerabilities, or attempt access. It is **not** Cyber Essentials or Cyber Essentials Plus certification, an audit or a penetration test, and does not guarantee your organisation is secure or will pass certification. Certification is only issued by IASME-licensed certification bodies. Results reflect the date of the check. Some checks (e.g. DKIM) use common selectors and may miss custom setups. Domain authorisation: SAMPLE REPORT: fictional business and made-up findings.

**SAMPLE REPORT for a fictional business (example-bakery.co.uk). Your report shows your own domain's results.**