CRITICAL END SECURITY

CYBERSECURITY

ASSESSMENT REPORT

Client: **Maplewood Family Dental**
Domain: **maplewoodfamilydental.com**
Date: May 20, 2026

41 **HIGH RISK**
out of 100

Prepared by Critical End Security | Confidential — not for distribution

Score Breakdown

Category	Score	Max
SSL/TLS Certificate	6	10
Security Headers	2	10
Email Security	3	10
Subdomain Exposure	7	10
HTTP→HTTPS Redirect	5	5
Cookie Security	2	5
CMS Detection	3	5
WHOIS / Domain Info	4	5
Dark Web Exposure	2	10
DNS Security	1	5

Broken Link Scanner	3	5
Port Scan	1	5
Google Safe Browsing	5	5
Typosquat Check	2	5
TLS Certificate Chain	5	5

Executive Summary

Maplewood Family Dental's web presence shows **significant cybersecurity exposure** with an overall risk score of **41 / 100 (HIGH RISK)**. The scan identified **17 issues across 15 security categories**, including missing email authentication, weak HTTP security headers, an outdated SSL configuration, and exposed administrative subdomains.

The most pressing risks center on **email impersonation** (no DMARC enforcement) and **credential exposure** (3 employee emails found in past data breaches). These two issues alone create a realistic path for attackers to impersonate your practice in phishing emails sent to patients — a serious concern for a healthcare business handling sensitive records.

The good news: most issues are quick wins. Implementing DMARC, adding the missing security headers, and rotating breached credentials can be done in **under a week** and would push your score above 70.

Top 3 Priorities

[1] Enable DMARC email authentication — Without it, attackers can send emails appearing to come from @maplewoodfamilydental.com. *Effort: Low. Impact: High.*

[2] Rotate compromised credentials — 3 staff emails were found in known breaches. *Effort: Low. Impact: High.*

[3] Add missing HTTP security headers — 4 of 6 critical headers are missing, leaving the site open to XSS and clickjacking. *Effort: Low. Impact: Medium.*

SSL / TLS Certificate

Grade: B

• Certificate is valid and trusted, issued by Let's Encrypt

• Expires in 47 days — within renewal window

• Supports TLS 1.2 and 1.3 — good

• **Issue:** TLS 1.0 and 1.1 still enabled — these are deprecated and exploitable

Recommendation: Disable TLS 1.0 and 1.1 in your web server config. Most hosting providers let you do this from the SSL settings panel. Takes about 5 minutes.

Security Headers

Score: 2 / 6 headers present

Missing headers:

• `Strict-Transport-Security` — forces HTTPS

• `Content-Security-Policy` — prevents script injection

• `X-Frame-Options` — blocks clickjacking

• `Referrer-Policy` — controls data leakage to other sites

Recommendation: These can all be added with a few lines in your web server or via Cloudflare's "Transform Rules." Quick and high-impact.

Email Security

• **SPF:** Configured but uses `~all` (soft fail) instead of `-all` (hard fail)

• **DKIM:** Not detected on the primary selector

• **DMARC: Missing entirely** — this is the biggest gap

Why this matters: Without DMARC, mail servers have no instruction to reject emails forged to look like yours. An attacker can register a lookalike domain or simply spoof yours and send phishing emails to your patients pretending to be the practice.

Recommendation: Start with a DMARC record set to `p=none` to monitor, then move to `p=quarantine` after 2 weeks of clean reports.

Subdomain Exposure

Out of 30 subdomains tested, **2 are publicly accessible:**

• `admin.maplewoodfamilydental.com` — appears to be a login page

• `staging.maplewoodfamilydental.com` — returns a default Apache page

Recommendation: Restrict `admin` to your office IP range. Take `staging` offline or place it behind HTTP basic auth.

HTTP → HTTPS Redirect

✓ All HTTP requests redirect to HTTPS. No issues found.

Cookie Security

The site sets **3 cookies**, none of which use the `Secure` flag, and only 1 uses `HttpOnly`.

Recommendation: If you're using WordPress, install the "Really Simple SSL" plugin — it auto-fixes this. Otherwise, your developer can set these flags in the cookie configuration.

CMS Detection

Platform: WordPress 6.2.1 (current latest is 6.5.3)

Risk: Running 4 versions behind. Several disclosed vulnerabilities exist for 6.2.x.

Recommendation: Update WordPress core and all plugins immediately. Schedule monthly updates going forward.

WHOIS / Domain Info

• **Registrar:** GoDaddy

• **Expires:** 2027-03-15 (renewal is healthy)

• **Privacy:** Domain privacy is enabled — good

No issues found.

Dark Web Exposure

3 staff email addresses found in known data breaches:

• `info@maplewoodfamilydental.com` — exposed in Adobe breach (2013)

• `admin@maplewoodfamilydental.com` — exposed in LinkedIn breach (2021)

• One additional address — exposed in MyFitnessPal breach (2018)

Recommendation: Reset passwords on these accounts immediately, and enable 2FA on all email accounts. Assume any password used at the time of breach is publicly known.

DNS Security

• **DNSSEC:** Not enabled

• **CAA records:** None configured

Recommendation: Enable DNSSEC through your DNS provider (most offer it for free). Add a CAA record limiting certificate issuance to Let's Encrypt to prevent rogue certificates.

Broken Link Scanner

Crawled homepage and 18 internal links. **2 broken links found:**

• `/old-services.html` returns 404

• An external link to a removed insurance partner page

Recommendation: Remove the broken links or update them. Broken links erode trust and may expose orphaned pages.

Port Scan

Open ports: 80, 443, 22, 3306

• **Port 22 (SSH):** Open to the public internet — this is a serious exposure

• **Port 3306 (MySQL):** Database port exposed publicly — should never be reachable from the internet

Recommendation: Restrict SSH to your office IP. Move MySQL behind the firewall (bind to localhost only). These two changes are the highest priority on this report.

Google Safe Browsing

✓ Domain is clean. Not flagged for malware or phishing.

Typosquat Detection

5 lookalike domains found registered:

• `maplewoodfamilydental.co` — parked

• `maplewood-family-dental.com` — parked

• `maplewoodfamliydental.com` (typo) — redirects to a different dental practice

• 2 others — parked with no content

Recommendation: Monitor these monthly. The misspelling redirecting to a competitor is the most concerning — consider purchasing it defensively (typically $10–15/year per domain).

TLS Certificate Chain

✓ Full certificate chain is valid and properly configured. No issues.

What To Do Next

The fastest path to a meaningfully better security posture for Maplewood Family Dental is:

This week:

• Enable DMARC (p=none)

• Reset compromised email passwords + enable 2FA

• Close SSH and MySQL ports to the public internet

• Update WordPress core

Next 2 weeks:

• Add the 4 missing HTTP security headers

• Disable TLS 1.0 / 1.1

• Take down or lock the staging subdomain

• Enable DNSSEC and add CAA record

Ongoing:

• Monthly WordPress + plugin updates

• Quarterly re-scan to track progress

After implementing this week's items alone, your score should jump from **41 to roughly 68**. After all items, you should be comfortably above 85.

This report is confidential. If you have questions about any finding, reach out and we'll walk you through the fix.