



External Security Check

Sample Report

Practice	Example Family Dental (fictional — demo data)
Prepared by	Christian Chavez — BlackWall Security, Omaha, NE
Assessment type	External · non-intrusive · no access to your systems
What was checked	Everything visible to the public internet
Report ID	SAMPLE-0001
Prepared	Illustrative example

About this sample. This is an illustrative example built with fictional data to show the format, depth, and plain-English style of a real External Security Check. It is not an assessment of any real organization, and every finding below is invented for demonstration.

Executive summary

I looked at Example Family Dental the way a criminal does before an attack — entirely from the public internet, without touching any of your systems or seeing any patient data. The goal is simple: find the doors you didn't know were unlocked, before someone else does.

This check found **7 issues** — 3 that need attention soon, 2 worth fixing, and 2 minor. The three most urgent: your practice's email can be impersonated by anyone, remote access to a computer is open to the whole internet, and three staff logins have already appeared in known data breaches. None of these need new hardware to fix, and most can be resolved in a few days.

3	2	2
Fix soon (high)	Worth fixing (medium)	Minor (low)

Why this matters for a dental practice. You store protected health information, so a breach isn't only downtime and lost trust — it can trigger HIPAA reporting obligations and penalties. Each issue below notes what it puts at risk in plain terms.

What I found

HIGH

1. Anyone can send email that looks like it's from your practice

WHAT I FOUND

Your domain has no DMARC record and a weak SPF setting, so a scammer can send email that appears to come from your practice address.

WHY IT MATTERS

This is how patient-invoice fraud and staff phishing start. A criminal emailing your patients "as you" damages trust and can expose payment info.

WHAT TO DO

Add a DMARC record (start in monitoring mode) and tighten SPF; add DKIM signing. Usually a same-day change with your email/DNS provider.

HIGH

2. Remote Desktop is open to the entire internet

WHAT I FOUND

A Remote Desktop (RDP) service on your office connection is reachable from anywhere on the internet, not just your staff.

WHY IT MATTERS

Internet-exposed RDP is one of the most common ways ransomware gets into small practices. Automated attacks find it within hours.

WHAT TO DO

Close RDP at the firewall and require a VPN, or restrict it to known addresses and enforce MFA. Priority fix.

HIGH

3. Three staff logins appear in known data breaches

WHAT I FOUND

Three email/password pairs tied to your domain were found in public breach databases from other websites staff had signed up to.

WHY IT MATTERS

Attackers try these leaked passwords against your Microsoft 365 and other logins ("credential stuffing"). Reused passwords make it easy.

WHAT TO DO

Reset those three accounts' passwords, confirm MFA is on, and move staff to a password manager so work logins are unique.

MEDIUM

4. Older Microsoft 365 sign-in method can skip MFA

WHAT I FOUND

Legacy authentication is still enabled on your Microsoft 365 tenant, which lets some sign-ins bypass multi-factor authentication.

WHY IT MATTERS

Even with MFA turned on, this older method leaves a side door open for account takeover.

WHAT TO DO

Disable legacy authentication and require MFA for all users via a Conditional Access policy.

MEDIUM

5. Your email 'from' protection is too permissive

WHAT I FOUND

Your SPF record ends in a soft setting (~all) that tells receivers to accept questionable mail instead of rejecting it.

WHY IT MATTERS

It weakens the protection above and makes spoofed mail more likely to reach inboxes.

WHAT TO DO

Move to a strict SPF policy (-all) once your legitimate senders are confirmed.

LOW

6. Firewall admin page is reachable from the internet**WHAT I FOUND**

The login page for your network firewall is visible publicly, though it does require a password.

WHY IT MATTERS

It gives attackers a target to guess passwords against and reveals the device model.

WHAT TO DO

Restrict management access to your internal network or a VPN.

LOW

7. Web server reveals its exact version**WHAT I FOUND**

Your website's server is publicly advertising its exact software version.

WHY IT MATTERS

It hands attackers a shortcut to find matching known vulnerabilities.

WHAT TO DO

Turn off version banners and keep the server patched.

SAMPLE

Your priority action plan

This week	Close internet-exposed RDP · reset the 3 breached logins and confirm MFA · add a DMARC record.
This month	Disable Microsoft 365 legacy authentication · tighten SPF and add DKIM · move staff to a password manager.
Then	Lock down firewall management access · remove server version banners · recheck in 90 days.

How I checked

This is an **external, non-intrusive** assessment. I use only publicly available sources — your domain's DNS and email records, public service and port discovery, and reputable breach databases. I don't log into anything, install anything, or attempt to exploit what I find, so there's no risk to your day-to-day operations and no access to patient data.

What this doesn't cover

An External Security Check is an outside-in snapshot — it's the fast, low-cost way to find your most exposed gaps. It does not watch your systems day to day (that's ongoing managed monitoring) and it doesn't go deep inside your network (that's a full penetration test, done only with your written authorization). This report is the starting point.

Next step. Want this run against your real practice? Email contact@blackwallsecurity.net or call (402) 819-9517.
— Christian Chavez, BlackWall Security, Omaha, NE.