SCOUTz

DOMAIN SCORECARD

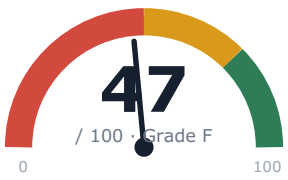
Example Workshop

OBSERVED AUGUST 30, 2026

VANTAGE — PUBLIC INTERNET ONLY

NO INTERNAL ACCESS USED

WHAT AN ATTACKER — OR AN INSURER — CAN SEE



47 / 100 · **GRADE F**

COMPOSITE OF 18 READABLE CHECKS
EXTERNAL SURFACE ONLY

From the open internet, your domain's public security hygiene is graded below — email authentication, encryption, DNS hardening, and lookalike exposure. Every check ran; every result is shown.

156 CHECK TYPES

6 FINDINGS

Point-in-time technical discovery. Not an underwritten guarantee, certification, or professional advice; holds no legal weight for insurance binding or compliance attestation.

COVERAGE — None OF None COLLECTORS READ · 0 DEGRADED THIS SCAN

18 CHECKS · 6 AREAS — ONE SQUARE EACH

Email Authentication — FINDING

senders declared · signed · enforcement pending

Website Encryption (TLS) — CLEAN

current certificates · strong versions · valid chain

DNS Hardening — CLEAN

zone locked · signing on · issuer list set

Security Headers — FINDING

transport pinned · browser rules missing

Lookalike Domains — CLEAN

no lookalike names observed

External Exposure — CLEAN

endpoints expected and current

VERIFIED CLEAN · NOT READABLE · FINDING

RE-CHECKED EVERY SCAN · ANYONE CAN VERIFY — IT'S PUBLIC

Dmarc Policy None

DMARC_POLICY_NON · August 30, 2026

What it is — You have the email-authenticity rule in place, but it's set to "watch only," so forged mail using your name is reported but still delivered.

Why it matters — Like a security camera that records the break-in but never locks the door.

The fix — Moving the policy from "watch" toward "reject" turns it into real protection — a staged DNS change.

Missing Security Header

MISSING_SECURITY · August 30, 2026

What it is — Your site doesn't tell browsers to stop guessing the type of the files it serves — a guess attackers can abuse to run a file as a script.

Why it matters — Like a mailroom that opens and acts on a package by guesswork instead of reading the label.

The fix — A one-line web-server setting ("nosniff") closes it.

Missing Security Header

MISSING_SECURITY · August 30, 2026

What it is — Your website doesn't tell browsers to block it from being secretly embedded inside another page — a trick used to overlay a fake "click here" on top of your real one.

Why it matters — Like letting someone tape a fake window-decal over your storefront — visitors think they're clicking your button, but they're clicking the scammer's.

The fix — A one-line web-server setting closes this — no code change.

Missing Security Header

MISSING_SECURITY · August 30, 2026

What it is — Your site doesn't limit how much of a visitor's browsing trail is shared with the outside sites they click through to.

Why it matters — Like handing every shop you walk into a note saying exactly which shop you came from.

The fix — A quick web-server setting tightens this.

Missing Security Header

MISSING_SECURITY · August 30, 2026

What it is — Your site doesn't switch off browser features it never uses — camera, microphone, location — leaving them available if a page is ever tampered with.

Why it matters — Like leaving every interior door unlocked because you've never needed them — better to lock the ones you don't use.

The fix — A quick web-server setting disables the unused features.

Spf Too Permissive

SPF_TOO_PERMISSI · August 30, 2026

What it is — Your email's "who's allowed to send as us" rule is set too loosely, which weakens your protection against someone forging your address.

Why it matters — Like a guest list that says "anyone who seems fine" instead of named people.

The fix — Tightening one DNS record (SPF) closes the gap.

INDUSTRY CONTEXT — NOT FROM YOUR SCAN

Impersonation scams open with what's publicly visible — a spoofable domain, a lookalike name. Everything on this page is what that outsider sees first — and the human element is present in 62% of breaches studied last year, which is why keeping this surface clean matters.

VERIZON DBIR · 2026

NEVER APPLIED TO YOUR COUNTS

COMPANY & EXPOSURE — PUBLIC, ORGANIZATION-LEVEL

Read directly from authoritative public records — registries, certificate logs, breach catalogs. Verified, not estimated.

0 **Historical breach records — a public fact**

Your domain appears in 0 historical breach corpus(es). The controls standing today and full detail are in your Breach Exposure report.

SOURCE: HAVE I BEEN PWNED · CC BY 4.0

1

Close the top finding

The highest-severity item above — already in this quarter's plan.

2

Harden DNS + headers

Signing, issuer rules, and browser headers — small settings, quick wins.

3

Lookalikes on watch

Observed names monitored; action only if one starts sending mail.

AUGUST 30	NEXT QUARTER	RE-READ
PUBLIC SURFACE READ — THIS PICTURE	ENFORCEMENT + HARDENING LAND	ANYONE CAN CHECK, IT'S PUBLIC

OPERATOR INTEL — NAMED

Signals suggest email is hosted on Google Workspace. signals suggest hosting on Amazon Web Services. website signals suggest Starfield Technologies; Go Daddy Website Builder 8.0.0000.

Cloud UC platform detected: Microsoft Teams / Skype for Business (SRV → sipdir.online.lync.com).

Industry benchmarks: Verizon DBIR 2026 / IBM 2025 — context only, not from this scan.

SCOUTz
YOUR PUBLIC FACE, KEPT CLEAN

EVERY CLAIM OBSERVED
EVERY CLAIM RE-VERIFIABLE

SEE THE NEXT EVIDENCE LAYER

SCOUTz can show much more with a customer-approved cloud review.

Schedule a conversation to explore the evidence boundary, likely scope, and the right next review for your MSP.

scoutzsecurity.io/open-beta