CLIENT RISK SCORECARD · PASSIVE OUTSIDE CHECK

# glowewebsites.com

Client: Sample: our own domain
Prepared by Your Agency Name
Checked 2026-11-28 · score 87/100

B

GRADE

| EMAIL SPOOFING | WEBSITE SOFTWARE | ENCRYPTION |
|---|---|---|
| Needs a look | Looks good | Looks good |

| DOMAIN | BLOCKLISTS | PUBLIC FOOTPRINT |
|---|---|---|
| Looks good | Looks good | Minor notes |

## What we saw, and how to fix it

- **DMARC is set to monitor only (p=none): fake email from @glowewebsites.com is reported but not blocked.**
  Fix: After checking the reports, change the DMARC policy to p=quarantine, then p=reject.
- **No anti-framing header: other sites can show this page inside a frame (clickjacking).**
  Fix: Add X-Frame-Options: SAMEORIGIN (or CSP frame-ancestors 'self').
- **Public certificate logs (crt.sh) didn't answer in time.**
- SPF lists which servers may send this domain's email.
- HTTPS works with a trusted certificate (issuer unknown).
- No outdated software visible in the page source.
- Domain registered until 2027-09-14 (NameCheap, Inc.).
- The web and mail servers we found (2) are on none of the spam blocklists we asked.

Passive outside check from public records only: public DNS records, the public homepage loaded once like any visitor, public certificate-transparency logs (crt.sh), public spam blocklists and the domain registry's RDAP record. Software versions are compared with WordPress.org's current releases, CISA's Known Exploited Vulnerabilities catalog and NIST's National Vulnerability Database. No login, no scanning, no tests for weaknesses. This is not a security audit, a certification or insurance advice: it lists what anyone can see from outside and how to fix it.