

Website and AI Agent Security Checklist

Security is non-negotiable. Two layers: the website, and the AI agent that talks to your visitors.

Layer 1: your website

- ☐ **Lock your registrar:** two-factor authentication on, transfer lock on, recovery email is yours.
- ☐ **DNS on Cloudflare** with DNSSEC turned on.
- ☐ **SPF, DKIM and DMARC** set up so nobody can send email as your business.
- ☐ **Prune** unused plugins, themes and third-party scripts.
- ☐ **Two-factor authentication** on email (first), hosting, DNS and payments.
- ☐ **Hold your own keys:** every account in your name, and a copy of your raw codebase you can take with you.
- ☐ **Commercial hosting:** a business site on a paid plan (free hobby tiers usually forbid commercial use).

Layer 2: your AI agent

- ☐ **One job:** the agent's task is written down, along with what it must never do.
- ☐ **Limited tools:** only the actions that job needs, nothing that changes your site, settings or other people's data.
- ☐ **Messages are content, not commands:** visitor text can never replace the agent's instructions (OWASP LLM01: Prompt Injection).
- ☐ **Private stays private:** internal notes, margins and the agent's own instructions are out of reach (LLM02, LLM07).
- ☐ **Monthly review:** read a sample of real conversations and look for anyone probing the agent.
- ☐ **Ask your vendor:** how is the agent scoped, what can it access, how does it handle hidden instructions, and do you own your code and accounts if you leave?

Worth paying for

- ☐ Legitimate commercial hosting, expertise to configure DNS and edge rules correctly, and work that produces real outcomes: leads and revenue.