Secure website launch checklist

Use this before publishing a new site or relaunching an existing one.

Click a box to mark it complete

- [ ] Hosting provider has patching, logs, backups, support, and incident response details
- [ ] Hosting, registrar, DNS, CDN, email, payment, and code accounts use MFA
- [ ] Admin access is limited to current people who need it
- [ ] HTTP redirects to HTTPS across the whole site
- [ ] TLS certificate covers all active domain versions and renews automatically
- [ ] No mixed-content warnings appear on key pages
- [ ] HSTS is configured only after HTTPS works everywhere
- [ ] CMS, plugins, themes, frameworks, and libraries are current
- [ ] Unused plugins, themes, scripts, demo content, and test files are removed
- [ ] User roles follow least privilege
- [ ] Forms validate input on the server
- [ ] Database queries use safe parameterized methods or framework protections
- [ ] File uploads are restricted, renamed, scanned where practical, and stored safely

Secure website launch checklist

Continue the launch review.

- [ ] Security headers are configured and tested
- [ ] Sensitive cookies use appropriate Secure, HttpOnly, and SameSite settings
- [ ] WAF, bot controls, and rate limits protect high-risk endpoints
- [ ] Third-party scripts and connected services are inventoried
- [ ] API keys and secrets are scoped, stored safely, and not exposed in browser code
- [ ] Registrar lock is enabled where available
- [ ] SPF, DKIM, and DMARC are configured for sending domains
- [ ] Backups include files and database
- [ ] At least one backup copy is stored away from production-only access
- [ ] A restore has been tested before launch
- [ ] Uptime, malware, file-change, vulnerability, login, and backup alerts are active
- [ ] Recovery steps are documented