MIDNIGHT WEBS

FREE RESOURCE · SECURITY CHECKLIST

Website Launch Security Checklist

Most hacked small-business sites were not targeted by clever attackers. They were running an outdated plugin, a reused password or an unprotected admin page. This checklist covers the 40-odd checks that close those gaps before a site goes live.

Updated November 2026 | 12 min read | 48 checks

WHO SHOULD USE IT	WHAT IT COVERS	HOW TO USE IT
Owners, project managers and developers preparing a launch	8 areas, from account access to launch-day tests	Give each item an owner and a date; "!" marks the ones not to skip

START HERE

If you only have an hour, do sections 1, 2 and 5. Two-factor login, a locked domain and a tested backup stop the most expensive failures.

TICK THE BOX WHEN DONE · MUST DO = HIGHEST IMPACT

01 Accounts and access

Weak or reused passwords remain the most common way into small-business sites, because attackers simply try passwords leaked from other services. Fix access first; it is also the cheapest work on this list.

- [ ] MUST DO **Turn on two-factor authentication everywhere that matters**
  Hosting, domain registrar, CMS admin, email and analytics. Prefer an authenticator app or passkey over SMS, which can be hijacked through SIM swapping.

- [ ] MUST DO **Use a password manager and generated passwords**
  Random passwords of 16+ characters, unique per service. NIST's current guidance favours length and uniqueness over forced complexity rules.

- [ ] **Give every person their own account**
  Shared logins make it impossible to see who changed what, or to remove one person without disrupting everyone.

- [ ] **Apply least privilege**
  An editor needs "Editor", not "Administrator". Keep the number of administrators to the people who truly need it, ideally two or three.

- [ ] **Remove people who left and unused accounts**
  Check hosting, registrar, Google/Meta accounts, payment tools and the CMS user list. Freelancers from previous projects are the usual leftovers.

- [ ] **Write down who owns each account**
  The domain, hosting and payment accounts should be registered to the business, not to a freelancer's personal email. Store recovery codes in the password manager.

HOW TO CHECK

Log out and open the admin URL in a private window: it must ask for a password and a second factor. Review the user list for names you do not recognise.

02 Domain, DNS and HTTPS

Your domain controls everything else. If someone takes it over, they control your site, your email and your reputation.

- [ ] MUST DO **Lock the domain and secure the registrar account**
  Enable the registrar lock (transfer lock) and 2FA, and turn on auto-renew. An expired domain can be re-registered by anyone, including people who will impersonate you.

- [ ] MUST DO **Serve every page over HTTPS with automatic renewal**
  Browsers now require it for payments and forms. Certificate lifetimes are shrinking (the industry agreed to move to 200 days from March 2026, then 100 days and 47 days), so manual renewal will not survive.

- [ ] **Redirect HTTP to HTTPS with a permanent (301) redirect**
  And pick one canonical version of the address, with or without "www", so the site does not exist in two places.

- [ ] **Publish SPF, DKIM and DMARC for your business email**
  Without them, criminals can send email that appears to come from your domain, and Gmail and Yahoo may route your real messages to spam. Start DMARC at `p=none` with reporting, then move to quarantine or reject once reports look clean.

- [ ] **Delete DNS records you no longer use**
  Old records pointing at cancelled services can be claimed by attackers (subdomain takeover). Check A, CNAME and MX records one by one.

- [ ] **Add HSTS once everything works over HTTPS**
  Start with a short max-age such as 300 seconds, test every subdomain, then raise it to a year. Only add "preload" if you are certain every subdomain will stay on HTTPS.

HOW TO CHECK

Run the domain through SSL Labs (ssllabs.com/ssltest) for the certificate, and `dig TXT yourdomain.com` and `dig TXT _dmarc.yourdomain.com` to confirm your email records exist.

03 Platform, software and server settings

Attackers scan the internet for known vulnerabilities in old software. Most successful attacks use a flaw that already had a public fix.

- [ ] MUST DO **Update the CMS, themes, plugins and server packages before launch**
  Then schedule updates, weekly at minimum for plugins. Enable automatic security updates where your platform supports them.

- [ ] **Delete everything you do not use**
  Deactivated plugins and themes can still be exploited. Fewer components means fewer updates and a smaller attack surface.

- [ ] **Remove demo content, test users and default accounts**
  A user called "admin" or "test" with a weak password is the first thing automated scripts try.

- [ ] MUST DO **Make sure private files are not public**
  Try yourdomain.com `/.env`, `/.git/config`, `/backup.zip` and `/phpinfo.php`. They must all return 404 or 403, never content. Keep secrets, API keys and database dumps out of the web root.

- [ ] **Switch off directory listing and in-dashboard file editing**
  On WordPress add `define('DISALLOW_FILE_EDIT', true);` to wp-config.php so a stolen admin login cannot edit code directly.

- [ ] **Add the standard security headers**
  `X-Content-Type-Options: nosniff`, a `Referrer-Policy`, clickjacking protection (frame-ancestors or X-Frame-Options) and, when you are ready to test it, a Content-Security-Policy. Check the result at securityheaders.com or Mozilla Observatory.

HOW TO CHECK

List every plugin and theme with its version, and compare it with the vendor's latest release. Anything abandoned for over a year should be replaced.

04 Forms, logins and payments

Every field a visitor can type into is an entry point. Assume all input is hostile until the server has checked it.

- [ ] MUST DO **Validate and sanitise on the server**
  Browser-side checks are for convenience only; anyone can bypass them. Use parameterised queries to stop SQL injection and escape output to stop script injection.

- [ ] MUST DO **Protect public forms from spam and abuse**
  Use a CAPTCHA alternative such as Cloudflare Turnstile, a honeypot field and rate limiting, so bots cannot flood your inbox or your email quota.

- [ ] **Add CSRF protection and safe cookies**
  Session cookies should be Secure, `HttpOnly` and `SameSite=Lax` (or Strict). This stops other sites from silently submitting actions as a logged-in user.

- [ ] **Restrict file uploads**
  Allow only the file types you need, check the real type and size, rename files and store them outside the web root where possible.

- [ ] **Collect only what you need**
  Every extra field is data you must protect and may have to delete on request under GDPR. If you do not use a phone number, do not ask for it.

- [ ] **Let a payment provider handle card data**
  Use hosted checkout or hosted fields (Stripe, PayPal, your bank's gateway) so card numbers never touch your server. That keeps your PCI compliance burden at its lightest level.

HOW TO CHECK

Submit each form with a long string, an apostrophe and `<b>bold</b>`. It should be accepted or rejected cleanly, and the formatting must never render on the page.

05 Backups and recovery

Backups protect you from hackers, but also from failed updates, accidental deletions and hosting problems. A backup you have never restored is only a hope.

- [ ] MUST DO **Automate daily backups of files and database**
  Keep at least 14 to 30 days of history so you can go back to before a problem started, not only to last night.

- [ ] MUST DO **Keep one copy somewhere else**
  The 3-2-1 rule: three copies, on two kinds of storage, one off-site. A backup stored in the same hosting account disappears with it.

- [ ] **Encrypt backups that contain personal data**
  Customer data in a backup is still customer data under GDPR.

- [ ] **Restore a backup to a test location before launch**
  Time how long it takes. That number is your real recovery time; most owners discover it during an emergency.

- [ ] **Write a one-page recovery note**
  Who can restore, where backups are stored, how to log in, and who to call at the host. Keep a copy that does not depend on the site being online.

HOW TO CHECK

Pick yesterday's backup, restore it on a staging copy and check that pages, images and form submissions all appear.

06 Monitoring and incident response

Compromised sites often run unnoticed for weeks. Monitoring shortens that to minutes.

- [ ] MUST DO **Set up uptime monitoring with alerts**
  Free tools such as UptimeRobot or Better Stack check every 1 to 5 minutes and message you when the site stops responding.

- [ ] **Watch certificate and domain expiry**
  Set alerts at 30 and 7 days before expiry, sent to two people.

- [ ] **Add Google Search Console and check Security issues**
  Google will tell you if it finds malware or hacked content, often before your visitors do.

- [ ] **Log failed logins and admin changes**
  Review them after launch, and alert on repeated failures from one address.

- [ ] **Send alerts to an inbox somebody reads**
  A security notification that goes to a former employee is not monitoring.

- [ ] **Prepare a short incident plan**
  Who to contact, how to put the site in maintenance mode, how to reset all passwords and who tells customers. Under GDPR, a personal-data breach must be reported to the authority within 72 hours of becoming aware.

HOW TO CHECK

Pause the site briefly in staging or point the monitor at a wrong URL. Confirm the alert arrives, and who receives it.

07 Privacy and legal basics

Collecting data creates obligations. A site that collects less and explains it clearly is safer and easier to defend.

- [ ] MUST DO **Publish a privacy policy that matches reality**
  List what you collect, why, who receives it (analytics, email provider, payment processor) and how long you keep it.

- [ ] MUST DO **Ask for cookie consent before non-essential cookies**
  Analytics, advertising and tracking pixels should not load until the visitor agrees, if you serve visitors in the EU or UK. Essential cookies (login, cart) do not need consent.

- [ ] **Sign data processing agreements with your providers**
  Email tools, analytics and hosting that handle personal data of EU residents need a DPA; most providers offer one to accept online.

- [ ] **Link policies where the data is collected**
  Next to forms, newsletter sign-ups and at checkout.

- [ ] **Check company details and contact information**
  Legal name, registration number, address and VAT number where applicable. In many countries these are required on commercial websites.

HOW TO CHECK

Open the site in a clean private window and check what loads before you click "accept" in the browser's developer tools (Network tab).

08 Launch-day tests

The final pass proves the site works with real devices, real data and real mail servers.

- [ ] MUST DO **Test every form and confirm the message arrives**
  Check the spam folder too. Reply-to and sender addresses should use your own domain.

- [ ] MUST DO **Test checkout end to end**
  A real small payment, the confirmation email and a refund. Delete test orders afterwards.

- [ ] MUST DO **Remove "`noindex`" and staging passwords**
  A forgotten `noindex` tag keeps a new site out of Google. Check `robots.txt` does not say "`Disallow: /`".

- [ ] **Add 301 redirects from every old URL**
  If you replaced an existing site, map old pages to new ones so rankings, bookmarks and links keep working.

- [ ] **Check 404 pages, broken links and images**
  Crawl the site with a free tool such as Screaming Frog (up to 500 URLs free) and fix every error.

- [ ] **Submit the sitemap**
  In Google Search Console and Bing Webmaster Tools.

- [ ] **Test on a real phone and on a slow connection**
  Use mobile data rather than office Wi-Fi.

- [ ] **Take a final backup and write down the launch time**
  If something goes wrong, you can roll back to a known good state.

HOW TO CHECK

Ask someone who has never seen the site to complete the main task (contact you, buy something) on their own phone while you watch.

Sources and further reading

OWASP Cheat Sheet Series
https://cheatsheetseries.owasp.org/

NIST SP 800-63B: Digital Identity Guidelines (passwords)
https://pages.nist.gov/800-63-4/sp800-63b.html

Mozilla Observatory (security header testing)
https://developer.mozilla.org/en-US/observatory

Google email sender guidelines (SPF, DKIM, DMARC)
https://support.google.com/a/answer/81126

Need a hand with this?

Midnight Webs designs, secures and maintains websites for small businesses. Tell us what you need and we will scope it.

midnightwebs.com/estimate

Read online: midnightwebs.com/resources/website-launch-security-checklist