The Complete Web Hosting Security Checklist

Audit and harden your hosting environment

Use this checklist as a one-time security audit of your hosting environment, after a hosting migration, after a security incident or as part of an annual security review. Record findings and remediation status as you go.

Audit details

Website / domain	_____	**Hosting provider**	_____
Domain registrar	_____	**CMS / platform**	_____
Audit date	_____	**Reviewed by**	_____

Quick security snapshot

SSL / HTTPS status	_____
2FA coverage	_____
Backup status	_____
Critical remediation items	_____

Group 1: SSL and HTTPS

- ☐ SSL certificate installed and valid: expiry date checked and not within 30 days
- ☐ SSL auto-renewal confirmed active: renewal status checked in hosting dashboard; DNS, CDN or proxy changes since last issuance noted as potential renewal risk
- ☐ No SSL error flags in the hosting control panel SSL section
- ☐ HTTP to HTTPS redirect active: http://yourdomain.com redirects to HTTPS with a 301 status code
- ☐ www and root domain both serving HTTPS correctly
- ☐ No mixed content warnings in browser developer console on homepage and key pages
- ☐ TLS version confirmed: TLS 1.2 minimum; TLS 1.3 preferred; TLS 1.0 and 1.1 disabled
- ☐ HSTS header considered: Strict-Transport-Security header present in response headers (optional but recommended once HTTPS is confirmed fully working)

Notes and remediation actions for this group

Group 2: Account Access and Authentication

- ☐ Two-factor authentication enabled on hosting account dashboard
- ☐ Two-factor authentication enabled on domain registrar account
- ☐ Two-factor authentication enabled on WordPress or CMS admin login
- ☐ Hosting account password strong, unique and stored in a password manager
- ☐ Registrar account password strong, unique and stored in a password manager
- ☐ CMS admin account password strong, unique and not reused from any other service
- ☐ Registrar domain lock enabled to prevent unauthorized domain transfers
- ☐ CMS user account audit complete: all accounts reviewed; inactive or unrecognized accounts removed
- ☐ FTP and SFTP accounts reviewed in hosting dashboard: unused accounts removed
- ☐ Default "admin" username not in use as a WordPress administrator account

Notes and remediation actions for this group

Group 3: Software Updates and CMS Hardening

- ☐ WordPress core updated to the latest stable version
- ☐ All active plugins updated to latest stable versions
- ☐ All active themes updated to latest stable versions
- ☐ Deactivated plugins deleted: no unused plugins remaining installed
- ☐ Unused themes deleted: only active theme, required parent theme and one current fallback theme retained
- ☐ PHP version confirmed: PHP 8.3 or 8.4 recommended where compatible; PHP 7.x is end-of-life and no longer receiving security updates
- ☐ WordPress file editor disabled: DISALLOW_FILE_EDIT set to true in wp-config.php

Notes and remediation actions for this group

Group 4: File Permissions and Server Hardening

- ☐ WordPress directories confirmed at 755 or 750 permissions depending on host
- ☐ WordPress files confirmed at 644 or 640 permissions depending on host
- ☐ wp-config.php hardened according to host requirements, commonly 600, 640, 440 or 400 depending on server configuration
- ☐ No files or directories set to 777
- ☐ Directory browsing disabled: Options -Indexes present in .htaccess or confirmed disabled at server level

- ☐ PHP execution blocked in the uploads directory
- ☐ readme.html removed from site root (note: may reappear after core updates; include in periodic reviews)
- ☐ license.txt removed from site root
- ☐ xmlrpc.php disabled or access restricted if XML-RPC is not required
- ☐ SFTP used for file transfers rather than plain FTP

Notes and remediation actions for this group

Group 5: Email Authentication

- ☐ SPF TXT record present and starting with v=spf1
- ☐ Exactly one SPF record exists for the domain (duplicate SPF records break authentication)
- ☐ SPF record includes all current sending sources: hosting server, email provider, third-party tools
- ☐ DKIM TXT record present at correct selector subdomain as specified by email provider
- ☐ DKIM record value contains correct current public key
- ☐ Old DKIM records from previous email providers removed
- ☐ DMARC TXT record present at _dmarc.yourdomain.com with at minimum p=none policy
- ☐ DMARC reporting address configured to receive aggregate reports
- ☐ All email records checked using MXToolbox or equivalent verification tool

Notes and remediation actions for this group

Group 6: Backups, Scanning and Firewall

- ☐ Automated daily backups confirmed active and running on schedule
- ☐ Backup verified restorable: test restore of at least one component performed
- ☐ Backup stored off-server: not only on the same hosting account
- ☐ Backup retention window confirmed: at least 7 days of restore points available
- ☐ Malware scan run and results reviewed: no flagged files or all flags investigated
- ☐ Malware scanning scheduled to run automatically rather than only on demand
- ☐ Web Application Firewall (WAF) active: hosting panel WAF, Cloudflare or security plugin WAF confirmed
- ☐ Login rate limiting or brute-force protection active on CMS admin login
- ☐ Security headers reviewed: X-Content-Type-Options, X-Frame-Options and Referrer-Policy headers present

Notes and remediation actions for this group

Disclaimer

This checklist is for general informational and organizational purposes only. It is not legal, financial, technical, security or professional advice and should not replace a personalized plan, licensed professional guidance or qualified technical review. Hosting environments, server configurations, control panel interfaces, CMS platforms and available security features vary by provider and can change over time. File permission changes, server configuration changes, DNS changes and security hardening steps can affect site functionality if applied incorrectly. Always back up your site first, test changes in a staging environment where possible and verify requirements directly with your hosting provider, domain registrar, CMS platform and any relevant service provider before making changes. This checklist must be adapted to your specific website, hosting environment, risk level and business requirements. Web Hosting Services makes no guarantees regarding outcomes based on use of this checklist in any format. For complex security requirements, regulated environments or business-critical websites, consider engaging a qualified security or hosting professional. If this checklist is reprinted or republished online, please credit Web Hosting Services (webhostingservices.co).

Credit

Web Hosting Services | webhostingservices.co