Free owner checklist · Diversified Tech Solutions

WordPress looks hacked? Start here.

Owner first-24-hours triage checklist (printable)

Avery Parker, principal · Remote nationwide · Onsite Tri-Cities / East TN / SW VA / Western NC
Active fire: 423-888-0252 · 828-484-1257
Packages: diversifiedtechsolutions.com/wordpress-incident-response/

Avery Parker · Diversified Tech Solutions

What this is: A practical checklist for the first day after you suspect a WordPress compromise. It helps you limit the damage, keep evidence, and decide when to call a professional.

What this is not: A promise that DIY steps will fully clean the site. It does not promise a cleanup timeline, ranking recovery date, or reinfection warranty. Complex or business-critical incidents need a named engineer - see current packages on diversifiedtechsolutions.com.

If the site is actively harming visitors, leaking data, or you are locked out of admin: call Diversified Tech Solutions at **423-888-0252** (Tri-Cities / East TN / SW VA) or **828-484-1257** (Western North Carolina). After-hours incident response by phone. Hub: https://diversifiedtechsolutions.com/wordpress-incident-response/

How to use this sheet

- Print it or keep it open while you work.
- Check boxes as you go. Note times in the margin.
- Prefer **contain and document** over "wipe and hope."
- Stop and call a professional if you hit a STOP line below.

1. Confirm it might be a compromise

Check all that apply:

☐ Google Search or Search Console shows casino, pharmacy, loan, or spam titles you did not write

- [ ] Visitors report redirects (especially on mobile) or odd pop-ups
- [ ] Links or pages appear that nobody on your team added
- [ ] An administrator or user account exists that you did not create
- [ ] Your host or CDN flagged malware or suspended the site
- [ ] A browser or Google shows "This site may be hacked"
- [ ] Checkout, login, or forms behave strangely (online stores / membership sites)
- [ ] Unexpected outbound email from the site or contact forms

Notes (what you saw + when you first noticed):

_____

_____

---

2. First-hour steps (before you "clean")

Keep access and evidence

- [ ] Write down who has admin, hosting, DNS, and email access today
- [ ] Screenshot Search Console notices, host alerts, and odd pages (include the URL and time)
- [ ] Export or screenshot current DNS settings at your registrar
- [ ] If you can still log in safely: note current plugins and themes (names + versions)
- [ ] Do **not** delete logs, odd files, or users yet - mark them for review

Limit the damage (without throwing away clues)

- [ ] Put the site in **maintenance / coming soon** mode only if visitors are being harmed **and** you can still reach admin or hosting afterward
- [ ] Temporarily disable public comments or open registration if those are spam vectors
- [ ] Tell your host you suspect a compromise; ask them **not** to wipe the account until you have a backup
- [ ] Pause paid ads pointing at the site if clicks are landing on junk pages
- [ ] If customer payment data may be involved: pause checkout and follow your payment processor's guidance (ask counsel if you are unsure)

STOP - call a professional now if:

- [ ] You cannot reach hosting or WordPress admin
- [ ] Ransomware, encryptor, or full server lockout
- [ ] Suspected card-skimmer on checkout
- [ ] Multiple business systems (email, VPN, office PCs) look compromised - not "just WordPress"

---

3. Backup before you change anything

- [ ] Take a **full** backup of files and the database (host panel, or a backup tool you trust)
- [ ] Download a copy **off the server** (your computer or separate cloud you control)
- [ ] Label it: `pre-cleanup-YYYY-MM-DD` and keep it read-only
- [ ] Spot-check that the backup file opens and is not empty
- [ ] Note backup location: _____

Do not restore an old backup yet unless you know it is clean **and** you understand you may lose recent orders or content. Prefer professional help when unsure.

---

4. Passwords and access cleanup

Change these **after** you have a backup, preferably from a computer you do not normally use for the site:

- [ ] WordPress administrator password(s) - unique, long, password manager
- [ ] Hosting control panel password
- [ ] SFTP / SSH keys and passwords; revoke old keys you do not recognize
- [ ] Database password (coordinate with your host if needed)
- [ ] CDN / Cloudflare / firewall account password + review API tokens
- [ ] Domain registrar account password + turn on 2FA
- [ ] Email accounts that can reset WordPress or hosting
- [ ] Review connected apps / "application passwords" in WordPress

Unknown admin users found: list username + email + role (do not delete until documented):

_____

---

5. Quick checks (not a full cleanup)

These are **checks**, not a full cleanup:

- [ ] Users: any unexpected Administrators?
- [ ] Plugins: any unknown plugins? Any must-use plugins you do not recognize?
- [ ] Themes: extra themes you did not install?
- [ ] Settings → General: site URL / WordPress URL still correct?
- [ ] Settings → Permalinks: unexpected changes? (Note first - do not save blindly)
- [ ] Homepage and key landing pages: visible spam or injected junk?
- [ ] On a phone: open the homepage in a private window - any redirect?
- [ ] Search Google for `site:yourdomain.com` - odd titles or URLs?
- [ ] Host file manager: unexpected PHP files in the uploads folder?

- [ ] Scheduled tasks in the host panel: jobs you do not recognize?

Findings log:

_____

_____

6. What not to do in the first 24 hours

- [ ] Do not install random "one-click malware remover" plugins from vendors you do not know
- [ ] Do not mass-delete files you do not understand
- [ ] Do not restore a backup that might still be infected without a plan
- [ ] Do not post passwords in chat tickets or email
- [ ] Do not promise customers a fixed "back tomorrow" date until the scope is known
- [ ] Do not ignore Google Search Console or host tickets - reply that you are investigating

7. Decide: stabilize yourself vs call for help

Reasonable to do with your host (limited):

- Containment passwords + backup + maintenance mode
- Removing an obviously new unknown admin *after* documenting it
- Disabling an obviously rogue plugin *after* documenting it
- Working with host support on account-level malware flags

Bring in Diversified Tech Solutions (recommended after a real compromise):

- Malware in core files, themes, must-use plugins, or the database
- Spam SEO pages indexed in Google
- Redirects you cannot find
- Online store / payment concerns
- You need a **written report** for a board, insurer, partner, or Google review
- You want cleanup and hardening in one engagement

Published packages (this PDF is not a price sheet):

See current cleanup and hardening packages on:

https://diversifiedtechsolutions.com/wordpress-incident-response/

Contact: 423-888-0252 · 828-484-1257 · https://diversifiedtechsolutions.com/contact/?topic=wordpress

If you can wait about 20 minutes: https://calendly.com/averyjparker/20-minute-dts-discovery-call

8. Have this ready for a cleanup call

Item	Your notes
Site URL(s)	
Hosting company + login path	
Who owns DNS / the domain	
Online store / paid ads? Y/N	
When symptoms started	
Google malware warning / host suspension? Y/N	
Anyone else already "cleaned"?	
Preferred contact phone	

9. After containment (next 48-72 hours)

- ☐ Keep the pre-cleanup backup safe
- ☐ Watch Search Console for new spam URLs
- ☐ Watch order, email, and form notifications for anything odd
- ☐ Plan hardening: updates, fewer admin users, login protection, lock the theme/plugin file editor, backups you have actually tested
- ☐ If professionals cleaned the site: finish their hardening list; do not reopen old admin accounts

10. Sign-off

Owner / responsible person: _____ Date: _____

Primary tech contact: _____ Phone: _____

Disclaimer: This checklist is educational guidance from Avery Parker / Diversified Tech Solutions. It is not legal, insurance, or payment-card advice. Outcomes vary by site complexity, hosting, and how long the problem was present. Always prefer current package details on diversifiedtechsolutions.com over any reprint of this sheet.