WPSecureStack

Incident Response Plan

wpsecurestack.com

■ **Your site has been hacked. Don't panic.** Follow these steps in order. Every minute counts — but rushing and skipping steps can make things worse.

■ RESPONSE TIMELINE AT A GLANCE

Phase 1 0 – 30 min Containment	Phase 2 30 min – 2 hrs Assessment	Phase 3 2 – 8 hrs Clean-up	Phase 4 8+ hrs Recovery

PHASE 1 — CONTAINMENT (Do this in the first 30 minutes)

1	■ **Take the site offline immediately** Put your site into maintenance mode or ask your host to temporarily disable it. This stops the attacker from doing more damage and protects your visitors from malware. ■ *Most hosts have a 'suspend site' button in the control panel. Use it now.*
2	■ **Change ALL passwords right now** Change: WordPress admin password, hosting control panel password, FTP/SFTP password, database password, and your email account password. Do this from a clean device. ■ *Use a password manager like Bitwarden or 1Password to generate strong unique passwords.*
3	■ **Revoke all active sessions** In WordPress, go to Users and click 'Log Out Everywhere Else' on all admin accounts. This kicks the attacker out if they are still logged in. ■ *Change your WordPress secret keys in wp-config.php to invalidate all sessions instantly.*
4	■ **Take a snapshot / preserve evidence** Before cleaning anything, take screenshots of defaced pages, note the date and time, and download a full backup of the infected site. You may need this for insurance or reporting. ■ *Ask your host for server access logs — these show exactly how the hacker got in.*
5	■ **Alert your hosting provider** Call or email your host immediately. Tell them your site has been compromised. Most hosts have a security response team and can help isolate the site quickly.

PHASE 2 — ASSESSMENT (30 minutes to 2 hours)

1	**■ Identify what was hacked and how** Check your server access logs, WordPress activity logs, and file modification dates. Look for files changed in the last 30–90 days that you did not change yourself. Common entry points: outdated plugins, weak passwords, nulled themes. ■ *Use your hosting file manager to sort files by 'last modified date' — malicious files often stand out.*
2	**■ Scan for malware and infected files** Use a trusted security plugin (Wordfence, MalCare, or Sucuri) to run a full malware scan. The scan will show you infected files, suspicious code injections, and backdoors. ■ *Run the scan on a copy — not directly on a live site — if possible.*
3	**■ List everything that was affected** Write down: which files are infected, which pages were changed, were any user accounts created, and was customer or payment data potentially exposed. This list guides your clean-up.
4	**■■ Decide: clean or restore from backup?** If the infection is limited to a few files, clean them. If the infection is widespread or you cannot find the source, restore from a clean backup. A clean backup is almost always faster. ■ *Only restore from a backup you know was made before the hack occurred.*

PHASE 3 — CLEAN-UP (2 to 8 hours)

1	**■■ Replace core WordPress files** Download a fresh copy of WordPress from wordpress.org. Replace all files EXCEPT wp-config.php and the wp-content folder. This removes any core file tampering. ■ *Do not re-upload plugins or themes from your old site — download fresh copies.*
2	**■ Clean or delete infected files** For each infected file found in the scan: if it is a plugin/theme file, delete and reinstall it. If it is a custom file, open it and remove the injected code (usually at the top or bottom of the file). ■ *Malicious code often looks like long strings of random characters — base64_decode() is a red flag.*
3	**■■ Clean the database** Scan the database for spam links, hidden admin users, and malicious scripts injected into posts. Tools like Adminer or phpMyAdmin can help. Look for unexpected users in the wp_users table. ■ *Delete any admin users you did not create. Attackers often leave hidden back-door accounts.*
4	**■ Remove all backdoors** Backdoors are hidden files that let the attacker return even after you clean the site. Run a second full malware scan after cleaning to ensure nothing was missed. Common backdoor file names: wp-logis.php, config.bak.php, 1ndex.php
5	**■ Update everything** Update WordPress core, all plugins, and all themes to the latest versions. Delete any plugin or theme that is no longer maintained or that you do not actively use.

PHASE 4 — RECOVERY (8 hours and beyond)

1	**■ Run a final security scan** Before bringing the site back online, run one more full malware scan. Get a green clean report from your security plugin. Only then proceed. ■ *Sucuri's free SiteCheck scanner can also confirm the site is clean from the outside.*
2	**■ Bring the site back online** Disable maintenance mode and restore normal access. Check every page, contact form, and payment process manually to confirm everything works as expected.
3	**■ Request Google / blacklist removal** If your site was blacklisted by Google (showing 'This site may harm your computer'), go to Google Search Console > Security Issues and request a review once clean. ■ *This process usually takes 24–72 hours after the review is submitted.*
4	**■ Harden the site to prevent recurrence** Enable a Web Application Firewall (WAF), set up two-factor authentication, change the login URL, and limit login attempts. Download our Security Checklist for the full 50-point guide.
5	**■ Notify affected parties if needed** If customer data (names, emails, payment info) may have been exposed, you may have a legal obligation to notify those customers. Check your local data protection laws (GDPR, CCPA, etc.). ■ *Consult a lawyer before sending breach notifications — the wording matters legally.*
6	**■ Document and do a post-incident review** Write down: how the attack happened, what was affected, what you did, and how long it took. Use this to improve your security so the same attack cannot happen again.

■ QUICK REFERENCE — CONTACTS & TOOLS

Resource	What it's for	Where to find it
WPSecureStack Emergency Help	Immediate hack recovery support	emmanuel@wpsecurestack.com WhatsApp: +256 785 832 643
Wordfence / MalCare / Sucuri	Malware scanning and clean-up	wordfence.com / malcare.com / sucuri.net
Google Search Console	Security warnings and blacklist review	search.google.com/search-console
Sucuri SiteCheck	Free external malware check	sitecheck.sucuri.net
Have I Been Pwned	Check if your email / passwords leaked	haveibeenpwned.com
WPSecureStack Resources	Checklists, snippets, guides	wpsecurestack.com/resources

Emmanuel Tatyabala | Co-Founder, WPSecureStack

emmanuel@wpsecurestack.com |
WhatsApp: +256 785 832 643

wpsecurestack.com/resources