How to Clean a Hacked WordPress Site: Removing Malware Step by Step

WordPress Guides · https://www.hyyat.com/en/knowledgebase/clean-hacked-wordpress-site-remove-malware/

In short If your WordPress site has been hacked: take a **backup**, lock the site temporarily, and find **how they got in**. Then replace WordPress core, plugins and themes with **clean original copies**, check `uploads`, `wp-config.php` and `.htaccess`, delete unknown users, and change every password and secret key. Finally update everything and ask Google for a review.



A hacked WordPress site is stressful, but it can be cleaned if you follow an organised plan. The cleanup must be thorough: one missed infected file is enough for the attacker to come back. This guide is the full plan; you will need access to cPanel or FTP, and phpMyAdmin.

Why do WordPress sites get hacked?

The main motive is money: placing links to gambling, pharmacy or shady sites to boost their Google ranking, sending spam from your site, or redirecting your visitors to scams. The most common ways

in:

- **Weak passwords** for admin or FTP accounts.
- **Outdated WordPress, plugins or themes** with known vulnerabilities.
- **Nulled plugins and themes** from unofficial sources, which come with malware.

Signs of a hack

- Unfamiliar links on your pages, sometimes hidden in the background colour.
- Visitors redirected to other sites, sometimes only on mobile or only when arriving from Google.
- Strange results when searching for your site, or a "This site may be hacked" warning.
- A notice from your host about unusual amounts of email sent from your site.
- Admin users in WordPress you do not recognise.

1) Prepare

1. **Take a full backup** of files and database, even if infected. You may need it for comparison or to roll back.
2. **Lock the site temporarily** so it does not infect visitors and the attacker cannot interfere during cleanup. You can allow only your own IP address by adding this to `.htaccess`, replacing the number with your address:

```
Require all denied
Require ip 203.0.113.10
```

2) Find how they got in

- Check your WordPress, plugin and theme versions against the WPScan vulnerability database.
- Open Google Search Console and look at Security issues.
- Check your site in Google's Safe Browsing report.
- Search your access logs for `POST` requests to unfamiliar php files. Not every POST is malicious; contact forms and the login page use it too.



3) Replace WordPress core files

1. **Find your WordPress version** in `wp-includes/version.php`.
2. **Download the same version** from the official WordPress archive and unzip it on your computer.
3. **Delete wp-admin and wp-includes** from your site and upload the clean copies.
4. **Replace the root files** in public_html with the originals, **except wp-config.php**.
5. **Check any other files or folders** in the root you do not recognise. If unsure, ask support before deleting.

4) Plugins and themes

- Delete every plugin or theme you do not use.
- Delete each plugin folder, then upload a clean copy from the WordPress repository or your developer account.
- Do the same with your theme. If it was customised, keep your changes in a child theme after checking them line by line.
- Delete any nulled plugin or theme.

If you see pop-ups or unwanted redirects, also read removing wp-vcd malware.

5) Check the remaining files

- **The uploads folder** should not contain `.php`, `.sh` or `.exe` files. Any you find most likely came from the attacker.
- **Files with no original copy:** search them for words like `eval`, `base64_decode`, `gzinflate` and `exec`, and for very long unreadable lines.
- **wp-config.php:** compare it with the original, remove any unfamiliar code, and change the secret keys (salts) to end all open sessions. Details in protecting wp-config.php.
- **.htaccess:** the standard WordPress file contains only these lines; anything else you do not recognise is worth checking:

```
# BEGIN WordPress
RewriteEngine On
RewriteBase /
RewriteRule ^index\.php$ - [L]
RewriteCond %{REQUEST_FILENAME} !-f
RewriteCond %{REQUEST_FILENAME} !-d
RewriteRule . /index.php [L]
# END WordPress
```

An `.htaccess` in uploads containing only `Options -Indexes` is normal.

6) Users, database and passwords

- Delete any user you do not recognise, especially administrators. Read WordPress user roles.
- Search the database posts and options tables for `<script` and links to strange sites.
- Change passwords for WordPress admins, cPanel, FTP, the database and email. You can reset a WordPress password from phpMyAdmin if you cannot log in.



7) After the cleanup

1. **Update WordPress, plugins and theme** to the latest versions. See updating safely.
2. **Reopen the site** by removing the lock lines from .htaccess, and browse your key pages.
3. **Ask Google for a review** in Search Console if it showed a warning.
4. **Protect the login page** as in protecting wp-admin, and turn on two-factor authentication for admins.

On Hyyat Host hosting: files are scanned with ImunifyAV and each account is isolated with CloudLinux, so a hacked site cannot spread to other sites on the server.

Summary

- Take a backup and lock the site before cleaning.
- Replace files with original copies instead of fixing them one by one.
- Change every password and key, then update everything.

Rather not clean it yourself? Our technical support and maintenance team can clean and secure your site.

Frequently asked questions

How do I know my WordPress site has been hacked?

Signs include strange links, visitors redirected elsewhere, a Google warning, unknown admin users, or a notice about lots of email sent from your site.

Is deleting the infected file enough?
Usually not. Attackers leave several files and backdoors. The safe cleanup is replacing all files with originals and changing passwords.

Can I restore an old backup instead?
Yes, if you are sure it predates the hack. Then update everything and change passwords, or the same hole will be used again.

Why does Google still show a warning after cleaning?
Google needs to re-check. Request a review in Search Console once you are sure the site is clean.

Related guides

- Pop-up Ads and Redirects on Your WordPress Site? How to Remove wp-vcd Malware
- How to Protect wp-config.php in WordPress: 7 Steps to Secure Your Most Important File
- How to Protect the WordPress Login Page (wp-admin): 7 Practical Steps
- How to Update WordPress and Plugins Safely Without Breaking Your Site
- WordPress User Roles and Permissions: Who Needs Administrator Access and Who Does Not
- Email Hacked or Sending Spam? Steps to Recover and Secure Your Mailbox

All guides in this section →

Need this service from Hyyat Host?Our team handles it for you, with support replying to tickets within 24 hours at most.
WordPress HostingWordPress design