

How to Recover a Hacked WordPress Site A Practical Recovery Guide

Discovering that your WordPress website has been compromised can feel like a disaster, but recovery is a well defined process once you know the steps. This guide focuses specifically on recovering a hacked WordPress site, getting it back online, clean and stable whether you have a recent backup to fall back on or need to rebuild the site from scratch. If you haven't already, it's also worth reading our complete guide on [how to fix a hacked WordPress website](#) for the full cleanup process.



Do not Panic: Your First Response Checklist

The first ten minutes after discovering a hack matter more than you might think. Before doing anything else:

1. Take a screenshot or note of exactly what looks wrong (redirects, defaced pages, warning messages)
2. Put the site into maintenance mode or take it offline
3. Change your WordPress admin password immediately
4. Note the exact time you noticed the issue, which will help later when reviewing logs
5. Avoid making any content changes until you understand the scope of the problem

Acting quickly limits the damage, but acting carefully prevents you from accidentally destroying evidence you will need to trace how the site was compromised.

Step 1: Isolate the Site

Put the site into maintenance mode immediately, or if the situation is severe, suspend the hosting account entirely. This stops the infection from spreading to other sites on the same server and prevents search engines from indexing malicious content while you work on recovery.

Step 2: Assess the Damage

Before jumping into a fix, get a full picture of what's affected:

- Check Google Search Console for security notices
- Review your file manager or FTP client for recently modified files
- Look at your hosting account's malware scan report, if one is available
- Check whether the database, files, or both were altered
- Confirm whether other sites on the same hosting account were also affected

This assessment determines whether a full backup restoration is possible or whether you'll need to do a manual, file by file recovery.

Step 3: Restore From a Clean Backup (The Fastest Recovery Path)

If you have an uninfected backup from before the attack, restoring it is almost always your quickest route back to a working site. Here's how to do it properly:

1. Confirm the backup predates the infection by checking file modification timestamps
2. Restore the backup to a staging environment first, not directly to production, so you can verify it's clean
3. Scan the restored staging site with a malware scanner before pushing it live
4. Once confirmed clean, restore both files and database to the live site
5. Immediately update WordPress core, themes and plugins after restoration
6. Change every password associated with the site before bringing it back online

Restoring an old backup without checking it first is a common mistake. If the backup itself contains the malware, you will simply reinfect the site.

Step 4: What to Do If You Do not Have a Clean Backup

Many site owners discover too late that their backups were either missing, outdated, or already infected. If that's your situation, manual recovery is necessary:

- Download a completely fresh copy of WordPress core from WordPress.org
- Replace the wp admin and wp includes folders entirely with the fresh copies
- Go through wp content folder by folder: reinstall each plugin and theme from its official source rather than trying to repair the existing files
- Carefully inspect the uploads folder for any PHP files, which should never exist there
- Review wpconfig.php line by line for injected code, since it's a common hiding spot for backdoors

If this process feels overwhelming, our [web solutions](#) team can take over the manual recovery for you.

Step 5: Reinstall Core WordPress Files

Even after restoring from backup, it is good practice to overwrite wp admin and wp includes with a fresh WordPress download matching your current version. This eliminates any lingering modified core files that a malware scan might have missed. If the restored site feels slow afterward, our [WordPress performance optimisation](#) service can help identify and fix the cause.

Step 6: Check the Database for Injected Content

The database is often overlooked during recovery, but it's a favorite hiding place for hackers. Search your database (via phpMyAdmin or a similar tool) for:

- Suspicious script tags inside post content or widget text
- Spam links inserted into page content, often hidden with CSS
- Unauthorized changes to the siteurl or home values in wp_options
- New administrator accounts you don't recognize in wp_users
- Unusual autoloaded options with encoded or obfuscated data

Step 7: Remove Suspicious Admin Users and Reset Access



Go through your list of users and delete any account you don't recognize, even if it looks legitimate at first glance hackers sometimes create admin accounts with innocuous looking usernames. Reset the passwords for every remaining user with elevated permissions and reset your database password, FTP/SFTP credentials and hosting control panel login as well.

Step 8: Update Everything Before Going Live

Before bringing the recovered site back online, make sure WordPress core, every theme and every plugin is fully updated. Delete any plugins or themes that are no longer maintained by their developers, since abandoned software is a common long term vulnerability. Our [WordPress solutions](#) team handles this kind of update and cleanup work as part of ongoing site care.

Step 9: Verify Site Functionality

Before removing maintenance mode, test the recovered site thoroughly:

- Check that all pages load without errors
- Confirm there are no unexpected redirects
- Test forms, checkout flows and any dynamic functionality
- Run a fresh malware scan to confirm a clean result
- Check page source code for hidden spam links or scripts

Step 10: Bring the Site Back Online and Monitor Closely

Once you're confident the site is clean, remove maintenance mode and monitor closely for the first few weeks. Set up uptime and security monitoring so you're alerted immediately if anything suspicious reappears, since a persistent hacker may have left a backdoor you missed. If the incident affected your search visibility, our [SEO services](#) can help you track and recover rankings during this period.

Step 11: Build a Backup Strategy So This Doesn't Happen Again

The best recovery plan is one you never have to fully use. Going forward:

- Set up automated daily backups stored offsite (not on the same server)
- Keep at least 30 days of backup history
- Test your backups periodically by restoring them to a staging site
- Combine backups with a security plugin and firewall for layered protection

Our [web maintenance packages](#) include automated backups, updates and monitoring, so recovery like this becomes far less likely in the first place.

Conclusion

Recovering a hacked WordPress site is a matter of following a clear, methodical process: isolate the damage, restore from a verified clean backup where possible, manually clean the site when no backup exists and lock down every access point before bringing the site back online. With a proper backup strategy and ongoing monitoring in place, you will not only recover faster from this incident but be far better protected the next time an attack is attempted. Need help with the recovery itself? Visit [ITLeadz](#) to explore our WordPress SEO services and site recovery support.

Frequently Asked Question (FAQs)

How long does it take to recover a hacked WordPress site?

A restoration from a clean backup can take as little as a few hours. A full manual recovery without a backup typically takes one to three days, depending on the size of the site and severity of the infection.

Is it safe to restore an old backup after a hack?

Only if you verify the backup predates the infection and scan it for malware before restoring it to your live site. Restoring an already infected backup will bring the hack right back.

What if I do not have any backups at all?

You'll need to manually clean the site by replacing core files, reinstalling plugins and themes from official sources and carefully checking the database for injected content.

Should I rebuild the site from scratch instead of recovering it?

For small, simple sites, a rebuild can sometimes be faster than a deep cleanup. For larger sites with lots of content, recovery through cleaning is usually more practical.

How do I stop my WordPress site from being hacked again after recovery?

Keep everything updated, use strong passwords with two factor authentication, install a firewall/security plugin and maintain tested, automated offsite backups.