

A 21-Step Checklist

To Secure WordPress Site

[SCAN YOUR SITE FOR MALWARE](#)

Daily Cloud Backups

Your backups are saved daily on our [secure cloud storage using Amazon S3 infrastructure](#). If anything happens, we have your core files and database stored remotely for easy access and 1-click back-up.

Force Secure Passwords

We do a full manual audit of admin user names to make sure it's [nearly impossible](#) for a bot to gain access through a brute force attack. We'll also require all new users to use strong passwords instead of weak ones.

Daily [Malware Scan](#)

Your website is [automatically scanned daily for known and new malware, any form of malicious code and potential backdoors](#). If our scans find anything, the team will repair any files altered by hackers immediately.

SSL Certificate

We'll support the installation of an [SSL certificate](#). Your URL will start with https, all the data on your site will be encrypted and your visitors will feel secure.

Database Protection

Our team [secures your database from SQL injection attacks](#), which add unwelcome content through the DB. This is a common website attack that we simply won't tolerate.

Real-Time Monitoring

We monitor websites for hack attempts in [real-time](#), meaning we can respond to any security issues immediately and tighten security as needed based on the individual threat level.

Brute Force Protection

We change your login URL, force strong passwords, set up a firewall and activate automated IP blocking so [nobody can force their way into your site](#).

Install a Firewall

[Implementing a firewall](#) is one of the best ways to keep hackers and spammers at bay. This includes effective blocking options to keep suspicious traffic away from your site.

IP Blocking

We'll implement [intelligent network blocking](#) to prevent traffic from specific locations. If someone tries to access your dashboard or files more than once, we'll lock out their IP address.



Custom Login URL

If you want, we'll change your WordPress dashboard login URL from `/wp-admin` to `/your-own-url`. That way bots and hackers can't find your login page so easily.

Blocking Fake Google Crawlers

Some malicious code can fake out security systems by simulating real Googlebots. Our protection system knows the difference and won't let them crawl your website.

Comment Spam Filtering

We'll clean out junk comments on a daily basis and keep your website and dashboard uncluttered. It also optimizes your database for speed and SEO.



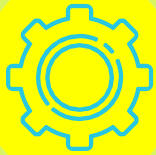
Daily Link Scan

We scan your website daily for any links sending visitors to suspicious content or broken pages. We'll make appropriate adjustments and change the link to point wherever you want.



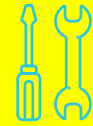
Daily Plugin + Theme Scan

We scan core, theme, and plugin files daily to ensure the files match the originals in the WordPress repository.



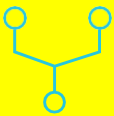
Authentication Keys + Salts

We'll implement a set of random variables that improve encryption of information stored in your users' cookies. Simply put, this makes it even harder to crack your password.



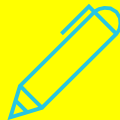
Daily Database Optimization

We perform daily cleaning of table overhead in your WordPress database to keep your website running at top speed.



2-Factor Authentication

If you want an added layer of security for your WordPress dashboard, we'll implement 2FA. This means you'll need a code sent to your mobile device to log in.



DNS Change Alerts

We scan your website daily for any DNS changes that occur. This could potentially cause website downtime, so we monitor it regularly.

File Permissions

We adjust file permissions so only designated people who you know and trust can add to your files. That means no content where you don't want it and no malicious code.

Verify Trusted Sources

We double check all your plugins and themes to make sure they're from a secure and trusted source. Everything on your website should be authenticated by wordpress.org.

Manage Inactive Plugins

Any plugins that aren't up-to-date can act as potential backdoors, even when disabled. We review the plugins you're using regularly and remove those you're not actively using.



WE TAKE
SECURITY
SERIOUSLY

**Partner with us & feel
the confidence**
of knowing your website will
pass any security test or
scan out there.

WORDPRESS HACKED? 🤪

! MALWARE CLEAN UP & REMOVAL !

WE WON'T STOP UNTIL YOUR SITE IS 100% SAFE



Free Evaluation

Only pay after cleanup is done.



24/7 Support Call
1-888-331-5797



Discount offered
for multiple sites

[Get Started](#)

Read Our Latest Posts

- WordPress Malware Redirect Hack 🦠 How To Detect & Fix It
 - Web Shell PHP Exploit 🦠 What, Why & How To Fix
 - How To Fix 🦠eval(base64_decode()) Php Hack in WordPress [Guide]
 - How to Scan & Detect Malware in WordPress Themes (Plugins Included)
 - “This Account Has Been Suspended” – WordPress Down[Fix]
 - How To Find & Fix A 🦠 Backdoor In Hacked WordPress Site?
 - Sorry, This File Type Is Not Permitted For Security Reasons ✖ FIXED
 - How To Remove Malware From WordPress Site
 - WordPress 5.0.1 Vulnerabilities – Security Release Update
 - WordPress XSS Attack – Exploit & Protection
-
- WordPress 5.0.1 Vulnerabilities – Security Release Update_
 - WordPress Not Sending Email Issue ✖ [FIXED]_
 - Optimize & Repair WordPress Database – Fix Corrupted Tables_
 - WordPress Theme Security – How to Ensure Safety Of Your Theme_
 - How To Remove Malware From WordPress Site_

cv



**Let Our Security Experts Do The HARD
WORK..**

Get Your Malware Infected WordPress Site Cleaned Up!!

**Let Us Know Who You Are!
Get Started TODAY!**