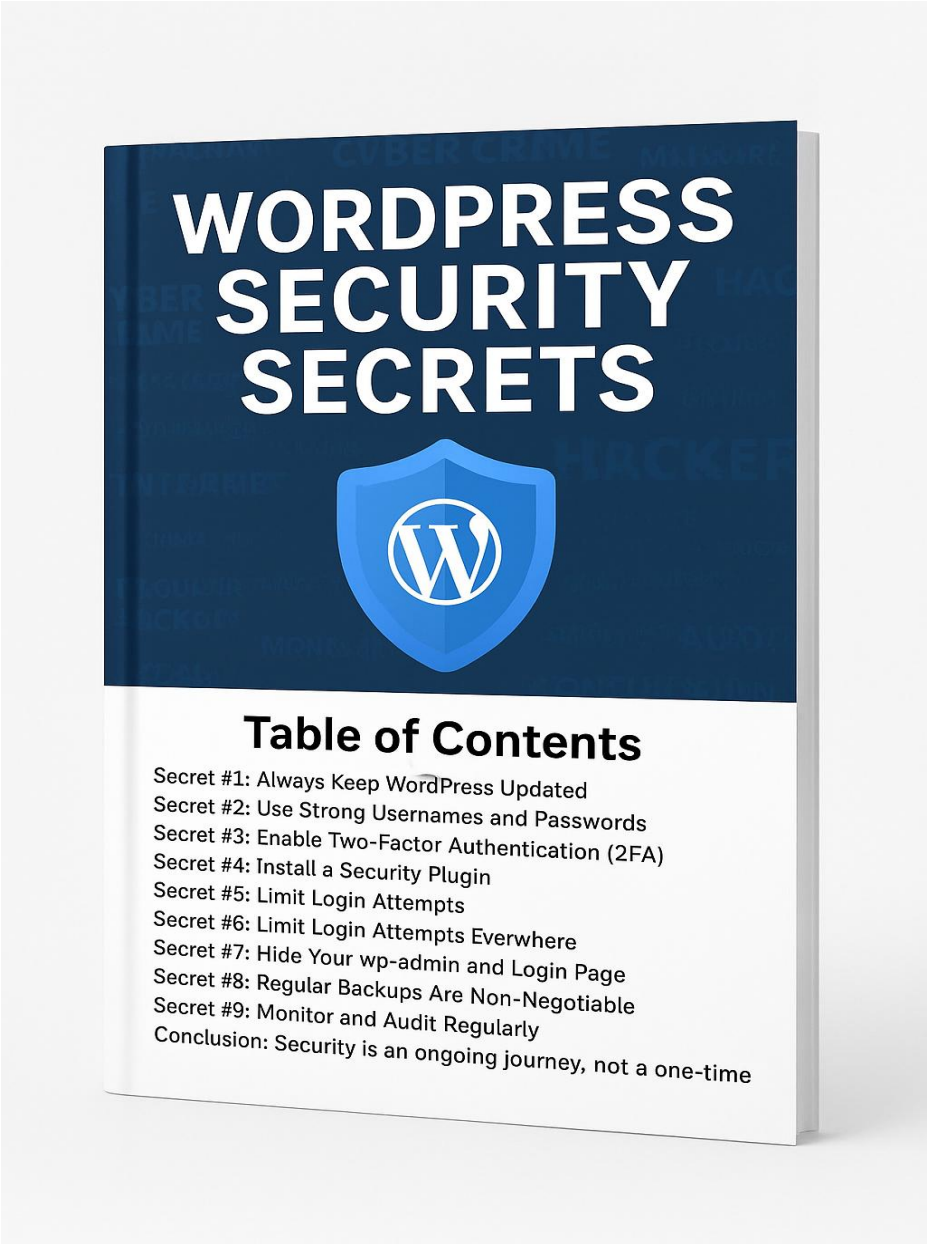
WordPress Security Secrets

(Bonus eBook for WPZora Proxy Shield Users)



Need a custom WordPress plugin? We build tailored solutions at affordable prices.
Contact us: support@wpzora.com

Table of Contents

WordPress Security Secrets

(Bonus eBook for WPZora Proxy Shield Users)

Introduction

WordPress powers over 40% of all websites on the internet. Its popularity is both its greatest strength and its greatest weakness. On one hand, it has a massive community, endless plugins, and themes that make building a website incredibly easy. On the other hand, being the most widely used content management system also makes it the number one target for hackers, spammers, and automated bots.

According to security researchers, there are more than 90,000 brute force login attempts against WordPress sites every single minute worldwide. Add to that the constant discovery of plugin vulnerabilities, misconfigured servers, and careless users — it becomes clear why so many WordPress sites get hacked.

The good news is: you don't need to be a cybersecurity expert to protect your website. By applying a handful of proven strategies, you can drastically reduce your risks and make your site a very difficult target for attackers.

This guide reveals 10 powerful WordPress Security Secrets. Each of these secrets is practical, actionable, and tested by professionals. If you follow them, your website will be safer, your visitors will trust you more, and your online business will thrive.

Secret #1: Always Keep WordPress Updated

One of the easiest — yet most neglected — steps in website security is keeping everything updated.

- WordPress Core: Every few months, WordPress releases new versions. Some are feature updates, others are critical security patches. If you ignore them, you're leaving known vulnerabilities open to attackers.
- Themes and Plugins: Over 50% of WordPress hacks occur through outdated plugins or themes. Hackers actively scan the internet for old versions with known bugs.

Case Study: In 2014, the popular *Revolution Slider* plugin had a vulnerability that allowed attackers to gain full control of sites. Over 100,000 websites were hacked simply because site owners didn't update.

Action Steps:

- Turn on auto-updates for WordPress Core.
- Regularly update plugins and themes (at least once a week).
- Remove unused plugins/themes completely — outdated inactive files are still a risk.

Pro Tip: If you run multiple sites, consider a management tool like ManageWP or MainWP to handle updates centrally.

Secret #2: Use Strong Usernames and Passwords

The most common way hackers break in is through weak credentials. “admin” as a username and “123456” as a password is still shockingly common.

Why Weak Credentials Fail:

- Hackers run brute force bots that try millions of combinations in seconds.
- If your username is easy to guess and your password is short, it’s only a matter of time before they succeed.

Better Practice:

- Never use “admin” as a username. Pick something unique.
- Use 12+ characters with uppercase, lowercase, numbers, and symbols.
- Passphrases are great: *BlueTiger!River2025* is easier to remember and much harder to crack than *Abc123*.
- Use a password manager like Bitwarden, LastPass, or KeePass to generate and store secure passwords.

Why This Matters: According to Verizon’s Data Breach Report, 81% of data breaches are caused by weak or reused passwords.

Secret #3: Enable Two-Factor Authentication (2FA)

Passwords are not enough anymore. With data leaks happening all the time, your login details might already be floating around the dark web without your knowledge.

What is 2FA?

Two-Factor Authentication adds a second step when logging in, usually a code from an app like Google Authenticator. Even if a hacker has your password, they can't log in without the code.

Benefits:

- Stops brute force attacks cold.
- Protects against stolen password leaks.
- Gives you peace of mind knowing there's a backup lock.

How to Set It Up:

- Install a plugin like WP 2FA or use a security plugin that includes it.
- Connect with an app (Google Authenticator, Authy, Duo).
- Make sure you keep backup codes in case you lose your phone.

Fact: Microsoft reported that 2FA blocks 99.9% of automated attacks.

Secret #4: Install a Security Plugin

A good security plugin is like having a guard dog at your door. It monitors traffic, checks for suspicious activity, and blocks known threats.

Top Options:

- Wordfence: Full firewall, malware scanner, brute force protection.
- iThemes Security: Focuses on hardening WordPress settings.
- WPZora Proxy Shield: (Your bonus) — specialized in blocking proxy/VPN/hosting IPs used by spammers and bots.

Features to Look For:

- Firewall to block malicious IP addresses.
- Malware scanning.
- File integrity checks (detect if a file was modified).
- Country/IP blocking.

Action Step: Install one security plugin only (multiple can conflict). Configure it properly and check logs weekly.

Secret #5: Limit Login Attempts

Hackers often use brute force to guess your password. If they can try unlimited times, eventually they might succeed.

Solution: Limit login attempts. After 3–5 failed tries, the IP should be locked for a period of time.

Recommended Plugins:

- Limit Login Attempts Reloaded
- WPZora SignLock (extra features: device/IP lock, country restrictions)

Why It Works: Bots are lazy. If they get blocked after a few tries, they move on to easier targets.

Secret #6: Use SSL (HTTPS) Everywhere

SSL (Secure Socket Layer) encrypts communication between your visitor's browser and your server. Without SSL, hackers can intercept data like login details or payment info.

Why It's Critical:

- Protects sensitive information.
- Google ranks HTTPS sites higher.
- Visitors trust the green padlock.

How to Implement:

- Use free SSL from Let's Encrypt (most hosts provide it).
- Or buy a premium SSL for business/financial sites.
- Force HTTPS using a plugin like Really Simple SSL or through .htaccess.

Pro Tip: Always redirect HTTP to HTTPS to avoid duplicate content issues in SEO.

Secret #7: Hide Your wp-admin and Login Page

Hackers know that /wp-admin and /wp-login.php exist on every WordPress site. They send bots to hammer these pages.

Solution: Change your login URL. Example: /mysecure-login/

Tools:

- WPS Hide Login
- WPZora SignLock (with built-in login masking)

Extra Tip: Combine this with IP whitelisting (allow only your IPs) for maximum protection.

Secret #8: Regular Backups Are Non-Negotiable

Even the best security can't guarantee 100% safety. That's why backups are your last line of defense.

What to Back Up:

- Database (posts, pages, users).
- wp-content (themes, plugins, uploads).
- wp-config.php and .htaccess.

Best Practice:

- Automate daily backups.
- Store offsite (Google Drive, Dropbox, Amazon S3).
- Test restore once a month.

Recommended Plugins: UpdraftPlus, BlogVault, WPVivid.

Scenario: Imagine your site gets hacked tomorrow. With backups, you can be back online in hours instead of losing everything.

Secret #9: Protect wp-config.php and Core Files

Your wp-config.php file contains the keys to your kingdom: database credentials and security salts. If attackers get this file, your site is finished.

How to Protect:

- Move it one directory above root (if your host supports).
- Use .htaccess to block direct access:

```
<files wp-config.php>
order allow,deny
deny from all
</files>
```

- Set file permissions correctly:
  - wp-config.php = 400 or 440
  - .htaccess = 444

Other Hardening Steps:

- Disable directory browsing.
- Remove readme.html (reveals WP version).

Secret #10: Monitor and Audit Regularly

Security is not "set and forget." It's an ongoing habit.

Why Monitoring Matters:

- Detects suspicious logins.
- Shows if a file was changed.
- Alerts you if someone installs a plugin without permission.

Tools:

- WP Activity Log
- Sucuri SiteCheck
- Hosting-level security dashboards

Monthly Audit Checklist:

- Review all user accounts (remove old ones).
- Check plugin list (delete unused).
- Verify backups are working.
- Scan for malware.

Conclusion

WordPress security is not about achieving perfection. It's about raising the cost of attack so high that hackers give up and move on.

By applying these 10 WordPress Security Secrets, you:

- Protect your website from 90% of common attacks.
- Safeguard your business reputation.
- Give your visitors the confidence to trust you.

Security is an investment, not an expense. And now, with WPZora Proxy Shield plus this guide, you're already steps ahead of most site owners.

Remember: A secure site is a successful site.

****