

**The Ultimate** [**WORDPRESS SECURITY**](https://secure.wphackedhelp.com/blog/wordpress-security-checklist-guide/) **Checklist [2019]**



Part 1: Simple Steps to Secure WordPress

**ALWAYS Keep Your Version of WordPress Up-To-Date**

1. Don’t Change WordPress Core
2. Make Sure All Your Plugins Are Updated
3. Remove Any Inactive or Unused Plugins
4. Make Sure All Themes Are Kept Updated
5. Install Themes, Plugins and Scripts ONLY From Their Official Source
6. Choose a Secure WordPress Hosting Service
7. Make Sure Your Site is Running the Latest Version of PHP
8. Change the Admin Username
9. Always Use Strong Passwords
10. Don’t Reuse Passwords
11. Protect Your Password(s) By Avoiding Plain-Text Password Transmission
12. Only Update Your Site From Trusted Networks
13. Use a Local Anti-Virus
14. Enable Google Search Console
15. Secure WordPress With a Bulletproof WordPress Security Plugin
16. If All Else Fails, Restore From Backup





SECURITY:

**Ultimate 32-Step Checklist**



Part 2: Advanced Steps for Security Freaks

. Limit Login Attempts

1. Enable Two-Factor Authentication
2. Ensure File Permissions Are Correct
3. Change the Default Table Prefix
4. Ensure You’ve Set WordPress Secret Authentication Keys
5. Disable PHP Execution
6. Segregate Your WordPress Databases
7. Restrict Database User Privileges
8. Disable File Editing
9. Secure Your wp-config.php File
10. Disable XML-RPC (If You Aren’t Using It)
11. Disable PHP Error Reporting
12. Install a Firewall
13. Use a Content Delivery Network Firewall
14. Monitor Your WordPress Security With Security Logging



Part 3: Steps for Webmasters

**HOSTING**



Ideally on a dedicated instance or server



For shared hosting, ensure that sites are isolated or “jailed”



Run an https-only website

**USER MANAGEMENT**

Grant only as much access as is needed

Review your user list frequently, deleting those that are obsolete, downgrading roles where possible

**WORDPRESS CORE, THEMES AND PLUGINS**

Enable auto-updates wherever possible / practical

Check for updates frequently (at least weekly) and install them as soon as possible. Only download themes and plugins from trusted sources

Remove all unused themes, plugins and old unused WordPress installations immediately

**AUTHENTICATION**

Ideally use 2-factor authentication

Require strong passwords for all users

Ensure that your login page is running on an https page

Limit the rate of login attempts

**SERVER ADMINISTRATION**

Only communicate with your server using an encrypted connection (sFTP for file transfer or SSH for shell access)

If you connect to your server over a public network, use a VPN

**SERVER ADMINISTRATION (CONTINUED)**

Secure access to your wp-config.php file, including copies



Secure access to your backups, log files, test files, temporary files and other PHP applications on your web server

Backup your WordPress files and database at least weekly

Use a strong password for your MySQL database user

Install a WordPress security plugin

**FEATURES TO LOOK FOR IN A WORDPRESS SECURITY PLUGIN**

Malware scanning Brute-force login protection

Protection against hacker recon techniques

Rate based throttling and blocking

Two-factor authentication

Password auditing

Country blocking

Advanced blocking techniques

**SECURE YOUR WORK ENVIRONMENT**

Protect your internet connection by using a VPN, especially on public networks

Only install trusted software on your workstation and mobile device

Use a reputable virus scanner

Protect your devices with strong passwords

Watch out for phishing, spear phishing and social engineering attacks

**TAKE STEPS TO DETECT HACKS EARLY**

Visit your site often

Search for your website in Google frequently

Set up email alerts in Google Search Console

Use a malware scanner like [WP hacked Help](https://secure.wphackedhelp.com/) and set up email alerts

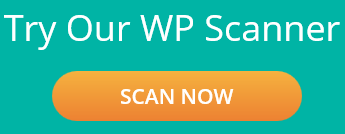
Investigate customer reports immediately



Use a source code scanner to verify site integrity

Use a website monitoring service that detects site changes

Watch for unexplained spikes in site traffic

[](https://secure.wphackedhelp.com/scanner.html?affCode=wphhorganic)

**Also See Our Top Rated Posts**

[Best WordPress Security Services & Plugins 2019 - How To Choose](https://secure.wphackedhelp.com/blog/best-wordpress-security-services/)

[How To Setup WordPress Two-Factor Authentication (2FA)](https://secure.wphackedhelp.com/blog/wordpress-two-factor-authentication/)

[Virtual Hardening & WAF 🛡️ How Does It Hardens WordPress?](https://secure.wphackedhelp.com/blog/virtual-hardening-waf-harden-wordpress/)

[How to Fix Error Establishing a Database Connection in WordPress?](https://secure.wphackedhelp.com/blog/fix-error-establishing-database-connection-wordpress/)

[WordPress Pharma Hack What It is & How To Fix It?](https://secure.wphackedhelp.com/blog/wordpress-pharma-hack-fix/)

[Website Security For Small Business - A Big Concern in 2019](https://secure.wphackedhelp.com/blog/website-security-for-small-business/)

[How To Disable Directory Browsing in WordPress Via .htaccess & Plugins](https://secure.wphackedhelp.com/blog/disable-directory-browsing-wordpress/)

[WordPress Arbitrary File Deletion Vulnerability Exploit FIXED](https://secure.wphackedhelp.com/blog/fix-wordpress-arbitrary-file-deletion-vulnerability-exploit/)