WORDPRESS SECURITY:
The Ultimate 32-Step Checklist

Part 1: Simple Steps to Secure WordPress

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

WORDPRESS SECURITY:

The Ultimate 32-Step Checklist

Part 2: Advanced Steps for Security Freaks

- [ ] 18. Limit Login Attempts
- [ ] 19. Enable Two-Factor Authentication
- [ ] 20. Ensure File Permissions Are Correct
- [ ] 21. Change the Default Table Prefix
- [ ] 22. Ensure You've Set WordPress Secret Authentication Keys
- [ ] 23. Disable PHP Execution
- [ ] 24. Segregate Your WordPress Databases
- [ ] 25. Restrict Database User Privileges
- [ ] 26. Disable File Editing
- [ ] 27. Secure Your wp-config.php File
- [ ] 28. Disable XML-RPC (If You Aren't Using It)
- [ ] 29. Disable PHP Error Reporting
- [ ] 30. Install a Firewall
- [ ] 31. Use a Content Delivery Network Firewall
- [ ] 32. Monitor Your WordPress Security With Security Logging