WordPress Security

SecuPress Checklist

Secure Your WordPress Now!

The ultimate 32 items to begin with security

Part 1: Users

☐ 1. Disable user registration if not needed

☐ 2. Limit the number of bad login attempts

☐ 3. Use a Two-Factor Authentication

☐ 4. Use a Captcha on your login page

☐ **5. Move the login page**

☐ **6. Force strong passwords**

☐ **7. Check the user list and delete the obsolete ones**

☐ 8. Downgrade old user roles when possible

Part 2: Plugins & Themes

☐ 9. Delete deactivated plugins

☐ 10. Delete unused themes

☐ **11. Update plugins**

☐ **12. Update themes**

Part 3: WordPress Core

☐ **13. Update the WordPress core**

☐ 14. Allow the automatic minor updates

☐ 15. Avoid using the default wp_ DB prefix

☐ 16. Disable the XML-RPC if you don't use it

☐ 17. Disable the REST API if you don't use it

Part 4: Sensitive Data

☐ 18. Prevent directory listing

☐ 19. Block too long url

☐ 20. Block SQL Injection attempts

☐ 21. Ban bad IPs

☐ 22. Use the correct rights on your file with chmod

Part 5: Don't forget to...

☐ 23. Schedule backups for your DB daily

☐ 24. Schedule backups for your files weekly

☐ **25. Choose a solid hosting company**

☐ 26. Use an updated antivirus on your computer

☐ **27. Don't connect your mobile on untrusted wifi networks**

☐ 28. Don't share your email box, it's like your toothbrush

☐ 29. Visit your site often to detect hacks as soon as possible

Part 6: Post Hack Aftermath

☐ 30. Hire a professional to help you

☐ **31. Install a plugin able to protect your site by taking care of a maximum of items from this security list**

☐ 32. Learn from previous mistakes and reinforce your WordPress

TRY SECUPRESS NOW