WORDPRESS SECURITY CHECKLIST (2026)

With Completion Tracker in The end of This PDF

Protect Your Site from Hacks & Malware - WPRole.com

INTRODUCTION

Use this checklist to secure your WordPress site. Go through each item and check it off once completed. Review this checklist monthly to maintain strong security.

SECTION 1: USER SECURITY

☐ Limit Administrator Accounts

- Keep only 1-2 trusted users as Administrators
- Downgrade unnecessary admins to Editor or lower
- Never give admin access to freelancers or clients

☐ Delete "admin" Username

- Create new admin account with unique username
- Log in with new account
- Delete old "admin" account
- Assign content to new account

☐ Enable Two-Factor Authentication (2FA)

- Install Wordfence or Sucuri Security plugin
- Enable 2FA for all Administrators
- Enable 2FA for all Editors (recommended)
- Enable 2FA for Shop Managers (if using WooCommerce)

☐ Use Strong Passwords

- Minimum 12 characters
- Mix of uppercase, lowercase, numbers, symbols

- No dictionary words or personal info
- Use password manager (LastPass, 1Password, Bitwarden)

☐ Limit Login Attempts

- Install Wordfence or Login LockDown plugin
- Set maximum login attempts to 3-5
- Set lockout duration to 24 hours
- Enable email notifications for lockouts

☐ Change Login URL (Optional)

- Install WPS Hide Login plugin
- Change from /wp-login.php to custom URL
- Example: /my-secret-login-2026
- Save new URL in password manager

☐ Audit User Roles Monthly

- Review all user accounts
- Remove inactive users (90+ days)
- Downgrade users with excessive permissions
- Delete accounts with fake/disposable emails

SECTION 2: SOFTWARE UPDATES

☐ Enable WordPress Auto-Updates

- Go to Settings → General
- Enable auto-updates for WordPress core
- Or manually update within 24 hours of release

☐ Update Plugins Promptly

- Update plugins within 48 hours of release
- Remove unused plugins (delete, don't deactivate)
- Only use plugins from trusted sources
- Check plugin reviews and ratings before installing

☐ Update Themes Promptly

- Update themes within 48 hours of release
- Remove unused themes (delete, don't deactivate)
- Only use themes from trusted sources
- Avoid nulled (pirated) themes

☐ Remove Unused Plugins & Themes

- Delete all inactive plugins
- Delete all inactive themes
- Keep only essential, well-maintained plugins
- Keep only 1 active theme (+ parent theme if child theme)

SECTION 3: HARDENING WORDPRESS

☐ Disable File Editing

- Add to wp-config.php:
  define('DISALLOW_FILE_EDIT', true);
- Prevents editing plugins/themes from dashboard

☐ Set Correct File Permissions

- Files: 644 (owner read/write, others read)
- Directories: 755 (owner r/w/x, others r/x)
- wp-config.php: 440 or 400 (read-only)
- Use FTP or hosting control panel to change

☐ Protect wp-config.php

- Move wp-config.php one level above WordPress root
- Or set permissions to 440 or 400
- This makes it inaccessible via web browser

☐ Disable XML-RPC

- Add to .htaccess:
  # Disable XML-RPC
  <Files xmlrpc.php>
  order deny,allow
  deny from all
  </Files>
- Prevents XML-RPC attacks

☐ Disable Directory Browsing

- Add to .htaccess:
  Options All -Indexes
- Prevents attackers from viewing directory contents

☐ Add Security Headers

- Add to .htaccess or use plugin:
  Header set X-Content-Type-Options "nosniff"
  Header set X-Frame-Options "SAMEORIGIN"
  Header set X-XSS-Protection "1; mode=block"

SECTION 4: SECURITY PLUGINS

☐ **Install Security Plugin**

Choose ONE of these:

- Wordfence Security (FREE + PREMIUM) - RECOMMENDED
- Sucuri Security (FREE + PREMIUM)
- iThemes Security (FREE + PREMIUM)
- All In One WP Security (FREE)

☐ **Enable Firewall Protection**

- Activate firewall in your security plugin
- Enable real-time threat defense (if premium)
- Configure firewall rules for your site

☐ **Enable Malware Scanning**

- Schedule daily or weekly scans
- Enable email alerts for detected malware
- Review scan reports regularly

☐ **Enable Login Security**

- Enable 2FA (see Section 1)
- Enable login attempt limiting (see Section 1)
- Enable reCAPTCHA on login form (optional)

☐ **Set Up Email Alerts**

- Configure email notifications for:
  - Failed login attempts
  - Malware detection
  - File changes
  - User account changes
- Use dedicated security email (not your main email)

SECTION 5: MONITORING & LOGGING

☐ Enable Activity Logging

- Install WP Activity Log or Simple History plugin
- Log user logins/logouts
- Log content changes (posts, pages, comments)
- Log plugin/theme changes
- Log user account changes
- Log settings changes

☐ Set Up Uptime Monitoring

- Use Uptime Robot (FREE) or Pingdom (PREMIUM)
- Check every 5 minutes
- Enable email/SMS alerts when site goes down
- Monitor from multiple locations

☐ Monitor File Changes

- Enable file change detection in security plugin
- Get alerts when core files are modified
- Get alerts when plugins/themes are modified
- Review file change alerts immediately

☐ Review Logs Weekly

- Check activity logs every week
- Look for:
  - Multiple failed login attempts
  - Unusual file changes
  - Unknown user accounts created
  - Plugins/themes installed without your knowledge
- Investigate and resolve any anomalies

SECTION 6: BACKUPS

☐ Set Up Daily Backups

- Use UpdraftPlus (FREE) or your hosting's backup solution
- Backup entire site (files + database)
- Schedule daily backups (or at least weekly)
- Store backups off-site (Google Drive, Dropbox, Amazon S3)

☐ Keep 30+ Days of Backups

- Retain at least 30 days of backup history
- More is better (90 days recommended)
- Delete old backups automatically to save space

☐ Test Backups Monthly

- Restore from backup on staging site
- Verify all content is intact
- Check database is complete
- Test site functionality after restore
- Document any issues

☐ Backup Before Major Changes

- Always backup before:
  - WordPress core updates
  - Major plugin updates
  - Theme changes
  - Site migrations
  - Security plugin changes

SECTION 7: DATABASE SECURITY

☐ Change Database Prefix

- Default: wp_
- Change to random prefix: x7k9m_ or similar
- Use plugin like iThemes Security or do manually
- Makes SQL injection attacks harder

☐ Use Strong Database Password

- Minimum 20 characters
- Mix of uppercase, lowercase, numbers, symbols
- No dictionary words
- Store in password manager

☐ Limit Database User Permissions

- Database user should only have permissions for:
  - SELECT, INSERT, UPDATE, DELETE
- Should NOT have: DROP, CREATE, ALTER
- Configure via hosting control panel or phpMyAdmin

SECTION 8: SSL & HTTPS

☐ Install SSL Certificate

- Use Let's Encrypt (FREE) or your hosting's SSL
- Ensure certificate is valid (not expired)
- Set up auto-renewal

☐ Force HTTPS

- Go to Settings → General
- Change WordPress Address to https://
- Change Site Address to https://
- Or use Really Simple SSL plugin (FREE)

☐ Enable HSTS (Optional)

- Add to .htaccess:
  Header set Strict-Transport-Security "max-age=31536000; includeSubDomains"
- Forces browsers to always use HTTPS

SECTION 9: POST-HACK RECOVERY

☐ Take Site Offline

- Enable maintenance mode
- Or upload static index.html with "Under Maintenance"

☐ Change All Passwords

- All WordPress admin accounts
- Database password (via hosting)
- FTP/SFTP accounts
- Hosting account
- Email accounts

☐ Scan for Malware

- Run full scan with Wordfence or Sucuri
- Review scan results
- Quarantine or delete infected files

☐ Restore from Clean Backup

- Find backup from before the hack
- Delete all WordPress files (via FTP)
- Drop all database tables (via phpMyAdmin)
- Restore files and database from backup
- Update all passwords
- Update WordPress, plugins, themes

☐ Audit User Accounts

- Delete unknown users
- Change all passwords
- Enable 2FA for all users
- Downgrade unnecessary Administrators

☐ **Request Google Review (If Blacklisted)**

- Go to Google Search Console
- Security & Manual Actions → Security Issues
- Click "Request Review"
- Explain what you did to fix the hack
- Wait 1-3 days for review

SECTION 10: ONGOING MAINTENANCE

☐ Weekly Tasks

- Review activity logs
- Check for failed login attempts
- Verify backups are running
- Check uptime monitoring

☐ Monthly Tasks

- Audit user roles (see Section 1)
- Review and update plugins
- Test backup restoration
- Review security plugin settings
- Check SSL certificate expiration

☐ Quarterly Tasks

- Full security audit (all sections above)
- Deep database audit
- Review and update security policies
- Test disaster recovery plan
- Update documentation

☐ After Any Security Incident

- Immediate full audit
- Change all passwords
- Review activity logs
- Scan for malware
- Update all software
- Document incident and lessons learned

BONUS: SECURITY TOOLS & RESOURCES

Recommended Security Plugins:

• Wordfence Security - https://wordpress.org/plugins/wordfence/
• Sucuri Security - https://wordpress.org/plugins/sucuri-scanner/
• iThemes Security - https://wordpress.org/plugins/better-wp-security/
• All In One WP Security - https://wordpress.org/plugins/all-in-one-wp-security-and-firewall/

Recommended Backup Plugins:

• UpdraftPlus - https://wordpress.org/plugins/updraftplus/
• BackupBuddy - https://ithemes.com/backupbuddy/
• BlogVault - https://blogvault.net/

Recommended Monitoring Tools:

• Uptime Robot - https://uptimerobot.com/ (FREE)
• Pingdom - https://www.pingdom.com/ (PREMIUM)
• Jetpack Monitor - https://jetpack.com/ (FREE)

Official Resources:

• WordPress.org Security - https://wordpress.org/support/article/hardening-wordpress/
• WPBeginner Security - https://www.wpbeginner.com/wordpress-security/
• Kinsta Security - https://kinsta.com/blog/wordpress-security/

COMPLETION TRACKER

Section 1: User Security [___/7]
Section 2: Software Updates [___/4]
Section 3: Hardening WordPress [___/6]
Section 4: Security Plugins [___/5]
Section 5: Monitoring & Logging [___/4]
Section 6: Backups [___/4]
Section 7: Database Security [___/3]
Section 8: SSL & HTTPS [___/3]
Section 9: Post-Hack Recovery [___/6]
Section 10: Ongoing Maintenance [___/4]

TOTAL COMPLETED: [___/46]

NOTES

Write your notes, action items, and reminders here:

_____

_____

_____

_____

_____