Bipul Roy
bipulroy.com

WordPress Security Checklist

Essential practices for securing WordPress websites.

Core System Security

- Keep WordPress core, themes, and plugins updated
- Remove unused plugins and themes
- Avoid outdated or abandoned plugins
- Use least-privilege user roles
- Avoid 'admin' username
- Enable strong passwords and 2FA
- Limit login attempts

Plugin & Theme Security

- Use only necessary plugins
- Prefer well-maintained plugins
- Avoid bloated multipurpose plugins
- Use lightweight, custom themes when possible

Hosting & Server Security

- Use reliable managed hosting
- Keep PHP updated
- Use correct file permissions (644/755)
- Disable file editing in WordPress
- Protect wp-config.php and sensitive files

Backup & Recovery

- Automate backups (daily or weekly)
- Store backups offsite
- Test restoration process regularly

Monitoring & Detection

- Enable activity logging
- Run malware scans
- Monitor uptime and performance

Performance & Security

- Reduce plugin count
- Optimize database
- Remove unused assets
- Avoid unnecessary scripts

Access Control & Workflow

- Use staging environments
- Separate code and content workflows
- Restrict admin access

Database Security

- Use secure database credentials
- Limit database permissions
- Clean up unused data

HTTPS & Data Protection

- Enforce HTTPS
- Redirect HTTP to HTTPS
- Secure cookies

Ongoing Maintenance

- Weekly updates and checks
- Monthly plugin and performance review
- Quarterly full security audit

Security is an ongoing process — not a one-time setup.

If you’re unsure whether your WordPress site follows these practices, I offer structured security audits and ongoing maintenance.