WordPress Security Checklist

Web-Smart.Co

Best SEO Agency in Hertfordshire

Protect your WordPress website with this comprehensive 30-point security checklist. Covers plugins, backups, user permissions, malware prevention, and essential security hardening measures.

Basic Security

'   Keep WordPress core updated to latest version

'   Update all plugins regularly

'   Update theme to latest version

'   Use strong passwords (20+ characters)

'   Enable two-factor authentication

'   Limit login attempts

'   Change default "admin" username

'   Use different usernames for different sites

'   Remove unused plugins and themes

'   Use SSL certificate (HTTPS)

Advanced Security

- ' Install security plugin (Wordfence, Sucuri)
- ' Enable firewall protection
- ' Scan for malware regularly
- ' Hide WordPress version number
- ' Disable file editing in wp-admin
- ' Change database table prefix
- ' Protect wp-config.php file
- ' Disable XML-RPC if not needed
- ' Add security headers
- ' Implement Content Security Policy

Backup Strategy

- ' Automated daily backups
- ' Store backups offsite (cloud storage)
- ' Test backup restoration regularly
- ' Backup database separately
- ' Include all files and media
- ' Retain backups for 30+ days
- ' Document backup process
- ' Set up automated backup notifications
- ' Use reliable backup plugin
- ' Have disaster recovery plan

User Management

- '   Assign appropriate user roles

- '   Remove unused user accounts

- '   Monitor user activity logs

- '   Restrict access to wp-admin

- '   Use role-based permissions

- '   Disable user enumeration

- '   Require strong passwords for all users

- '   Regular security audits of users

- '   Limit administrator accounts

- '   Review and update permissions regularly

Need WordPress Security Help?

Web-Smart.Co offers WordPress security services:

- Complete security audits
- Ongoing maintenance and monitoring