# Website Security Checklist

1. Regular Software Updates - Ensure your CMS (WordPress, Joomla, etc.), plugins, and themes are always up-to-date.

2. Use Strong, Unique Passwords - Create complex passwords for all logins (admin panel, hosting, database) and update them regularly.

3. Enable Two-Factor Authentication (2FA) - Add an extra layer of security by requiring a second form of verification.

4. Install an SSL Certificate - Encrypt data transferred between your site and its users.

5. Limit Login Attempts - Prevent brute force attacks by restricting the number of failed login attempts.

6. Use a Web Application Firewall (WAF) - Protect your site from malicious traffic and common threats.

7. Backup Your Website Regularly - Schedule automated backups daily, and store copies offsite for recovery.

8. Scan for Malware and Vulnerabilities - Perform regular security scans to detect malicious code or vulnerabilities.

9. Remove Unused Plugins and Themes - Deactivate and delete any unnecessary plugins or outdated themes.

10. Secure File Permissions - Set proper file permissions (e.g., 644 for files and 755 for directories) to restrict unauthorized access.

11. Disable Directory Browsing - Prevent hackers from viewing your website's directory structure.

12. Monitor Website Activity Logs - Track user logins, failed login attempts, and changes to files.

13. Change Default Login URLs - Rename the default admin login path (e.g., /wp-admin or

/administrator).

14. Secure Your Database - Use complex database names and prefixes to avoid SQL injection attacks.

15. Deactivate File Editing from Dashboard - Prevent hackers from editing files directly from your WordPress dashboard.