WordPress Security Checklist

Important – Read Me

Many of the tasks listed in the checklist below can be completed by non-technical users simply by following the tutorials in our **WordPress Security** training module.

Some tasks, however, should only be carried out by more technically advanced users. If you don't understand what to do or don't feel confident performing one or more tasks, please ask a professional and experienced WordPress service provider for assistance.

Always backup your WordPress site (database and files) before making changes to files. Even small mistakes can have disastrous consequences if you are not careful.

Please note that we have no control over the software and services mentioned in this checklist and that under no circumstances will we be held responsible for any losses or damages incurred either directly or indirectly as a result of following the recommendations below.

For updated links to all of the tutorials and resources listed on this checklist, go here:

http://wpcompendium.org/wordpress-security/wordpress-security-checklist

Basic Website Security Checklist:

- ❑ **Computer is fully protected** and free of spyware, malware, and viruses (antivirus, malware scanner, and firewall installed and active), and the operating system is up to date.
- ❑ **Password management system** in place (e.g. **Roboform**)
- ❑ WordPress site is hosted with a trusted and reliable **webhost**
- ❑ **Download files are protected**.

WordPress Security Setup Checklist:

- ❑ Protect your site against **spam** (Install an antispam plugin, e.g. *Akismet*)
- ❑ Perform a full **security scan** of your WordPress files (Install a security scan plugin, e.g. **Defender**).
- ❑ Secure your **WP database** (change database table prefix).
- ❑ Option 1: Install a **brute-force attack prevention plugin** (e.g. *Login Lockdown*, *Limit Login Attempts*), or
- ❑ Option 2: Install a comprehensive security plugin (e.g.
- ❑ **Defender**)
- ❑ Secure your *wp-admin* folder.
- ❑ Secure your *uploads* folder.
- ❑ Secure your *wp-config.php* file.
- ❑ Delete redundant WordPress core files (e.g. readme.html, install.php, etc.)
- ❑ Set **secure permissions** for files and folders.
- ❑ Protect server directories (e.g. add empty index.php files to directories)
- ❑ Add a secure admin user.
- ❑ Set correct permissions for users (**User Roles and Capabilities**)
- ❑ Remove user registration capabilities (if not required)
- ❑ Set up an Intrusion Detection System (Install a **file monitoring plugin**, e.g. *File Monitor Plus*)
- ❑ Add **Antivirus protection** (Install an antivirus plugin, e.g. *Antivirus for WordPress*)
- ❑ Add Firewall protection (Install a firewall plugin like *WordPress Firewall 2*, *Block Bad Queries*, etc …)
- ❑ Enable data logging and archiving.
- ❑ Secure PHP.
- ❑ Set up hosting monitoring (e.g. **Uptime**, **Sucuri**)

WordPress Security Maintenance Checklist:

Schedule the tasks below to be performed on a regular basis:

- ❑ Learn how to perform a complete **WordPress maintenance routine**.
- ❑ **Backup your site manually** using cPanel once, and then every so often.
- ❑ Install an automatic data backup system (e.g. **Snapshot**)
- ❑ Schedule **automated WordPress backups** (e.g. weekly, monthly).
- ❑ Perform a complete **security scan**.
- ❑ Check site files, logs, and security plugin reports.
- ❑ **Change passwords** every so often
- ❑ Perform regular WordPress updates
    - Keep **WordPress software** up to date
    - Keep **WordPress plugins** up to date
    - Keep **WordPress themes** up to date
- ❑ Delete unused files (see **How To Clean Up WordPress**)
- ❑ Delete inactive users (see **WordPress User Management**)
- ❑ Delete inactive plugins (see **How To Clean Up WordPress**)
- ❑ Delete inactive themes (see **WordPress Theme Management**)
- ❑ Subscribe to WordPress security information updates

Critical Website Information Checklist:

Have this information handy and keep it in a safe place!

- ❑ WordPress Service Provider Contact / Support Details
- ❑ WordPress Logins
- ❑ **Domain Registrar** Login
- ❑ **Hosting Company** Login
- ❑ **Email Logins** & Settings
- ❑ **FTP Login** Information
- ❑ FTP Account Data
- ❑ **Amazon S3 Account** Logins
- ❑ **Google Account** Logins
- ❑ Social Media Account Logins
- ❑ API Keys & Permission Codes
- ❑ Activation Keys (e.g. Premium WordPress plugins and themes)
- ❑ Browser Add-Ons Data