WordPress Website Security Checklist

When looking at the security of your WordPress website, use this checklist as a quick reference guide to make sure you've covered all the points.

□ Latest version of WordPress installed

□ All theme and plugins are up-to-date

□ Double check plugins in use have been updated recently by developer

□ Deleted all unneeded themes

□ Removed any unnecessary and inactive plugins

□ Install & set-up anti-virus software on computer

□ Create hard to guess usernames

□ Set-up super strong passwords for administrator and all other users

□ Change password every 3 months

□ Assign each user only the role they need

□ Hide author usernames

□ Password protect your admin directory

□ Prevent directory browser

□ Use correct file and directory permissions

□ Add two-factor authentication (google authenticator, clef)

□ Update your security authentication keys (https://api.wordpress.org/secret-key/1.1/salt/)

□ Move wp-config file up a directory

□ Backup website (files and database) before outsourcing any work. Delete their WordPress user and FTP account when they are done with the work.

the PORTABLE ENTREPRENEUR

www.PortableEntrepreneur.com

□ Disable the theme and plugin editor

□ Deny access to wp-login via .htaccess file

□ Deny access to wp-config.php file via .htaccess

□ Change default WordPress database prefix

□ Schedule a periodic review of your site (to remove plugins, extra files, etc)

□ Put website on best host possible for your budget