Wordpress Security Checklist

This basic checklist will help you secure your Wordpress website. Please note that this checklist should not be seen as comprehensive. These practices will protect your website from most rudimentary and fundamental attack attempts.

- ❑ You have a security plugin like iThemes Security set up and configured.
- ❑ You've changed the /wp-admin/ URL so bots can't find it.
- ❑ All user levels require strong passwords.
- ❑ You have a website database and file backup plugin configured, like UpDraft Plus.
- ❑ Two-factor authentication (spam-prevention) is active on your website.
- ❑ There is no user with the ID of 1 on your website.
- ❑ The default "admin" user has been renamed or deleted.
- ❑ Your Wordpress website's database has a custom, random name. Not the default "wrd01" name.
- ❑ Your Wordpress website's database uses a custom prefix. Not the default "_wp" prefix.
- ❑ In your wp-config.php file, you have re-generated the Wordpress Salts.
- ❑ In FTP, you've deleted these files: install.php, upgrade.php, wp-config-sample.php, & readme.html.
- ❑ Your wp-config.php and .htacess files have the proper permissions of 644 or 444 set.
- ❑ In wp-config.php, you've added code to disable Dashboard access of the File Editor.
- ❑ Automatic user registration is disabled.
- ❑ Public browsing of backend folders has been disabled.
- ❑ Automatic public posting of comments is disabled.

NOTES