WordPress 101:
Basic Website Security Checklist

Ensuring that your WordPress website is secure is a multi-faceted process that will take time to perfect. This WordPress security checklist will show you how to protect your website from malicious attacks. After going through this course, you'll be able to do most (if not all!) of these things on your own.

❏ Start with a web host who follows industry security best practices. I love Siteground for budget needs and Kinsta for best-in-class performance. Both offer SSL certificates to encrypt users' personal data.

❏ Choose a strong password. WordPress can generate an *almost*-uncrackable password automatically for you.

❏ While you're at it, create a strong username as well. No, not "*admin*".

❏ Use a password manager like LastPass to easily store and recall your complicated password. You can also share passwords with other people on your team through LastPass in a much more secure fashion than emailing unencrypted login information.

❏ Use two-factor authentication for login. This pushes an expiring code to a user's phone to input as part of verifying a login session.

❏ Limit login attempts. **Login Lockdown** is set to lock a user out for an hour with an IP block after 3 failed login attempts within 5 minutes.

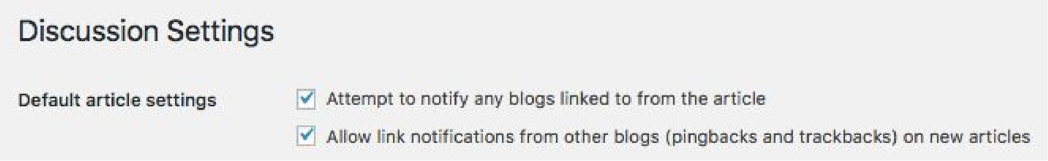
❏ Rename your WP Login/WP Admin page to something unique.

❏ Install a backup plugin like UpdraftPlus (free & premium versions available) so that if you or a hacker breaks your website, you can easily get back up and running.

❏ Update WordPress whenever a new version is available. Update plugins and themes when new versions are available. Delete any plugins and themes you aren't using. Comb through your website afterward to make sure it didn't accidentally break something. Use a WordPress maintenance service for safely taking care of updates for you.

❏ Disable trackbacks and pingbacks to help prevent comment spam and DOS attacks.

To do this, go to **Settings** > **Discussion**, then uncheck the boxes next to "*Attempt to notify any blogs linked to from the article" and "Allow link notifications from other blogs (pingbacks and trackbacks) on new articles*".



Discussion Settings

Default article settings

☑ Attempt to notify any blogs linked to from the article

☑ Allow link notifications from other blogs (pingbacks and trackbacks) on new articles

❏ Activate Akismet (free or donation) if you haven't already — this tool will help immensely with comment spam. Brought to you by the creators of WordPress — Automattic.

❏ Install a WordPress security plugin... or two. I love Wordfence (free & premium versions available) because of its firewall feature and daily email reports.

By Maddy Osman, The-Blogsmith.com

I've included affiliate links for products and services that I use and love