

# WPLOUNGE\*

## Checklist WordPress beveiligen

Gebruik de onderstaande checklist om te controleren hoe goed jouw WordPress-website beveiligd is.

Meer informatie: <https://www.wplounge.nl/checklist-wordpress-beveiligen/>

- Kies een betrouwbare hostingpartij ([meer info](#))
- Zorg dat je website alléén via HTTPS bereikbaar is ([meer info](#))
- Controleer de gebruikersaccounts en hun rechten
- Zorg dat alle gebruikers een sterk wachtwoord gebruiken
- Zorg dat gebruikers niet méér rechten hebben dan nodig ([meer info](#))
- Zorg dat de gebruikersnaam van de beheerder géén "admin" is
- Update alle themes, plugins en WordPress zelf naar de laatste versie
- Maak regelmatig (automatische) backups van je WordPress-website
- Staan er *salts and keys* in je wp-config.php-bestand? ([meer info](#))
- Verwijder het **readme.html**-bestand
- Verwijder themes en plugins die je niet nodig hebt
- Beperk het aantal login-pogingen ([meer info](#))
- Gebruik een sterk wachtwoord voor je MySQL-database
- Zet e-mail notificaties aan in Google Search Console
- Verander je database *table prefix* in iets anders dan "wp\_"
- Verander regelmatig je WordPress-wachtwoord
- Verander regelmatig het wachtwoord van je FTP-account

## Meer lezen?

<https://www.wplounge.nl/wordpress-beveiligen/>

<https://www.wplounge.nl/wordpress-website-gehackt-oplossingen/>