RESTYLES

Beveilig jouw Wordpress website met deze 8 tips.

+ Checklist!

RESTYLES

BEVEILIG JE WORDPRESS WEBSITE

1. Kies de juiste hostingpartij

Kies een hostingpartij die maatregelen neemt om jouw website te beschermen. Zie de checklist met punten waarop je moet letten bij het kiezen van een hostingpartij.

2. Juiste Wordpress installatie

Tijdens de installatie van Wordpress op jouw website, zijn er een aantal mogelijkheden om hackers buiten de deur te houden.

3. Plugins & themes

De plugin 'Limit Login Attempts' zorgt ervoor dat men maar 3 kansen heeft om een wachtwoord in te voeren, hierna wordt het account tijdelijk geblokkeerd. Maar let op: niet alle plug-ins en themes zijn even veilig. Developers van plug-ins en themes kunnen kwade bedoelingen hebben.

4. Geef de juiste permissions

Wanneer je bent ingelogd via FTP of DirectAdmin, kun je "permissions" geven aan mappen en bestanden op je server. Geef (indien je hier verstand van hebt) de volgende permissions:

Mappen en directories: 755 of 750
Bestanden: 644 of 640
WP-config.php: 600

5. Pas het .htacces-bestand aan

Door onderstaand stukje code toe te voegen aan het .htacces-bestand wordt je website extra beveiligd:

```
<files wp-config.php>
order allow,deny
deny from all
</files>
```

Daarnaast zorg je ervoor dat er maar met één IP-adres ingelogd kan worden door de volgende code toe te voegen:

```
order deny,allow
allow from <span style="color:
#ff0000;">123.456.7.8</span>
deny from all
```

6. Two step authentication

Beveilig je Wordpress niet enkel met je gebruikersnaam en wachtwoord, maar ook met een two step authentication.

7. Verberg je WP serienummer

Als hackers het serienummer van je Wordpress weten, is het makkelijker om de website te hacken. Verberg deze daarom.

RESTYLES

Checklist

Check dit altijd even bij je hostingpartij:

- [ ] De laatste versies van PHP en MySQL worden ondersteunt.
- [ ] De server is geoptimaliseerd voor Wordpress-websites.
- [ ] De hostingpartij maakt gebruik van een firewall.
- [ ] De hostingpartij maakt regelmatig back-ups van je website.
- [ ] De hostingpartij is actief bezig met het voorkomen en oplossen van beveiligingsproblemen.

Let bij de installatie op het volgende:

- [ ] Je gebruikersnaam van Wordpress is niet de standaard 'Admin".
- [ ] Je wachtwoord is sterk, het bevat hoofdletters, kleine letters, cijfers en vreemde tekens.
- [ ] Je gebruikt niet de standaard prefix "wp_" maar bv. "wp123321_"
- [ ] Plaats in het wp-config-bestand de code van de volgende link: https://api.wordpress.org/secret-key/1.1/salt/

En houd verder rekening met deze zaken:

- [ ] De plug-in Limit Login Attempts is geïnstalleerd.
- [ ] Het serienummer van je Wordpress is verborgen.
- [ ] De juiste permissions zijn gegeven.
- [ ] Two authentication is ingesteld.
- [ ] De plug-ins en themes hebben goede recensies en worden regelmatig geüpdatet.