Seguretat Wordpress

1. No facis servir l'usuari admin

- En la instal·lació de WordPress, a l'usuari que apareix per defecte se li assigna el nom de admin. I hi ha molta gent que ho deixa tal qual.

- **No canviar el nom d'aquest usuari és un error de llibre**, ja que és el primer nom que qualsevol persona malintencionada va a provar per tractar de colar-se en el teu panell d'administració de WordPress.

- De la mateixa manera, canviar l'ID per defecte de l'usuari administrador (que normalment té com a valor el número 1) també és una bona mesura de prevenció davant atacs.

2. Mot de pas llar i complexe

- Que sigui **llarga** (com a mínim jo la faria de 12 caràcters).
- Que contingui lletres **majúscules i minúscules**.
- Que contingui **nombres**.
- Que contingui **caràcters especials** (comes, guions, símbols, etc.)

3. Canvia el prefix wp_ a les taules de la base de dades

- Igual que ocorre amb l'usuari administrador, tampoc és recomanable deixar els prefixos de taula per defecte de la instal·lació de WordPress.

- La resposta una vegada més és molt simple: **el prefix wp_ serà el primer que provin els scripts dels hackers que intenten fer-te la punyeta per colar-se on no deuen.**

- NOTA IMPORTANT: el nou prefix que vagis a utilitzar no necessàriament han de ser només **dos caràcters**. Poden ser més.

4. Fes servir un pluguin de seguretat

- Pues eso... jo recomano aquest.

7. Fer servir un pluguin antispam

8. Modificar la URL d'accés al teu panell d'administració

- Igual que t'he dit amb l'usuari o el prefix de les taules a la base de dades, deixar obert al públic la típica URL miweb.com/wp-admin no és per res recomanable.

- El millor és que canvies aquest wp-admin del final per **una altra paraula o seqüència de caràcters diferent.**

- **Millor que ho facis via pluguin de seguretat si no tens clar com es fa.**

9. No vagis donant alegrement usuaris administradors a tothom

- Només ha d'haver com a molt dos administradors.
- La resta de gent millor que tingui usuari editor o publicador.

10. Pluguins sempre actualitzats

- I que surtin d'un lloc de confiança si no els captes directament desde el Panel de Control del teu lloc WP.
- La resta de gent millor que tingui usuari editor o publicador.
- Fuig en la mesura del possible de connectors que porten sense actualitzar-se molt temps o que ja no compten amb noves actualitzacions.

11. Oju amb les plantilles gratuites

- I amb molts llocs web que ofereixen plantilles gratuïtes que després no son bones i a més porten mil porqueries. Agafa plantilles de llocs de confiança.

12. Actualitza sempre la versió de WordPress

- Les noves versions que surten periòdicament per a WordPress permeten precisament anar **combatent les vulnerabilitats del CMS** i els nous tipus d'atac que van sorgint amb el pas del temps, de manera que aquesta tasca d'implementar aquestes noves versions és una cosa que no has de deixar passar.

13. Protegeix les carpetes i els arxius

- Com t'he esmentat en el punt anterior, totes les instal·lacions de WordPress tenen carpetes i fitxers amb noms i característiques similars.

- Aquests fitxers són precisament els que més cal cuidar i sobreprotegir, ja que són la base del funcionament del teu gestor de continguts.

13. Protegeix les carpetes i els arxius

- El dolent d'aquests fitxers és que no es pot canviar el seu nom com sí que passava amb el prefix de la base de dades o l'usuari administrador.

- Per això, no està de més que els facis **el menys visible possible**, evitant la seva indexació o l'accés dels bots de Google a ells, així com tirant un cop més de iThemes Security per capar-los en la mesura del possible.