10 MESURES DE SEGURETAT IMPRESCINDIBLES PEL TEU WORDPRESS

En aquest article veurem deu mesures de seguretat imprescindibles per mantenir la nostra pàgina web en bon estat i evitar atacs i virus que la puguin perjudicar.

1. Fes servir una contrasenya difícil d'esbrinar.

La primera i més important mesura de seguretat a WordPress és incorporar una contrasenya difícil d'esbrinar.

Per això, són recomanables les contrasenyes denominades "fortes"; aquelles que incorporen molts caràcters (més de vuit) i que combinen lletres, números i signes de puntuació.

Quan canviem la contrasenya, el mateix WordPress ens indicarà el seu nivell de seguretat. També existeixen pàgines web i connectors per comprovar la seguretat de la contrasenya. Per exemple: Kaspersky.

2. No facis servir la paraula "admin" com a nom d'usuari.

Una altra de les mesures de seguretat obligatòries que haurem de dur a terme és eliminar la paraula "admin", que és el nom d'usuari que WordPress assigna per defecte. Els pirates informàtics, ja siguin persones o robots, el primer que intenten és accedir a la pàgina amb aquest nom, perquè és el més evident. Per això podem crear un nou usuari des del *backend* del web i eliminar "admin". Cal tenir en compte que tampoc no hauríem de fer servir el nom del web com a nom d'usuari. Es tracta d'un altre recurs massa fàcil per accedir-hi.

3. Fes còpies de seguretat amb regularitat.

Aquest és un altre dels punts més importants per mantenir la seguretat del nostre web. Hem de fer còpies de manera periòdica i sempre fer-les en servidors externs, fora del mateix WordPress, per evitar perdre-ho tot de cop.

4. Posa límits als intents d'accedir al web.

Una altra mesura important per a la seguretat del web és limitar els intents d'accés a la pàgina (*backend*). És recomanable posar només tres intents com a màxim, per si ens equivoquem nosaltres. Qualsevol *hacker* intentarà entrar a la força i provar diferents combinacions de contrasenyes i noms d'usuari, però, si ho acotem, reforçarem molt més la seguretat.

Existeixen connectors com Loginizer que ajuden a controlar-ho.

5. Controla l'*spam* als comentaris.

En una pàgina web amb blog i on hi hagi els comentaris habilitats, aquesta part és una font contínua de missatges de correu brossa i també una porta a virus i programes fraudulents. WordPress té el connector Akismet, que controla aquest aspecte, és a dir, realitza un filtre per deixar passar segons quins comentaris o missatges.

6. No instal·lis gaires connectors.

Sabem que els connectors són la manera de personalitzar i aportar diferents funcionalitats a la nostra pàgina web, però també s'ha de tenir en compte que cada connector que instal·lem és una possibilitat més de què hi hagi errors o problemes. El més recomanable és provar abans el connector en un entorn diferent del de la nostra pàgina web. Alguns programadors no fan servir codi segur i per això la nostra recomanació és instal·lar només els imprescindibles i descarregar-los de les pàgines web oficials.

7. Manté el WordPress i els connectors actualitzats.

Les actualitzacions de WordPress normalment són correccions d'errades i vulnerabilitats del sistema; per això, sempre hem de tenir la versió més recent possible. De totes maneres, hem de vigilar, perquè les actualitzacions de WordPress poden generar incompatibilitats amb alguns dels connectors. Procurem fer sempre còpies de seguretat i intentem actualitzar la pàgina de manera esglaonada.

8. No instal·lis *themes* o connectors anul·lats de WordPress.

Insistim en la importància de descarregar els *themes* i els *plugins* des de pàgines oficials. Molts ja no estan en vigor, però es poden continuar descarregant des de pàgines pirates. Evitem en tot moment fer-los servir, perquè són una font de programari maliciós i entrada de virus.

9. Tingues ubicat el WordPress en un hosting segur.

Existeixen moltes empreses que asseguren l'allotjament web i garanteixen la seva seguretat. Molts d'aquests allotjaments ja tenen l'opció de fer còpies de seguretat automàticament i també eines d'escaneig de virus.

10. Fes servir *plugins* de seguretat.

Existeixen connectors que duen a terme totes les mesures necessàries per mantenir la teva pàgina web al dia i de manera segura. Els més populars són iThemes Security i Wordfence. Aquest últim és del mateix WordPress i és un dels que funcionen millor.