

10 TIPŮ NA ZABEZPEČENÍ VAŠEHO WEBU



WordPress je redakční systém, aplikace, která vám umožní vytvořit a spravovat webové stránky. Samotná WordPress aplikace je velmi bezpečná, protože je pod odbornou kontrolou. Bezpečnost vašeho webu je ovšem úkolem pro vás jako jeho správce, protože každý web je originál – i ten váš. Může tedy obsahovat slabiny.



1. VYBÍREJTE PEČLIVĚ

komponenty (pluginy, doplňky, služby) pro váš web vybírejte pečlivě a **nechte si poradit** od odborníků. **Instalujte pouze udržované a legální doplňky.**



3. VYBERTE SI KVALITNÍ HOSTING

Vybírejte poskytovatele, **který poskytuje více vrstev zabezpečení** a záloh. Rozhodně se nevyplácí volit poskytovatele jen podle ceny.



5. POUŽÍVEJTE VÝHRADNĚ HTTPS

Přenos dat zabezpečeným protokolem **https je dnes již naprostou nutností** a bezpečnostním standardem. **Weby bez https nebudou vidět ve výsledcích vyhledávání**, nelze je propagovat reklamami.



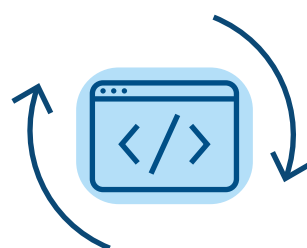
7. BRAŇTE SE AKTIVNĚ SPAMU.

Pomocí vhodných pluginů lze proti spamu velmi účinně bojovat. **Spamové komentáře** mohou představovat bezpečnostní riziko – **často obsahují škodlivé odkazy či nevyžádanou reklamu**. Kromě toho snižují kvalitu vašeho obsahu.



9. DVOUFÁZOVÉ OVĚŘENÍ

Zvykněte si na dvoufázové ověření. Velmi **spolehlivý způsob zabezpečení zahrnující propojení telefonu či jiného zařízení s WordPressem**. Po zadání hesla je nutné zadat unikátní kód, který se v krátkých intervalech mění. **Bez zadání kódu není možné se přihlásit.**



2. AKTUALIZUJTE PHP

na hostingu, WordPress i jeho součásti. Pravidelně kontrolujte dostupnost nové verze systému a **provádějte aktualizace včetně pluginů, šablon a jejich rozšíření.**



4. AKTIVNĚ ZÁLOHUJTE

Pravidelné zálohování (**ideálně na jiný server nebo úložiště**) by se mělo stát samozřejmostí. Nespoléhejte na to, že zálohuje hosting, **jde o vaše data.**



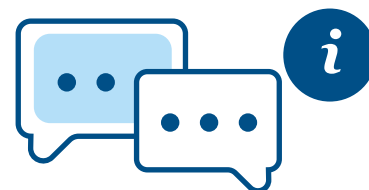
6. POUŽÍVEJTE AKTIVNÍ FIREWALL

Nainstalujte si plugin pro ochranu webu a aktivní firewall. Bezpečnostní plugin pro WordPress chrání vaše stránky před škodlivým softwarem, útoky hrubou silou a pokusy o vniknutí. Firewall monitoruje, filtruje a blokuje nežádoucí provoz a **chrání váš web před hackery a škodlivým provozem.** Ujistěte se, že je plugin **efektivně nastavený** a že je na webu pouze jeden.



8. POUŽÍVEJTE SILNÉ PŘÍSTUPOVÉ ÚDAJE

Používejte silné přístupové údaje a trezory pro jejich uložení. **Silné heslo je základem bezpečnosti.** Jako jméno nepoužívejte slova admin, administrator, wordpress a podobná. **Tyto údaje si ukládejte do trezoru na hesla a propojte jej s prohlížečem.**



10. BUĎTE INFORMOVANÍ

Čtěte informace a snažte se jim alespoň rámcově porozumět. **Ptejte se. Čtěte blogy. Absolvujte vzdělávací kurz.** Chodte na online i offline setkání uživatelů WordPressu a seznámte se s ostatními.

Chci návod na zabezpečení webu



Pokud si chcete web zabezpečit, požádejte o zaslání návodu, který vás provede nastavením populárního pluginu WordFence a vysvětlí vám, co a jak v něm nastavit.