

Segurança Wordpress

Recomendamos fortemente que alguns passos sejam realizados para melhorar a segurança de plataformas WordPress, sendo

- Renomear usuários padrões para nomes alternativos, exemplo: admin -> Administrador.

Ao realizar o cadastro de uma instalação do WordPress, realizar **alteração do nome de usuário**, para fugir do padrão e diminuir as chances de um possível ataque de força bruta ao painel Wordpress.

- Usar senhas fortes para usuários administrativos.

Recomendamos realizar a geração aleatória de senha de pelo menos **16 dígitos**, senha seguras é um ponto chave para segurança da sua plataforma Wordpress.

[Gerador de senhas aleatória](#)

- Alterar a URL de login do Wordpress e não utilizar o wp-admin.

Alteração de URL normalmente é utilizada com a instalação de plugin, nossa recomendação é o plugin WPS hide login

[Plugin WPS Hide Login](#)

- Sempre manter a plataforma Wordpress atualizada.

Ambiente Wordpress está sempre em atualizações constantes, adicionando melhorias e correções de bugs, **mantenha sempre sua plataforma atualizada.**

Ao atualizar o Wordpress lembre-se sempre de validar plugins, os mesmos podem ficar incompatíveis com a atualização.

- Utilizar plugins e temas sempre atualizados e de fontes seguras.

Manter plugins e temas atualizados é um ponto crucial, maioria das invasões ocorre por falhas na segurança de plugins desatualizados.

- Manter sempre versões de PHP atualizadas.

Manter sempre a Versão PHP atualizada ela da mais segurança e uma estrutura mais robusta ao seu site.

Como o PHP é a estrutura do seu site, ao alterar a versão, plugins desatualizados ou temas antigos, podem acabar quebrando.

Alterar versão PHP

- Trocar senhas administrativas regularmente.

Sempre trocar suas senhas mantendo uma rotina e evitar que elas possam vazarem e comprometer seu projeto.

- Instalação de plugin limitador de tentativas de acesso ao painel admin.

Realizar instalação de plugin que limita as tentativas de acesso, prevenindo ataques de bots possam interferir na performance do site.

Recomendamos o plugin Limit Login Attempts Reloaded

Plugin Limit Login

- Utilização de firewall em seu website, além de scan regular ao menos uma vez na semana.

É necessário um firewall interno para realizar buscar de possíveis vulnerabilidades internas que seu site pode ter.

Recomendamos a utilização do firewall Wordfence

Plugin Wordfence

Além disso também recomendamos algumas boas praticas em relação ao cPanel.

- Sempre acessar a plataforma cPanel/WHM via https
- Não compartilhar a senha de acesso com outras pessoas
- Revisar periodicamente se existe ips liberados para realizar conexões ao banco de dados do servidor
- Excluir qualquer conteúdo que você tenha dúvida

Com estes passos você terá um ambiente mais seguro para a plataforma Wordpress.

Revision #9

Created 2024-02-09 16:36:53 UTC by Ewerton Henrique

Updated 2024-08-01 19:48:32 UTC by Gabriel Prado