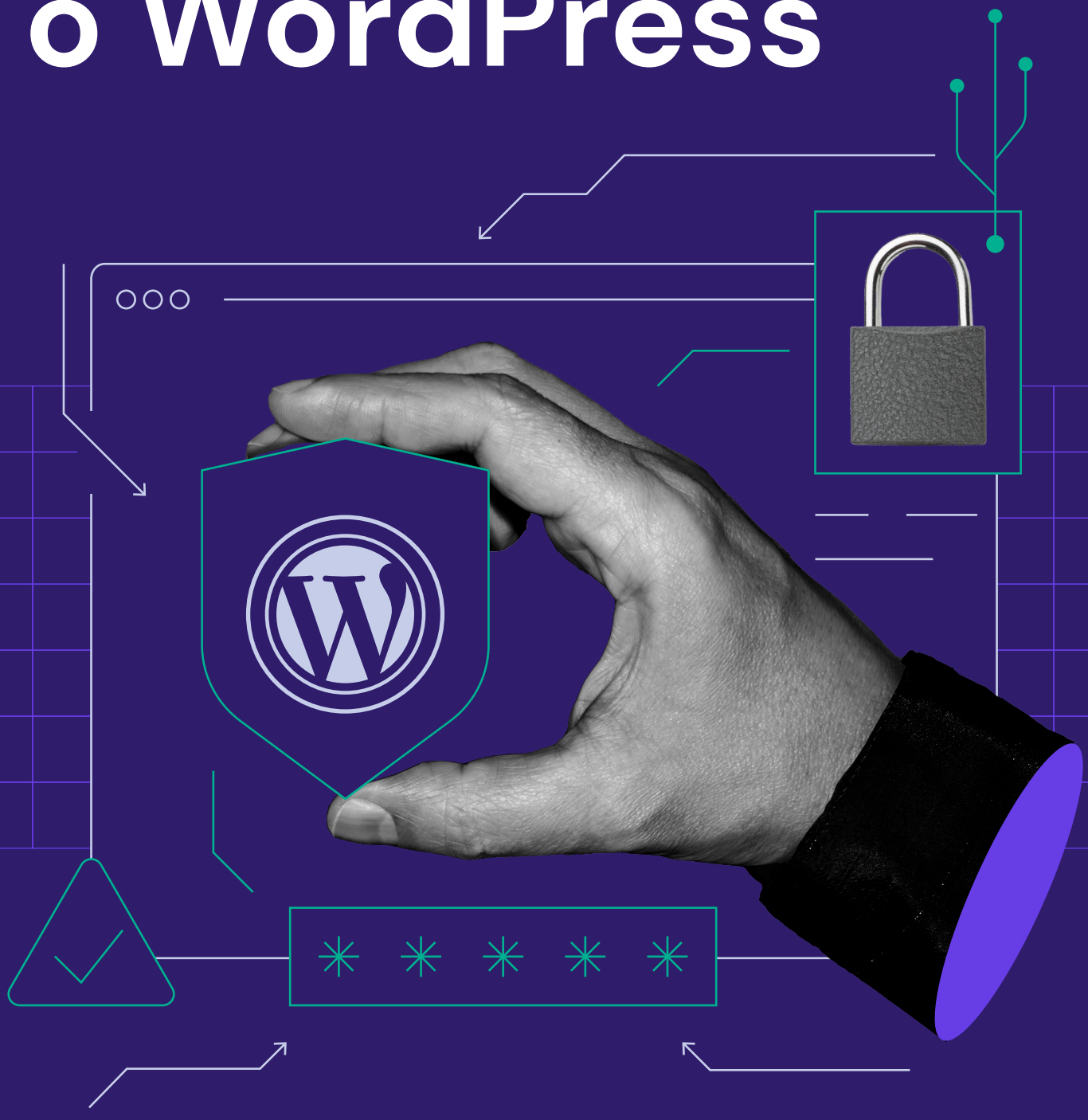
HOSTINGER

Três. Dois. Online

Checklist de Segurança para o WordPress



Checklist de Segurança para o WordPress

Implementar as medidas de segurança corretas é essencial para proteger o seu site de ataques cibernéticos. Essas práticas, que não requerem grande conhecimento técnico, podem aprimorar significativamente a segurança do WordPress.

Para te ajudar a reforçar a segurança do seu site, nós preparamos uma checklist com as melhores dicas e práticas de segurança para o WordPress.

Atualize o software do WordPress

Toda nova versão do WordPress traz melhorias de segurança, como correções de bugs e novos recursos. Ter o software sempre atualizado reduz o risco de brechas de segurança no seu site.

Atualize seus temas e plugins

Assim como o software do WordPress em si, os temas e plugins da plataforma também recebem atualizações para corrigir quaisquer vulnerabilidades. Atualize-os assim que novas versões estiverem disponíveis.

Use temas confiáveis

Escolha temas do repositório oficial do WordPress ou de desenvolvedores reconhecidos. Nunca use um tema pirateado, pois eles podem apresentar falhas de segurança.

Use credenciais de login seguras no WP-admin

Use uma senha forte e um nome de usuário personalizado para dificultar o acesso à sua conta e proteger o seu site de ataques de força bruta.

Ative a autenticação de dois fatores

Adicione uma camada extra de segurança ao processo de login. Os usuários precisam digitar um código temporário, transmitido via SMS ou algum app de autenticação, para entrar em suas contas.

Faça backups regulares do WordPress

Uma dica de remediação que pode te ajudar a recuperar os dados do seu site no caso de algum incidente, ciberataque ou problema no servidor.

Atenção aos malwares

Configure escaneamentos regulares para evitar danos relacionados a malware e, caso detecte algum agente malicioso, remova-o assim que possível.

Remova plugins e temas sem uso

Evite ataques de backdoor causados por plugins e temas obsoletos ou abandonados.

Instale um certificado SSL

Estabeleça um protocolo de transferência de dados seguro para proteger a troca de informações entre o seu site e os seus visitantes.

Configure uma whitelist e uma blacklist para a página de administração

Evite que a página de administração do WordPress seja acessada por endereços IP não autorizados.

Estabeleça um limite de tentativas de login

Use um plugin de segurança para bloquear o login de um determinado endereço IP após um número pré-determinado de tentativas.

Altere a URL da página de login do WordPress

Uma URL personalizada torna mais difícil para os invasores chegar até a página de acesso.

Faça o logout de usuários inativos automaticamente

Muitas vezes, usuários esquecem de fazer o logout dos painéis dos seus sites, deixando suas sessões abertas. Use um plugin de segurança para evitar que uma pessoa não-autorizada tenha acesso à página de administração ao usar o mesmo dispositivo.

Oculte a versão do WordPress

Deixar visível a versão do WordPress que você usa ajuda invasores a explorar vulnerabilidades, especialmente caso a sua versão seja mais antiga.

Monitore a atividade dos usuários

Preste atenção a qualquer atividade incomum que possa comprometer o seu site. Este passo é muito importante caso você tenha múltiplos usuários acessando o painel de administração do WordPress.

Desative o relatório de erros

O relatório de erros PHP mostra vulnerabilidades e outras informações sobre o back-end do seu site que podem ser usadas por invasores.

Escolha uma hospedagem web segura

O provedor de hospedagem deve garantir que todos os dados e arquivos do seu site estão armazenados com segurança em seus servidores. Escolha uma empresa com bons recursos de segurança, como monitores e atualizações.

Desative a edição de arquivos

Visitantes não autorizados podem explorar o editor de arquivos nativo do WordPress para acessar o seu site. Você pode desativar este recurso adicionando uma simples linha de código no arquivo **wp-config.php**:

```
define( 'DISALLOW_FILE_EDIT', true );
```

Restrinja acessos usando o .htaccess

Use o arquivo **.htaccess** para configurar permissões para executar comandos PHP em pastas específicas e proteger o arquivo **wp-config.php**.

Altere o prefixo padrão do banco de dados do WordPress

Se proteja de ataques via injeção de SQL alterando o prefixo padrão **wp_** do seu banco de dados.

Desative o XML-RPC

Este recurso tem vulnerabilidades que podem ser exploradas por invasores em ataques de força bruta ou DDoS.

Bloqueie hotlinks

Sites de terceiros que fazem hotlink para o seu conteúdo podem ocupar recursos do seu servidor e comprometer o desempenho do seu site.

Gerencie as permissões de arquivos

Use um cliente FTP ou o gerenciador de arquivos do seu provedor de hospedagem para definir quais usuários podem ler, gravar ou executar permissões na pasta principal e nos arquivos do WordPress.

Dicas Extras

- Crie uma senha forte de acesso ao WordPress. Use mais de 12 caracteres ou recorra a um gerador de senhas.
- Evite nomes de usuário genéricos, como **admin** ou **administrador**.
- Instale um plugin de segurança abrangente, como o Wordfence. Plugins como esse costumam oferecer recursos como autenticação de dois fatores, limite de tentativas de login e escaneamento de malware.
- Use o Patchstack para detectar vulnerabilidades em seus temas e plugins.
- Armazene os dados de backup do seu site em vários locais, como a memória do seu computador, um drive USB e um serviço de armazenamento na nuvem.