

PLANEJAMENTO DE REMOÇÃO DE MALWARE NO WORDPRESS

Este planejamento tem como objetivo guiar você nas melhores práticas para remoção de malware do seu site WordPress.

1 - Instale o ambiente localhost

Você deverá fazer a instalação do ambiente localhost pois todo trabalho de remoção de malware será feita aqui.

Não é uma boa prática fazer a remoção de malware no ambiente de produção pois se houver outro site infectado junto do site que estiver sendo desinfectado pode ocorrer de um passar o vírus para o outro e vice versa.

Logo precisamos isolar o site infectado, tratar ele isoladamente.

2 - Instale o WordPress virgem no localhost

Faça uma instalação em branco do WordPress em localhost para que possamos restaurar o seu site.

3 - Faça backup do banco de dados do seu site infectado

Vá até o PHPMYADMIN da sua hospedagem ou utilize o plugin Migrate DB para exportar APENAS o banco de dados do seu site infectado, vamos precisar do banco para voltar todos os dados do seu site.

4 - Instale todos os plugins originais

Após Instalar o WordPress, você deverá instalar todos os plugins novamente. NÃO FAÇA BACKUP DOS PLUGINS pois eles provavelmente estarão infectados, por tanto você deverá instalar cada um deles novamente, se todos forem plugins grátis basta ir no diretório de plugins do WordPress e instalar.

Se você estiver usando plugins premium, você deverá acessar o site onde comprou e baixar a ultima versão, se você não tiver acesso a última versão do plugin, deverá providencia-la ou mudar de plugin.

A única coisa que você deve ter em mente é: não compre plugin no mercado livre ou sites de plugins piratas. Não baixe plugins premium em sites de download grátis, pois eles podem esta com vírus.

5 - Instale o tema original

Baixe o seu tema original e instale ele no seu site em localhost. Não se preocupe se você não estiver vendo seus conteúdos. É assim mesmo.

6 - Faça backup da sua pasta de UPLOADS

A única pasta que você deverá resgatar do seu site infectado é a pasta de uploads, no entanto muito cuidado, ela pode ter arquivos infectados dentro dela.

A minha dica aqui é: Ao invés de extrair ela diretamente no site que você está limpando, crie uma nova instalação em branco só para você utilizar uns dos plugins explicados no módulo anterior para fazer uma varredura rápida. Essa varredura tem como objetivo encontrar alguma arquivo PHP com código malicioso. Se você encontrar o código malicioso basta remover e depois.

Se você tem certeza que a pasta de Uploads está segura livre de vírus, você poderá copiar ela para dentro da pasta wp-content da sua instalação.

7 - Importe o banco de dados

Agora é hora de você importar o banco de dados que você exportou no item 3, para isso acesse o localhost/phpmyadmin e localize a tabela do banco de dados do seu site que está trabalhando, selecione todas as tabelas que estão lá e clique em DROP.

O DROP serve para excluir as tabelas que o WordPress criou.

Depois de ter executado este comando, não haverá mais tabelas no seu banco de dados.

Agora você deverá clicar no menu importar no PHPMYADMIN e selecionar o banco de dados que você exportou.

Pronto, seu banco de dados está pronto.

Agora você será capaz de ver o seu site funcionando 100%.

8 - Procedimentos de Segurança

Agora é hora de você efetuar os procedimentos de segurança, para isso assista o nosso curso de Segurança WordPress para aprender as boas práticas de Segurança no WordPress.

9 - Clonar e restaurar

Depois de ter finalizado o procedimento 8 chegou a hora de voltar o site. Para isso recomendo que você utilize o plugin ALL IN ONE MIGRATION pois com ele você não precisará mexer com FTP.

Exporte o site do localhost e importe no ambiente de produção.

ATENÇÃO:

Se você tiver muitos sites na sua hospedagem, tenha certeza que os outros não estão infectados, uma vez que você importar um site limpo junto com outros sites com problemas, a probabilidade de você ter o seu site infectado novamente é grande.

Logo você precisa primeiro remover o vírus de todos os sites que estão na sua hospedagem.

Se você tiver 10 sites, você terá que fazer este procedimento 10x, isso irá garantir que tudo ocorrerá bem.

10 - Atualizações e cuidados

Para finalizar vou te dar algumas dicas finais.

1 - Cuide do seus sites, tenha uma rotina fixa de atualização dos mesmos. Veja o nosso Curso de Manage WP para aprender como criar rotinas automatizadas de atualização.

2 - Não instale Plugins e temas Piratas. Evite comprar temas e plugins no mercado livre, pois tudo lá é pirata.

3 - Faça backups regulares, veja nosso conteúdo especial sobre Backups WordPress.

4 - Instale um bom plugin de segurança. Nós indicamos o WordFence.

Ao seguir todos os passos descritos neste planejamento você não terá mais nenhum problema de Segurança.

Utilize este documento sempre que precisar realizar uma ação de Remoção de Malware.