

Boas praticas contra Spam

i Infelizmente o recebimento de Spams atualmente é um problema bastante incômodo. Na maioria das vezes você tem que excluir diversas mensagens Spam por dia, para que sua caixa de e-mail não lote e venha acarretar maiores transtornos. Existem alguns procedimentos que você pode realizar para ajudar a minimizar o recebimento de Spam. São eles:

1

Habilitar o Apache SpamAssassin

O SpamAssassin é uma ferramenta que atua na análise das mensagens que chegam para suas contas. Além de analisar o conteúdo, a ferramenta pode classificar ela como Spam e direcionar para o diretório spam ou excluir automaticamente. Para maiores detalhes, nossa equipe também elaborou um tutorial informando maiores detalhes sobre a ferramenta, basta pesquisar por **SpamAssassin**.

i **Observação:** Essa ferramenta utiliza um tipo de pontuação (score) que vai de 0 à 10, onde: score menor que cinco, a ferramenta torna-se mais agressiva, podendo até bloquear mensagens legítimas. Pontuação superior à cinco, o SpamAssassin torna-se mais conservador, nesse caso podendo deixar algumas mensagens Spam chegar na caixa de entrada das contas.

2

Boxtrapper

O BoxTrapper é uma ferramenta que também filtra os e-mails de sua caixa de entrada, assim como o SpamAssassin, porém ele possui etapas de verificação de e-mail. Caso algum endereço de e-mail que não esteja presente na Whitelist da ferramenta, envie e-mail para uma de suas contas, a ferramenta irá enviar uma mensagem de confirmação para o remetente, essa mensagem contém um link de confirmação, com isso a partir do momento que o remetente clicar nesse link, o endereço será adicionado na lista branca da ferramenta e as mensagens chegarão para suas contas.

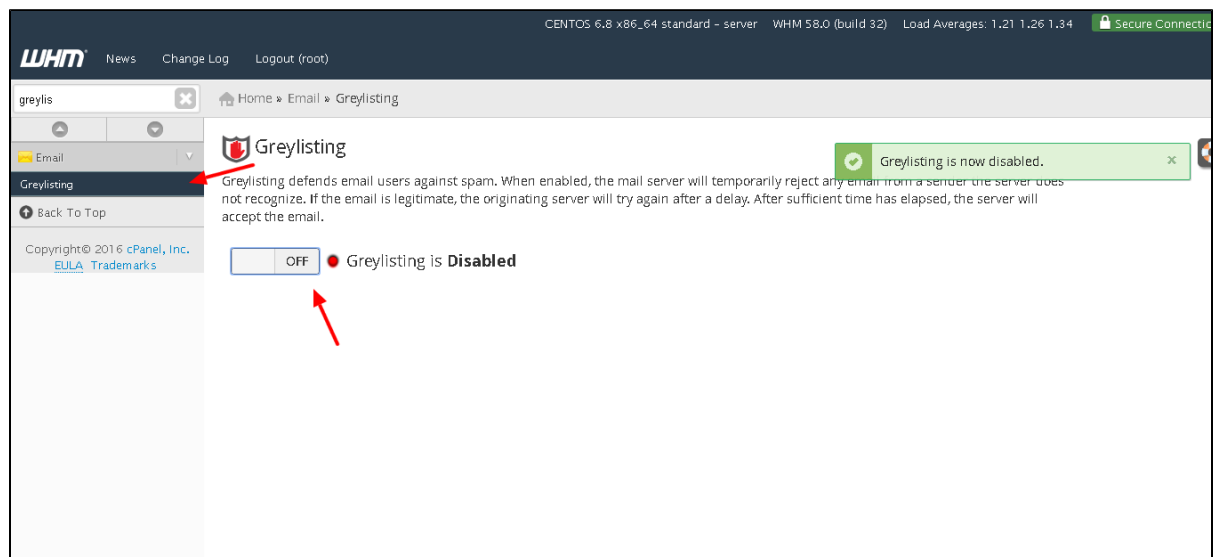
i **Observação:** A ferramenta em questão está disponível apenas para nossos planos corporativos (VPS e servidores dedicados que utilizam CentOS + cPanel).

3

Greylisting

A Greylisting protege os usuários de email contra spam. Quando habilitado, o servidor de email rejeita temporariamente qualquer email de destinatários não reconhecidos pelo servidor. Caso o email seja legítimo, o servidor de origem tentará novamente após um intervalo. Após decorrido tempo suficiente, o servidor aceitará o email.

Caso você deseje habilitar a ferramenta em questão, acesse o seu painel WHM e localize a opção "**Greylisting**", veja:



A greylisting também pode acabar por bloquear mensagens autênticas para seus domínios, mas é possível adicionar o ip do domínio remetente como host confiável, para assim normalizar o envio:

The screenshot shows the WHM interface for Greylisting configuration. The 'Trusted Hosts' tab is selected, and the 'New Trusted Hosts' section is highlighted with a red arrow. The table below shows existing hosts and their comments.

Host IP Address	Comment	Actions
17.0.0.0-17.255.255.255	Script populated entry for the 'apple' Mail Service	Edit Delete
25.216.136.98	Script populated entry for the 'yahoo' Mail Service	Edit Delete
26.216.136.98	Script populated entry for the 'yahoo' Mail Service	Edit Delete
32.112.138.98	Script populated entry for the 'yahoo' Mail Service	Edit Delete
34.112.138.98	Script populated entry for the 'yahoo' Mail Service	Edit Delete
34.118.196.66	Script populated entry for the 'yahoo' Mail Service	Edit Delete

Quando habilitada, a Greylisting irá atuar em todas as contas cPanel do servidor, porém, caso você deseje é possível desativar a ferramenta de forma individualmente, por conta cPanel.



Observação: A ferramenta Greylisting está disponível apenas para os nossos planos corporativos: Servidores dedicados e VPS que utilizam CentOS + cPanel.

Este artigo te ajudou?



Your Rating:



Results:



1 rates

Ainda precisa de ajuda?

ABRIR UM CHAMADO