



SISTEMA DE PROTEÇÃO DE FRAUDES DE E-MAILS/ BEC

MailInspector 5 - Fevereiro de 2019

Sumário

05. O que é Fraude de E-mail?

05. Dicas para identificar um e-mail falso

- 05. O remetente do e-mail é desconhecido ou estranho
- 05. O e-mail promete ganhos fáceis e rápidos, sem esforço
- 05. O e-mail pede seus dados bancários ou cadastrais
- 05. O e-mail tem um boleto, fatura ou nota fiscal anexa
- 05. As informações do e-mail são desconhecidas ou têm erros de português
- 05. Senso de urgência
- 05. Erros de ortografia
- 05. Os e-mails do remetente e resposta ao remetente são diferentes
- 05. Oferta incompatível

05. Alguns tipos de e-mails falsos

- 05. Adulteração do campo "Envelope From"
- 05. Adulteração do campo "Mail From"
- 05. Uso de domínio similar
- 05. Uso de contas de email "roubadas"

05. Dicas de Prevenção a Fraudes de E-mail

Sumário

05. Proteção a Fraude de Email no MailInspector

- 05. Verificação de SPF
- 05. Verificação de DKIM
- 05. Verificação de DMARC
- 05. Verificação de SenderID
- 05. Verificação de domínio recentemente criado
- 05. Verificação de domínio similar (Cousin domain attack / Look-A-Like Attack)
 - 05. 1. Bloqueando a Nível de Conexão
 - 05. 2. Bloqueando a Nível de SPAM
 - 05. 3. Quarentena Customizada com DNSTwister
- 05. Validação da lista de emails externos de confiança
- 05. Proteção a fraude de email pela análise do Display Name
- 05. Sistema da Proteção a Spoofing de Domínio
- 05. Sistema de Proteção a Spoofing de Domínio de Saída
- 05. Sistema de Controle de novos Domínios
- 05. Sistema de comparação de domínios diferentes no cabeçalho
- 05. Sistema de detecção de uso de Free Mail
- 05. Proteção e prevenção a invasão ao email interno

05. Considerações Finais

O que é Fraude de Email?

E-mail spoofing é a falsificação de um cabeçalho de e-mail para que a mensagem aparente proceder de alguém ou algum lugar diferente da fonte real. Os distribuidores de spam frequentemente utilizam spoofing como tentativa de conseguir destinatários que abram e respondam às suas solicitações.

Mesmo se você não fornecer nenhuma informação, o fato de clicar em links com spoofs pode permitir que os ladrões acessem o seu computador, gravem suas teclas e capturem as suas senhas.



Dicas para identificar um email falso

O remetente do e-mail é desconhecido ou estranho

Mesmo que o assunto pareça importante, antes de abrir, pare e leia o endereço de e-mail do remetente. Se for desconhecido ou o nome parecer estranho, com letras e números misturados, não caia na tentação de abrir. Além de golpe, pode ser também uma forma de infectar seu computador ou celular com vírus.

O e-mail promete ganhos fáceis e rápidos, sem esforço

Um dito popular ensina: ***“quando a esmola é grande, o santo desconfia”***. Fique de olhos bem abertos com promessas de ganhos milagrosos, brindes, ofertas imperdíveis e oportunidades únicas.

Desconfie, principalmente, se o endereço do remetente não tiver o nome da empresa (por exemplo: www.serasaconsumidor.com.br) e quando tiver o nome da empresa tome cuidado com grafias muito parecidas, mas não oficiais. As promoções e ofertas idôneas geralmente vêm identificadas. Se não for o caso, há grandes chances de ser uma fraude ou golpe.

O e-mail pede seus dados bancários ou cadastrais

O remetente é seu conhecido e o assunto diz: “Estou tentando depositar dinheiro na sua conta, mas não consigo”. Confiando que se trata de seu amigo ou parente, você abre a mensagem e informa seus dados bancários, nome completo e CPF.

Acredite: **Se você não está esperando receber dinheiro dessa pessoa, o e-mail é falso**. Jamais passe qualquer informação sem confirmar, por telefone, com o remetente. Se alguém quiser realmente entrar em contato com você, irá procurá-lo por outros canais ou pessoalmente.



O e-mail tem um boleto, fatura ou nota fiscal anexa

Se você fizer uma compra pela internet, provavelmente irá imprimir o boleto diretamente do site. Se você tiver contas atrasadas, terá que entrar em contato com o credor para negociar a dívida. Não faz sentido receber um boleto ou fatura que você não pediu para pagar por compras ou contas atrasadas. Se isso acontecer com você, desconfie. Não é tão difícil para fraudadores criar boletos falsos e disparar na internet, fazendo-se passar por bancos, empresas de varejo e outras instituições. A Serasa não envia e-mails com boletos ou cobranças.

Todo cuidado é pouco!

As informações do e-mail são desconstruídas ou têm erros de português

Cada vez mais os fraudadores estão se especializando, mas há situações em que os erros são tão grosseiros que basta uma lida com um pouco mais de atenção para perceber que se trata de um e-mail falso. Observe se a mensagem contém palavras escritas incorretamente e dados conflitantes de mais de uma instituição no mesmo e-mail.

Exemplo: O remetente é o Itaú, mas o boleto é do Bradesco.

Senso de urgência

E-mails informando que o seu pedido será cancelado ou que a oferta irá expirar se você não responder.

Erros de ortografia

Pode conter erros de ortografia evidentes que ajudam os e-mails falsos a evitar filtros de spam.

Os e-mails do remetente e resposta ao remetente são diferentes

O e-mail pode vir de "BigCompany.com", mas a resposta é para "SomeOtherCompany.com".

Oferta incompatível

O produto ou serviço oferecido não está relacionado com a principal competência da empresa e/ou apresenta uma oferta tão boa que é quase impossível de resistir a compra.



Alguns tipos de E-mails falsos

Adulteração do campo “Envelope From”

É muito utilizado para “validar” o domínio do email, por exemplo: O fraudador está mandando email do gmail, mas quer disfarçar como se fosse enviado do Banco Bradesco, então ele além de forjar o campo “Mail From”, ele também forja o “Envelope From”, para dar a impressão real de que o email veio do Banco Bradesco.

Adulteração do campo “Mail From”

Este é o campo que aparece para os usuários finais, isto é, é o que aparece no leitor do Outlook, Thunderbird, etc... Com a alteração deste campo, o usuário final acha que está recebendo um email válido.



Esse tipo de adulteração é o mais comum de acontecer, o email é enviado de um servidor ou máquina contaminada e finge ser outro remetente, por exemplo uma máquina contaminada na China mandando email fingindo ser o Banco Bradesco. No exemplo acima, ele está fingindo ser o próprio usuário que mandou email para ele mesmo.

Uso de domínio similar

Muitos spammers/golpistas mandam email com domínio parecido, enganando o leitor do email.



Repare que o domínio é semelhante, mas não é o mesmo: acme.com, diferente de acmes.com.

Uso de contas de email “roubadas”

Este é o mais difícil de ser detectado, uma vez que por mais que seja feita uma inspeção do cabeçalho do email, não terá nenhuma evidência de fraude. Por sorte, esta também é a forma mais difícil do golpista conseguir executar. É necessário que o golpista tenha controle sobre a caixa de e-mail de alguém.

Geralmente o golpista começa mandando email de phishing, para coletar os dados da pessoa, muitas vezes são aqueles e-mails dizendo que a conta do email venceu e que será encerrado o email e para evitar isso, a vítima terá que atualizar os dados da sua conta de email.

Uma vez que a vítima mande todas as informações, o golpista consegue acessar a caixa de email e começar a efetuar ataques a outras pessoas, se passando pela vítima.

Dicas de Prevenção a Fraudes de E-mail

- Tomadores de decisão devem pensar em acrescentar o processo de verificação em duas etapas quando se trata de movimentar as finanças ou recursos da empresa, tais como canais de comunicação alternativos ou assinaturas digitais;
- Todos os funcionários (não apenas os gerentes de TI) precisam estar familiarizados com esquemas usados para enviar ameaças de Fraudes de Email;
- Verifique cuidadosamente os emails, antes de enviar pagamentos de faturas e apague imediatamente mensagens de spam.
- O FBI também recomenda usar a função “Encaminhar” em vez de “Responder” para que você possa digitar o endereço de email de seu contato e garantir que o endereço correto está sendo usado.
- Os gerentes de TI podem instalar soluções de segurança para bloquear malware que muitas vezes são utilizados junto a um email falso antes que eles cheguem.



Proteção a Fraude de Email no MailInspector

A proteção a fraude de emails / BEC (Business Email Compromise) no MailInspector passa por múltiplas camadas específicas para esse tipo de ataque:

- *Verificação de SPF;*
- *Verificação de DKIM;*
- *Verificação de DMARC;*
- *Verificação de SenderID;*
- *Verificação de domínio recentemente criado;*
- *Verificação de domínio similar;*
- *Validação da lista de emails externos de confiança;*
- *Proteção a fraude de email pela análise do Display Name;*
- *Sistema de Proteção a Spoofing de Domínio na ENTRADA;*
- *Sistema de Proteção a Spoofing de Domínio na SAÍDA;*

Verificação de SPF

SPF é uma abreviação de *Sender Policy Framework* que é um sistema que **evita que outros servidores enviem e-mails não autorizados em nome de seu domínio.**

O SPF é configurado na tabela de DNS de seu domínio com uma entrada TXT, aonde é informado os servidores que tem autorização de enviar e-mails utilizando o seu domínio.

Quando um e-mail é recebido, o servidor do destinatário verifica se o servidor que está enviando tem realmente autorização de uso do domínio. Caso o servidor não tenha, ou o SPF seja inválido, o e-mail é pontuado/rejeitado.

HSC MailInspector pode ser configurado para identificar a autenticidade de mensagens através da verificação do SPF, o protocolo SPF permite:

- **ao administrador de um domínio:** definir e publicar uma política SPF, onde são designados os endereços das máquinas autorizadas a enviar mensagens em nome deste domínio;
- **ao administrador do HSC MailInspector:** estabelecer critérios de pontuação de mensagens em função da checagem das políticas SPF publicadas para cada domínio.



O processo de publicação de uma política SPF é independente da implantação de checagem de SPF por parte do HSC MailInspector, estes podem ou não ser feitos em conjunto.

No MailInspector o administrador pode definir a pontuação que será atribuída a mensagens verificadas pelo SPF:

- **Mensagens Válidas:** Mensagens consideradas válidas, quando o endereço IP do servidor de origem da mensagem pertence ao registro SPF configurado para o domínio.
- **Mensagens Classificadas como FAIL:** Mensagens consideradas inválidas, quando o endereço IP do servidor de origem da mensagem não pertence ao registro SPF configurado para o domínio.
- **Mensagens Classificadas como SOFT FAIL:** Mensagens consideradas inválidas, quando o endereço IP do servidor de origem da mensagem informado SMTP não pertence ao registro SPF configurado para o domínio, porém o registro DNS foi configurado como final “?all”.
- **Mensagens Classificadas como Neutral:** O proprietário do domínio declarou explicitamente que não pode ou não deseja afirmar se o endereço IP está autorizado ou não.

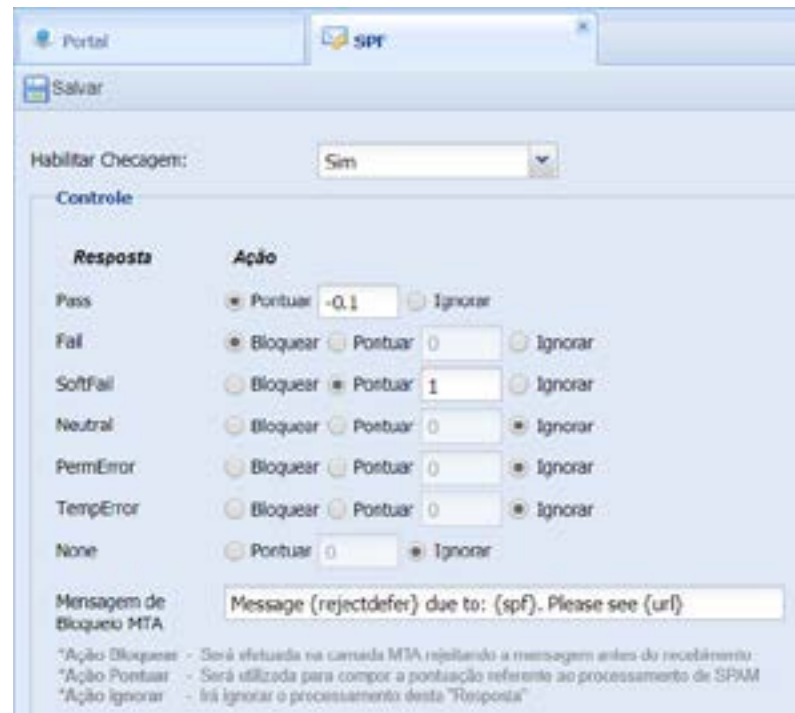
- **Mensagens Classificadas como PERMERROR:** Ocorreu um erro permanente (por exemplo, registro SPF mal formatado).
- **Mensagens Classificadas como PERMERROR:** Ocorreu um erro transitório.
- **Mensagens Classificadas como PERMERROR:** O resultado “NONE” significa que nenhum registro foi publicado pelo domínio ou que o domínio não pôde ser determinado.

<i>Opção</i>	<i>Ação que o administrador pode tomar</i>
Pass	Pontuar e Ignorar
Fail	Bloquear, Pontuar e Ignorar
SoftFail	Bloquear, Pontuar e Ignorar
Neutral	Bloquear, Pontuar e Ignorar
PermError	Bloquear, Pontuar e Ignorar
TemError	Bloquear, Pontuar e Ignorar
None	Pontuar e Ignorar

As ações tomadas são referentes a cada tipo de detecção do SPF.



No caso do administrador do sistema optar por bloquear, é possível criar uma mensagem de bloqueio customizado.

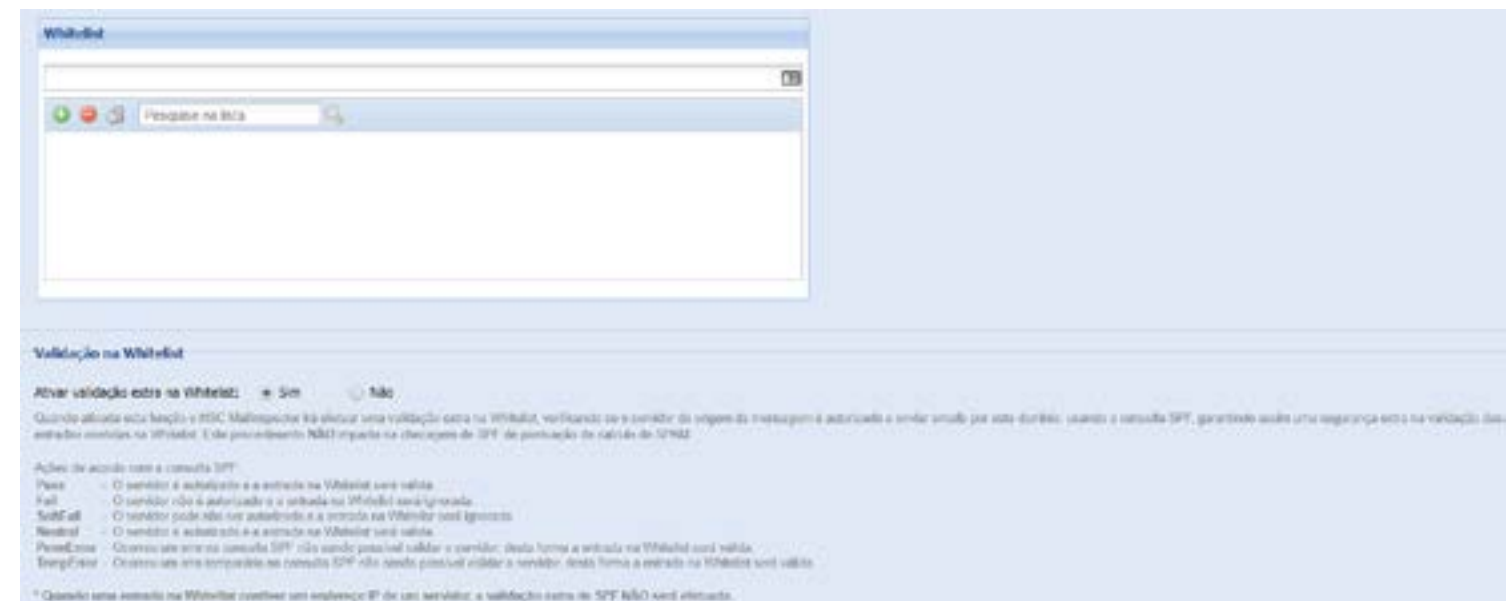


Verificação SPF no MailInspector

Ainda é possível ao administrador customizar uma ação específica baseado em uma resposta de SPF em relação a um remetente/destinatário:

Configurações > Filtros de SPAM > Controle Avançado

O MailInspector também permite inserir Whitelists em relação a SPF, dessa forma os domínios que estiverem na whitelist, não serão pontuados, nem verificados quanto a SPF.



Whitelist

Verificação de DKIM

DKIM (**Domain Key Identified Mail**) é uma especificação do **IETF RFC 6376** que define um mecanismo para autenticação de e-mail baseado em criptografia de chaves públicas.

Através do uso do DKIM, **uma organização assina digitalmente as mensagens que envia, permitindo ao receptor confirmar a autenticidade da mensagem.**

Para verificar a assinatura digital, a chave pública é obtida por meio de consulta ao DNS do domínio do assinante.

Ao contrário do SPF, que verifica somente o envelope, o DKIM verifica o cabeçalho da mensagem. Esta técnica acarreta um custo computacional adicional por mensagem, tanto para o MTA remetente quanto para o receptor.

Estas são as principais vantagens dessa tecnologia:

- O destinatário poderá **confiar na origem do email** e no conteúdo da mensagem se a análise do DKIM for concluída;
- Aumento na **eficiência das listas negras e brancas** de domínios;
- **Controle antispam mais eficaz**, além de opções de ações automatizadas que podem ser executadas nos resultados da análise do DKIM;
- Agora, os proprietários de **domínios abusivos podem ser rastreados**;
- O DKIM é inteiramente **compatível com todos os servidores baseados em SMTP e DNS**;

Ao ativar a verificação de DKIM, o administrador pode customizar a pontuação a ser contabilizada como email impostor:

Habilitar Verificação das Assinaturas:	Sim
Pontuação para Mensagens Inválidas - Assinatura não Confere:	1
Pontuação para Mensagens Assinadas - Assinatura da Mensagem Confere:	-0.01
Pontuação para Mensagens Assinadas e com Checksum MD5 verificado:	-0.2

Pontuação na verificação de DKIM

No MailInspector o administrador pode indicar a pontuação para as classificações em relação DKIM:

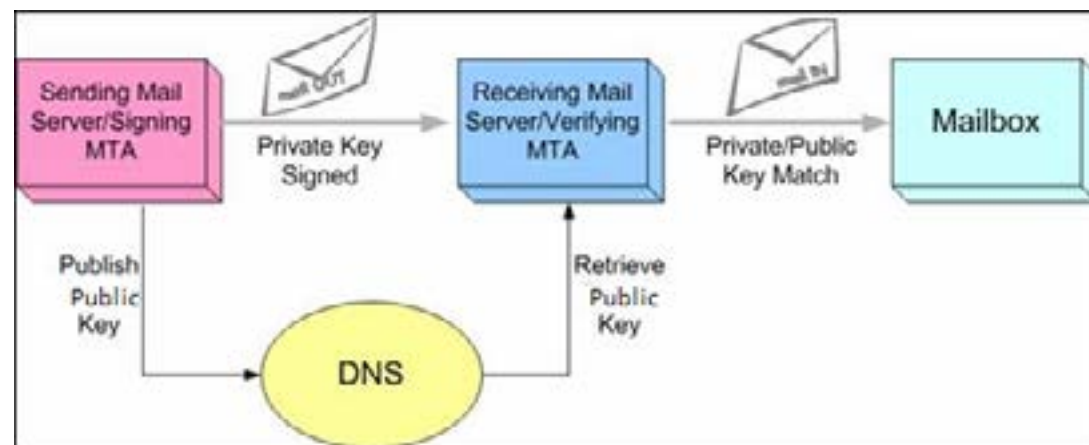
- **Pontuação para Mensagens Inválidas - Assinatura não Confere:**
Valor da pontuação atribuída as mensagens consideradas inválidas.

- **Pontuação para Mensagens Assinadas - Assinatura da Mensagem Confere:**
Valor da pontuação atribuída as mensagens que foram assinadas com DKIM.

- **Pontuação para Mensagens Assinadas e com Checksum MD5 verificado:**
Valor da pontuação atribuída as mensagens consideradas inválidas.

Os pontos verificados são:

- Quando DKIM está com assinatura inválida;
- Quando a assinatura do DKIM está em conformidade;
- Quando a assinatura está em conformidade e verificação do MD5 também deu conformidade;



1. Email sai do servidor com a chave privada nela;
2. Ao "bater" no DESTINO, é verificado a compatibilidade das chaves (que está no email, com o do arquivo TXT do registro DNS, que foi anteriormente inserido);
3. Ao casar as duas chaves de criptografia, comprova-se de que o email é autêntico.

Obs: Também é possível incluir emails/domínios em uma Whitelist para ignorar completamente o DKIM.



O MailInspector também pode "gerar" a chave utilizada pelo DKIM. Se o administrador optar por efetuar a saída de emails passando pelo MailInspector, o sistema de proteção a emails, assinará digitalmente (se o administrador optar por assinar os emails de saída com DKIM pelo MailInspector) os emails. A chave pública poderá ser baixada e implementada no DNS da empresa.

Verificação de DMARC

DMARC (*Domain-based Message Authentication, Reporting, and Conformance*) é uma especificação do **IETF RFC 7489**.

Este novo padrão baseia-se nos protocolos SPF e DKIM adicionando ligação ao nome de domínio do autor ("De:"), políticas publicadas para tratamento de falhas de autenticação e relatórios de receptores para remetentes, para melhorar e monitorar a proteção do domínio de email fraudulento.

O DMARC é um mecanismo de autenticação de mensagens eletrônicas que permite ao remetente garantir aos seus destinatários que as mensagens que irão receber partiram da organização de origem (valida as mensagens). Em outras palavras, **DMARC é um conjunto de regras que permite aos remetentes e destinatários trabalharem em conjunto detectando e tratando os e-mails fraudulentos**. O DMARC é basicamente um novo padrão que visa unificar as validações atuais.



Ação

Ação para casos de falha do DMARC: Bloquear Ignorar Pontuar

A grande diferença entre o DMARC e outros sistemas, é que com o DMARC será possível o administrador do domínio receber alertas (reports) de servidores que estão tentando mandar email usando o seu domínio, dessa forma, o aviso é preventivo, ou seja, o administrador poderá tomar ação de proteção "antes" de algum usuário cair em golpes.

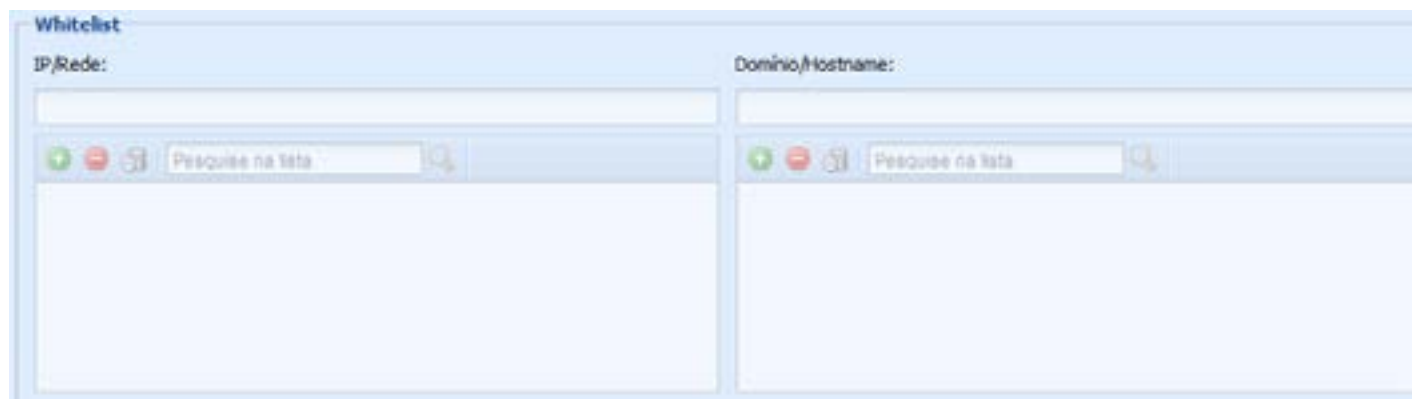
No MailInspector o administrador pode tomar as seguintes ações em relação ao DMARC:

- **Bloquear** emails sem DMARC ou com erros no DMARC;
- **Ignorar** (deixar passar direto);
- **Pontuar** (e definir a pontuação) os emails sem DMARC ou com erros no DMARC;

É possível criar whitelist para o módulo DMARC, ao qual não serão verificados os registros indicados quanto a esse protocolo de segurança.

Aceita-se as entradas em:

- *Verificação de SPF;*
- *Verificação de DKIM;*
- *Verificação de DMARC;*
- *Verificação de SenderID;*
- *Verificação de domínio recentemente criado;*



Verificação de SenderID

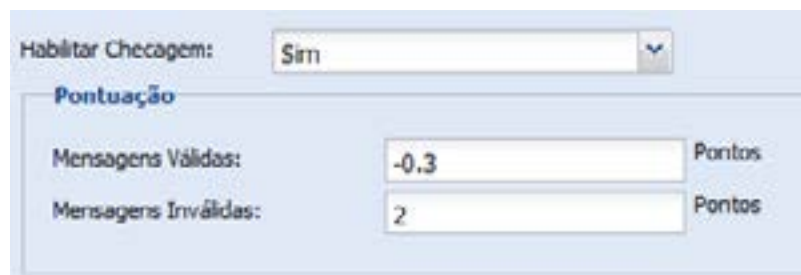
O Sender ID (definido na RFC 4406) é um protocolo da Microsoft derivado do SPF (de sintaxe idêntica), que valida o campo do endereço da mensagem no cabeçalho, de acordo com RFC 2822. A validação segue um algoritmo chamado PRA (Purported Responsible Address, RFC 4407).

O algoritmo certifica se o campo do cabeçalho com o endereço do e-mail é responsável por enviar a mensagem. Como ele deriva do SPF, pode também validar o MAIL FROM, mas ele irá definir uma nova identidade, PRA e novos campos de política de envio, substituindo o MAIL FROM (MFROM por Sender ID), PRA, ou os dois.

O HSC MailInspector pode ser configurado para identificar a autenticidade de mensagens através da verificação do protocolo Sender ID, porém, este protocolo é menos utilizado, este mecanismo permite:

- **ao administrador de um domínio:** definir e publicar uma política Sender ID, onde são designados os endereços das máquinas autorizadas a enviar mensagens em nome deste domínio; e
- **ao administrador do HSC MailInspector:** estabelecer critérios de pontuação de mensagens em função da checagem das políticas Sender ID publicadas para cada domínio. O processo de publicação de uma política Sender ID é independente da implantação de checagem de Sender ID por parte do HSC MailInspector, estes podem ou não ser feitos em conjunto.

No MailInspector no módulo de SenderID o administrador pode definir a pontuação das mensagens válidas e das mensagens inválidas.



Habilitar Checagem:	Sim
Pontuação	
Mensagens Válidas:	-0.3 Pontos
Mensagens Inválidas:	2 Pontos

Verificação de domínio recentemente criado

Sabendo que uma das técnicas de ataque é comprar um domínio novo similar ao utilizado pelo alvo (ex: Comprar o domínio santandeer.com.br para ficar similar ao santander.com.br) e mandar email pelo domínio recém adquirido.

Sabendo que o domínio santandeer.com.br logo será “queimado”, o hacker logo após a compra dele, já dispara uma série de emails na esperança de que o usuário não perceba a diferença do domínio de origem em relação ao domínio original.

O administrador do MailInspector pode selecionar a opção do que acontecerá em relação aos emails com domínios recém adquiridos:

- **Bloquear;**
- **Ignorar;**
- **Pontuar.**



Controle de novos Domínios	
Domínios Recentes / Suspeitos:	<input type="radio"/> Bloquear <input type="radio"/> Ignorar <input checked="" type="radio"/> Pontuar <input type="text" value="1"/>
Domínios de Remetentes que foram registrados a menos de <input type="text" value="12"/> mese(s)	

Verificação de domínio similar (Cousin domain attack / Look-A-Like Attack)

Outra técnica de ataques utilizados por hacker é compra de domínios “parecidos” em relação ao domínio alvo.

O MailInspector consegue verificar se a origem do email é similar com o domínio aplicado no remetente e ainda compara com eventual problema de SPF em relação ao domínio.

Além da proteção já mencionada, podemos utilizar o sistema de DNSTwister para verificar domínios parecidos com o domínio original.

O cousin domain ou domínios primos, também chamado de lookalike domain (também conhecidos como domínios similares), é um domínio DNS (sistema de nome de domínio) semelhante a outro nome quando processado por um agente de usuário de email (MUA).

Por exemplo, **americanas1.com** ou **americamas.com** são domínios primo de **americanas.com**.

Outros exemplos incluem erros de ortografia de um domínio, como **americamas.com** e **americanas.com**

TOP Violações de SPF por Domínio

Do Domínio	SPF HELO SOFTFAIL	SPF FAIL	SPF SOFTFAIL	TOTAL
sestsenat.org.br	-	89	-	89
news-voeazul.com.br	-	23	-	23
ofispf.oficialfarma.com.br	-	16	-	16
ecampaigns.dell.com	-	10	-	10
supernotadez.com.br	-	10	-	10
novidademaraviha.com.br	-	8	-	8
email.rdstation.com.br	-	7	-	7
abrlink.abradirs.com.br	-	6	-	6
amazonses.com	-	5	-	5
minder-educ7.com.br	-	5	-	5



Os domínios primos geralmente são criados como uma ferramenta de phishing para falsificar sua marca e seu nome de domínio.

No MLI existem 3 (três) formas de bloqueio a domínios similares:

1) Bloqueio a nível de conexão;

2) Bloqueio a nível de pontuação de SPAM;

3) Bloqueio a nível de quarentena customizada;

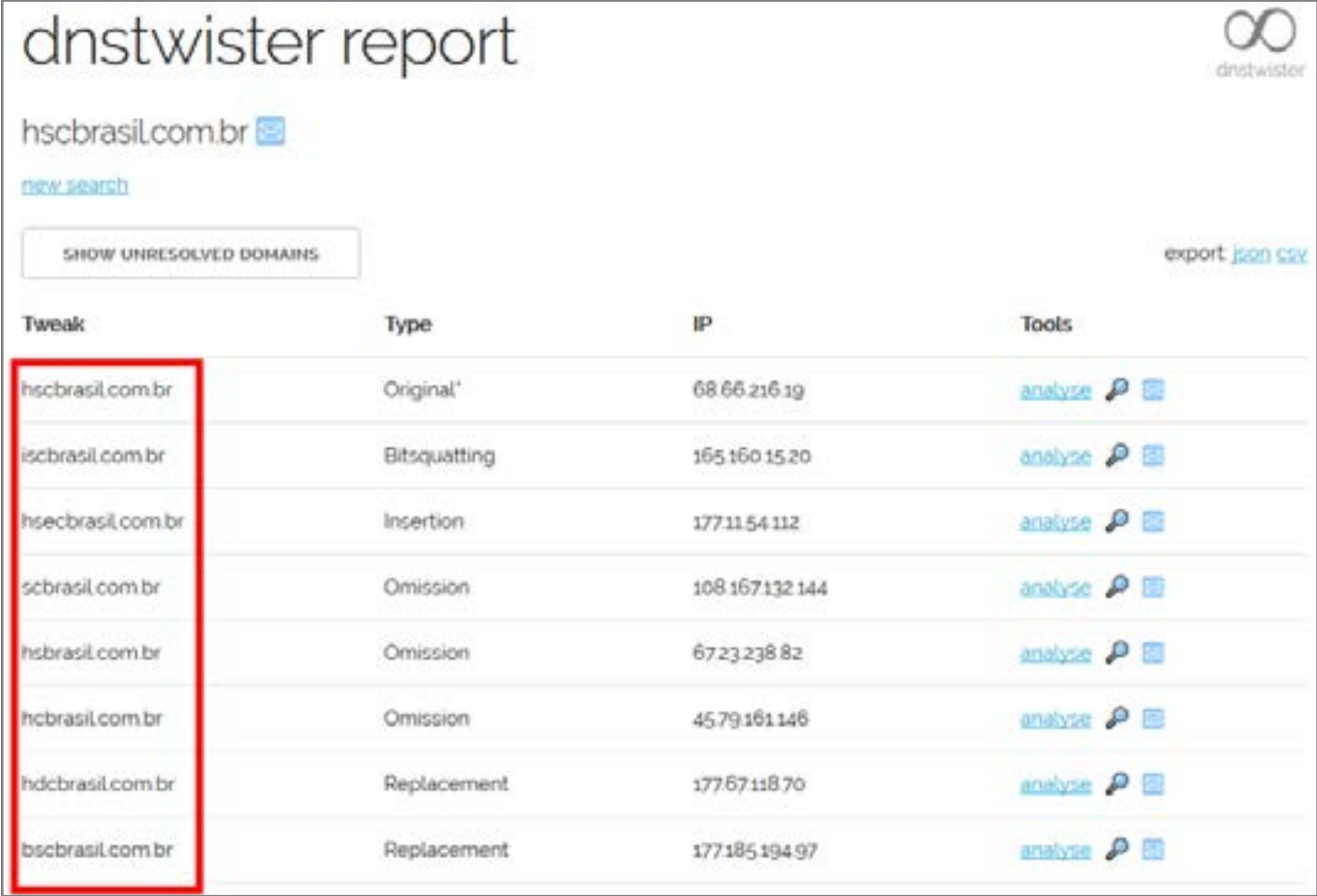
Em qualquer uma das formas de bloqueio, primeiramente o administrador deverá acessar o DNSTwister e verificar as variações do domínio já registradas.

















No exemplo à direita, vamos considerar o domínio HSCBRASIL.COM.BR

<https://dnstwister.report/>

Então temos os domínios variantes:

icsbrasil.com.br hsebrasil.com.br scbrasil.com.br **hscbrasil.com.br**
hdcbrasil.com.br bscbrasil.com.br



Tweak	Type	IP	Tools
hscbrasil.com.br	Original	68.66.216.19	analyse  
iscbrasil.com.br	Bitsquatting	165.160.15.20	analyse  
hsecbrasil.com.br	Insertion	177.11.54.112	analyse  
scbrasil.com.br	Omission	108.167.132.144	analyse  
hsbrasil.com.br	Omission	67.23.238.82	analyse  
hcbrasil.com.br	Omission	45.79.161.146	analyse  
hdcbrasil.com.br	Replacement	177.67.118.70	analyse  
bscbrasil.com.br	Replacement	177.185.194.97	analyse  

Verificação de domínio similar através do sistema DNSTwister

É possível também verificar os domínios que ainda não foram registrados (possíveis domínios similares), para isso, basta clicar no botão

SHOW UNRESOLVED DOMAINS.

Com as variações dos domínios em mãos, é possível bloquear os domínios similares por alguns métodos:

1. Bloqueando a Nível de Conexão

Em *Configurações > Cadastros > Configurações do MTA > Filtragem*

Inclua toda a lista apresentada no DNSTwister, como exemplo a seguir:



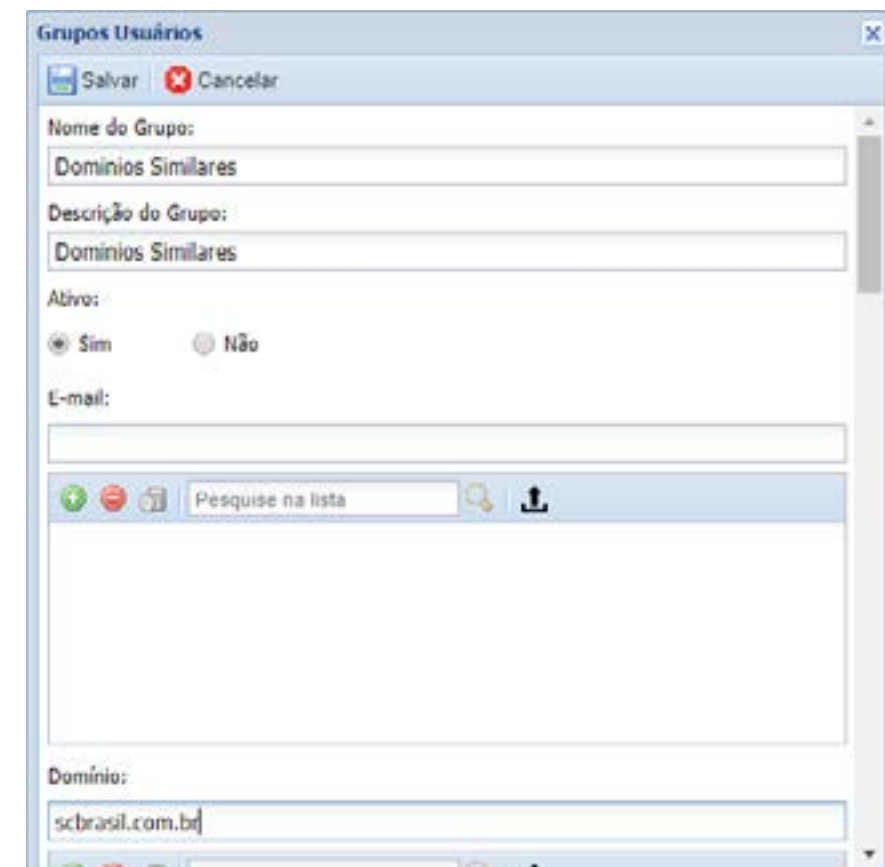
Repita o processo acima até finalizar com todos os domínios similares.

Clique em **Salvar** > Clique em **Aplicar Configurações**.

2. Bloqueando a Nível de SPAM

Em *Configurações > Cadastros > Grupos de Usuários*

Crie um Grupo de usuários (domínios), com toda a lista dos domínios similares indicados pelo DNSTwister.



Clique em **Salvar**.

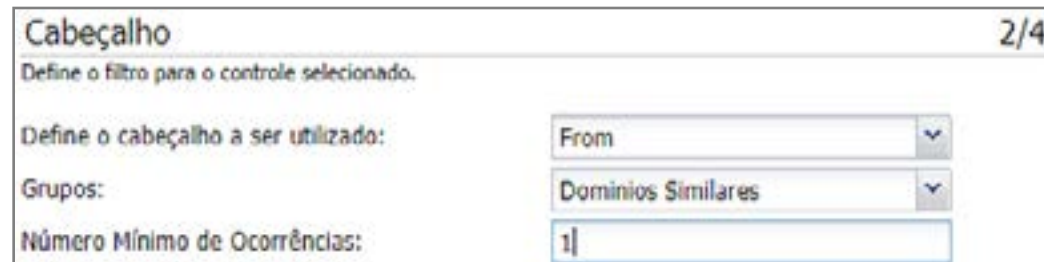
Depois vá em: *Configurações > Filtros de SPAM > Controle Avançado*

Clique em **Adicionar**

Regras do Controle Avançado

Seleção de Controle: **Cabeçalho** > Clique em **Avançar**

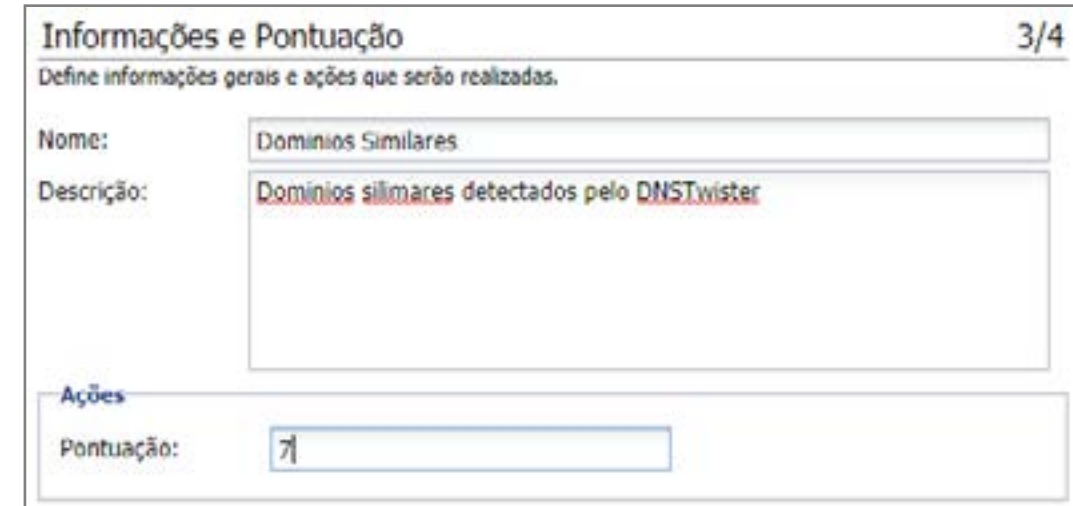
- Defina o Cabeçalho a Ser Utilizado: **From**
- Grupos: **Domínios Similares**
- Número Mínimo de Ocorrências: **1**



Clique em **Avançar**

Informações e Pontuação

- Nome: **Domínios Similares**
- Descrição: **Domínios similares detectados pelo DNSTwister**
- Pontuação: **7**



Clique em **Avançar** e conclua o processo.



Clique em **Salvar** > Clique **Aplicar Configurações**



3. Quarentena Customizada com DNSTwister

Em **Configurações > Quarentena > Customizada**

Clique em **Adicionar**

- Nome: **Domínio Similar**
- Tamanho: **0**
- Tempo de Armazenamento de Mensagens: **30**
- Tempo de Armazenamento de Logs: **90**

Nome:	<input type="text" value="Domínio Similar"/>
Tamanho (""): <small>* Para tamanho ilimitado deixe o campo em branco (0 GB).</small>	<input type="text" value="0"/> GB
Tempo de Armazenamento das Mensagens:	<input type="text" value="30"/> Dias
Tempo de Armazenamento dos Logs:	<input type="text" value="90"/> Dias
Permissões	
Administradores:	<input checked="" type="checkbox"/>
Usuários locais:	<input checked="" type="checkbox"/>
Usuários remotos (LDAP):	<input checked="" type="checkbox"/>

Clique em **Salvar**

Em **Configurações > E-mail Compliance > Regras**

Clique em **Adicionar**

- Seleção de Controle: **Cabeçalho**
- Defina o cabeçalho a ser utilizado: **From**
- Grupos: **Domínios Similares**
- Número Mínimo de Ocorrências: **1**
- Nome: **Domínios Similares**
- Descrição: **Domínios Similares**
- Tipo: **Quarentena**
- Armazenar na Quarentena: **Domínio Similar**

Conclusão do Processo	4/4
Salvar a configuração da regra de compliance.	
Nome: Domínios similares Descrição: Domínios similares	
Propriedades	
Controle: Cabeçalho Define o cabeçalho a ser utilizado: From Grupo: Domínio Similar Número Mínimo de Ocorrências: 1	
Ações	

Clique em **Salvar > Clique Aplicar Configurações**



Validação da lista de emails externos de confiança

O que é Sistema de Email de Confiança?

São aqueles emails considerados os mais importantes da sua empresa, geralmente sendo dos diretores executivos (CEO's), diretores financeiros (CFO's), etc.

Qual a finalidade dessa classificação?

Ter listado os emails EXTERNOS/PARTICULARES dos diretores e melhorar a classificação destes em relação aos outros emails, por exemplo:

O diretor para uso particular usa um determinado email do GMAIL. Para reduzir a chance de ser barrado é possível considerar este email como de confiança.

Como funciona a proteção sobre emails de confiança?

No MailInspector é possível criar regras específicas para grupos cadastrados no sistema. A boa prática recomenda que criemos uma regra para os emails de confiança.

Planejamento

- 1) Criar um grupo de emails em Grupos de Usuários, que conterão os emails considerados de confiança (**Emails Externos**);
- 2) Criar um grupo chamado Emails Internos (**Diretoria**), ao qual serão cadastrados todos os emails importantes;
- 3) Na classificação de SPAM (**regras avançadas de SPAM**), vamos pontuar negativamente de acordo com regras previamente determinadas por nós.

Opcionalmente é possível fazer o inverso, isto é, pontuar emails que chegam fingindo serem do diretor que não vierem dos emails de confiança.



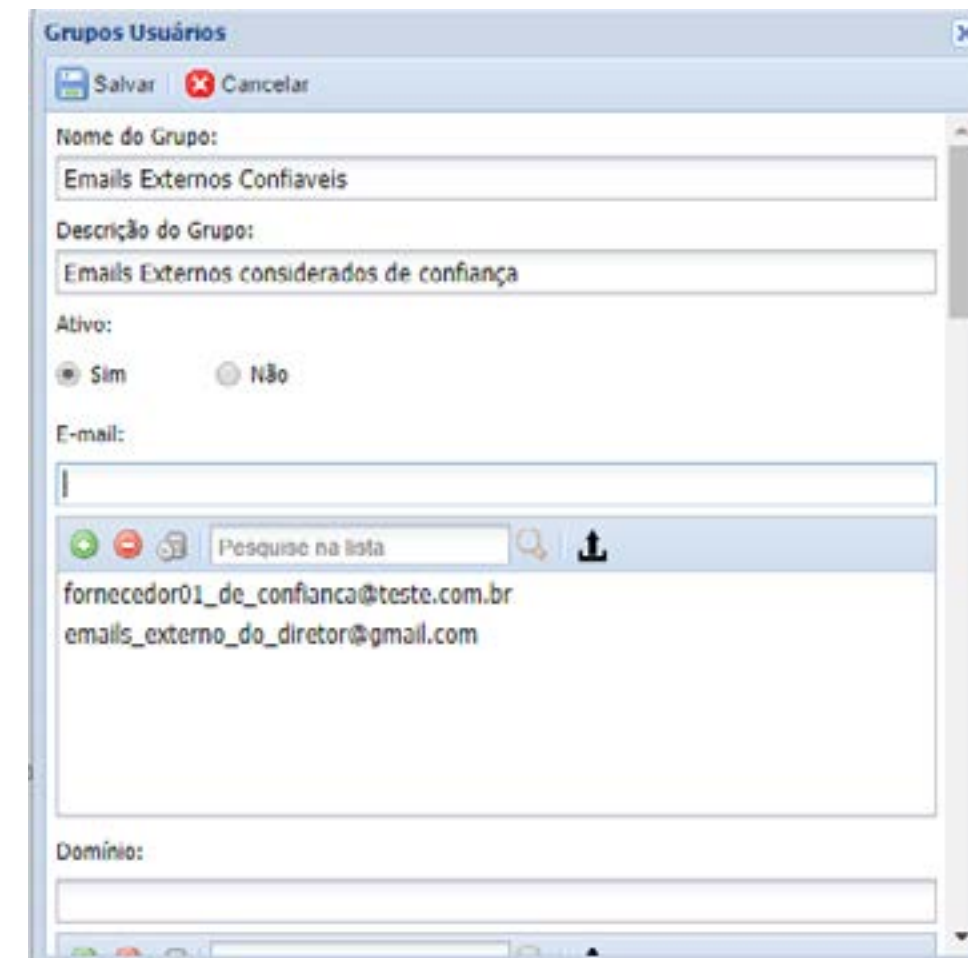
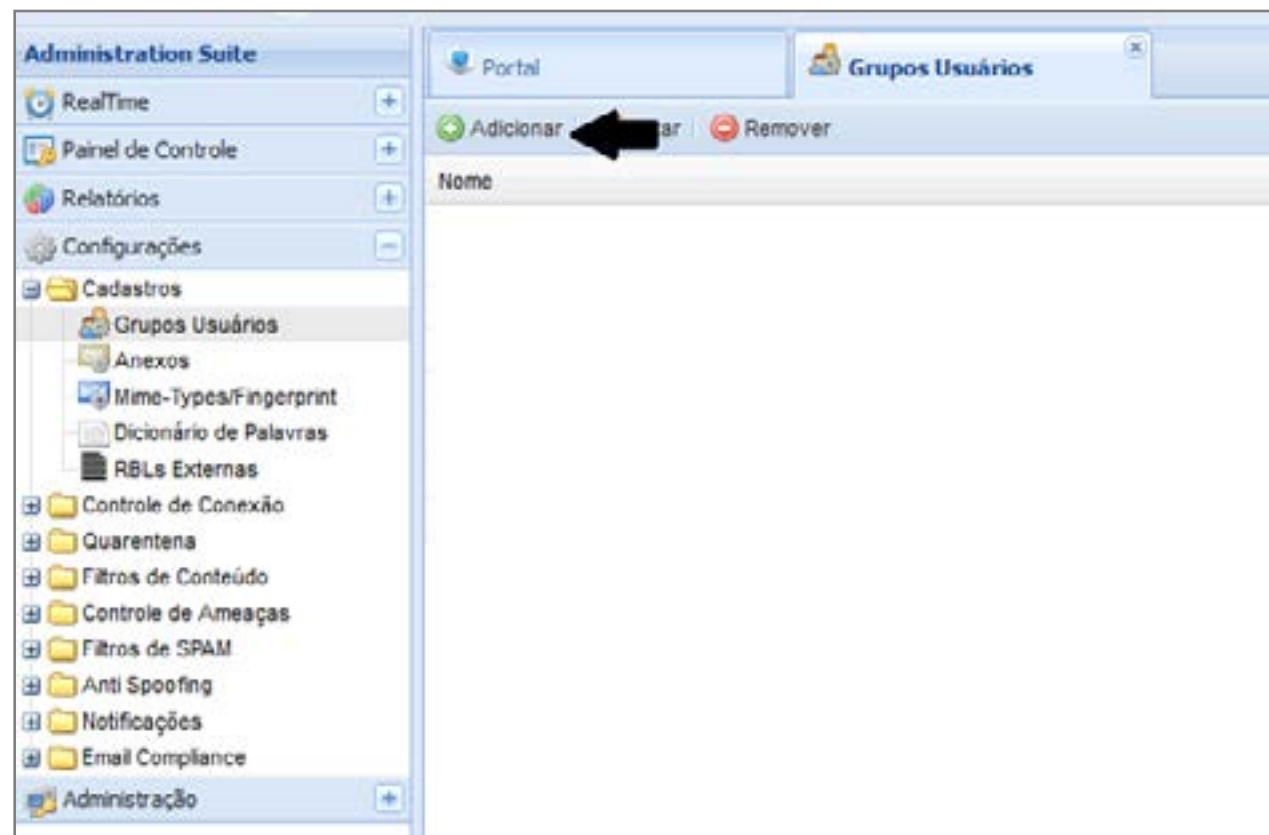
Criação de Grupo de Emails Externos de Confiança

Vá em **Configurações > Cadastro > Grupo de Usuários**

Clique em **Adicionar** > Insira no nome do Grupo (no exemplo foi Emails Externos), descrição e os e-mails dos destinatários a serem protegidos.

Obs: Não esqueça de clicar em + para incluir o email na lista.

Após inserida a lista de remetentes, clique em **Salvar**. Será fechada a janela de Grupos de Usuários e aparecerá na lista o grupo que você acabou de criar.



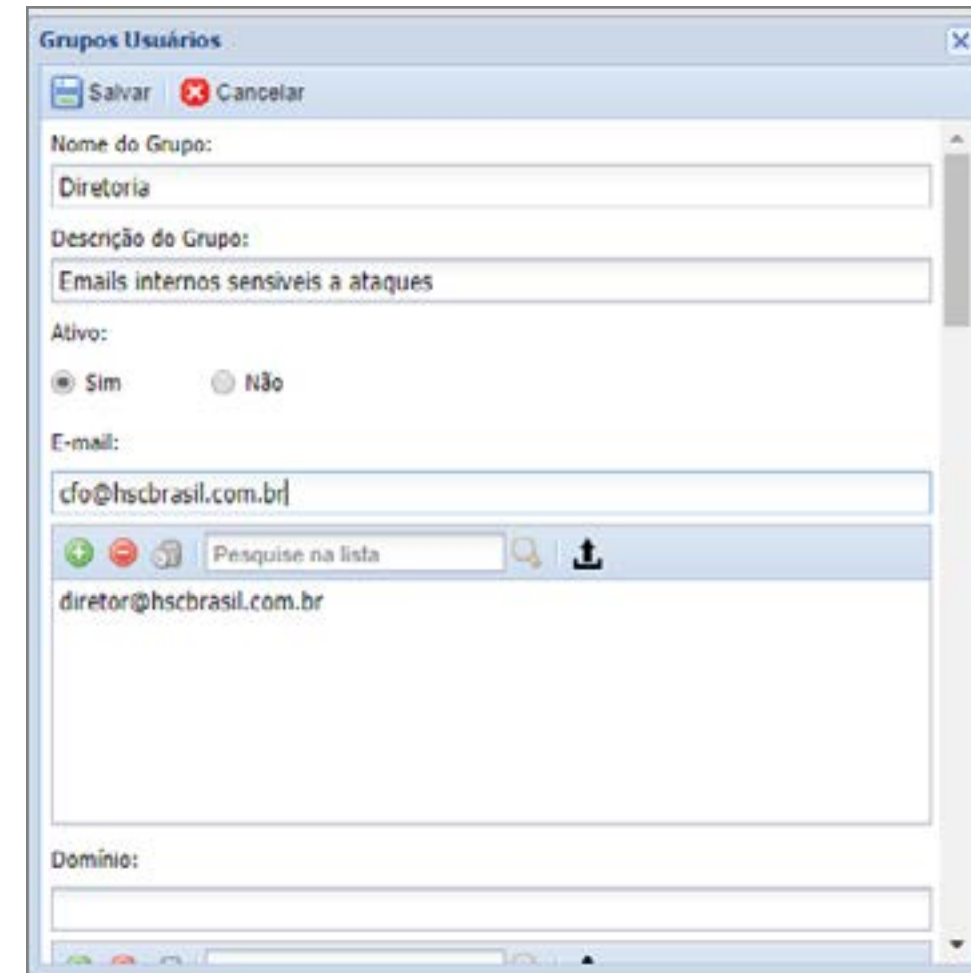
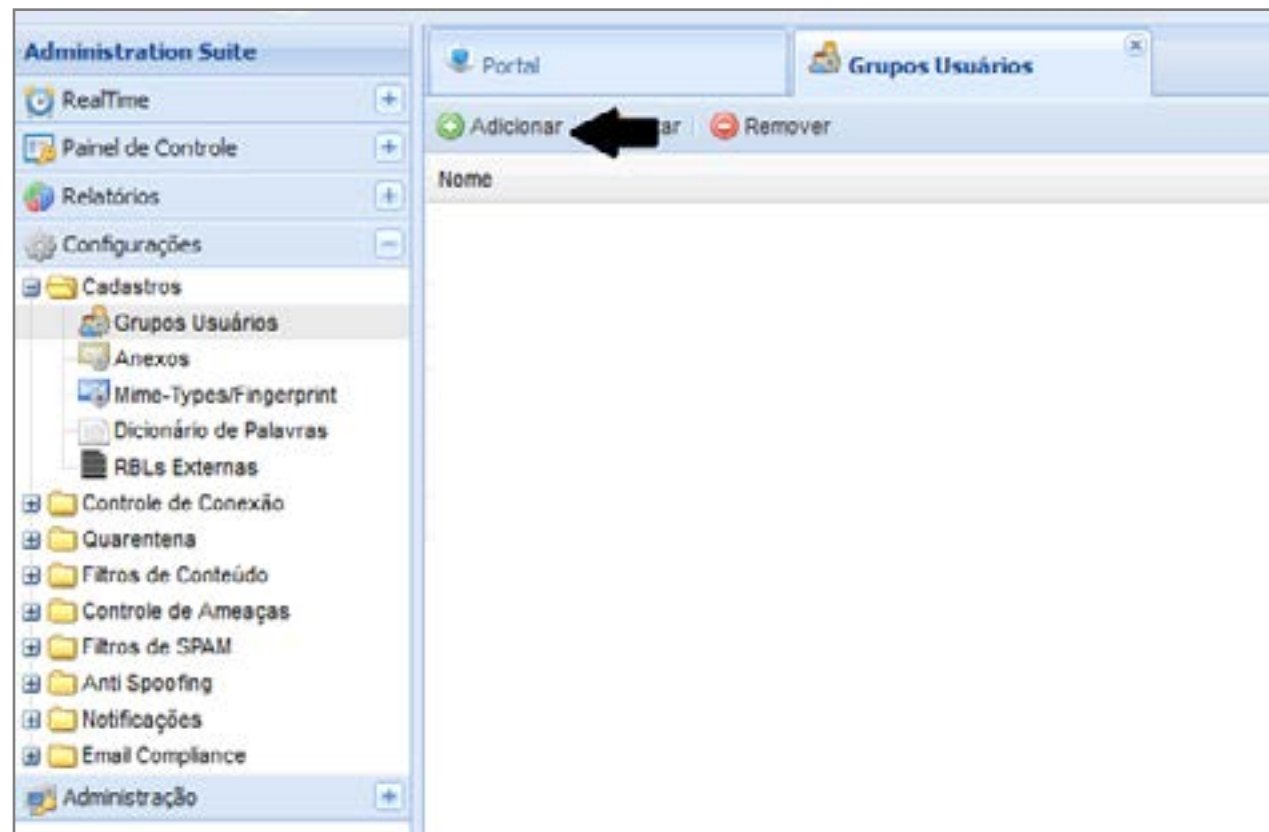
Criação de Grupo de Emails dos Diretores

Configurações > Cadastro > Grupo de Usuários

Clique em **Adicionar** > Insira no nome do Grupo (no exemplo foi Diretoria), descrição e os e-mails dos Diretores/emails sensíveis a ataques.

Obs: Não esqueça de clicar em + para incluir o email na lista.

Após inserida a lista da diretoria, clique em **Salvar**. Será fechada a janela de Grupos de Usuários e aparecerá na lista o grupo que você acabou de criar.



Regra de SPAM – Email Externo Confiável

Em Configurações > Filtro de SPAM > Controle Avançado

Clique em **Adicionar**

- Seleção de Controle: **Cabeçalho**
- Defina o cabeçalho a ser utilizado: **From**
- Grupos: **Emails Externos Confiáveis**
- Número Mínimo de Ocorrências: **1**

Cabeçalho 2/4

Define o filtro para o controle selecionado.

Define o cabeçalho a ser utilizado:

Grupos:

Número Mínimo de Ocorrências:

Na etapa de **Informações e Pontuação**

- Nome: **Emails Externos Confiáveis**
- Descrição: **Emails Externos Confiáveis**
- Pontuação: **-1**

Informações e Pontuação 3/4

Define informações gerais e ações que serão realizadas.

Nome:

Descrição:

Ações

Pontuação:

Clique em **Avançar** > E depois de apresentado o resumo, clique em **Salvar**.

Emails Externos Confiáveis	Cabeçalho	Pontuação: -1
----------------------------	-----------	---------------

Regra de SPAM – Diretoria

Em Configurações > Filtro de SPAM > Controle Avançado

Clique em **Adicionar**

- Seleção de Controle: **Cabeçalho**
- Defina o cabeçalho a ser utilizado: **To**
- Grupos: **Diretoria**
- Número Mínimo de Ocorrências: **1**

Cabeçalho 2/4

Define o filtro para o controle selecionado.

Define o cabeçalho a ser utilizado:

Grupos:

Número Mínimo de Ocorrências:

Na etapa de **Informações e Pontuação**

- Nome: **Diretoria**
- Descrição: **Emails da diretoria e/ou sensíveis a ataques**
- Pontuação: **-1**

Informações e Pontuação 3/4

Define informações gerais e ações que serão realizadas.

Nome:

Descrição:

Ações

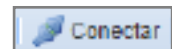
Pontuação:

Clique em **Avançar** > E depois de apresentado o resumo, clique em **Salvar**.

Diretoria	Cabeçalho	Pontuação: -1
-----------	-----------	---------------

Casando as regras

Emails Externos Confiáveis	Cabeçalho	Pontuação: -1
Diretoria	Cabeçalho	Pontuação: -1



Selecione as duas regras e clique em **Conectar**

Conectar Regras

Salvar Cancelar

Emails Externos Confiáveis: Casar

Operador Lógico: E

Diretoria: Casar

Ações

Pontuação: -5

- Pontuação: **-5**

Resumo da regra

O que vier dos emails de confiança > Diretoria, ele baixará a pontuação, deixando mais relaxado para eles, pois o grupo de usuário Email Externos Confiáveis fazem parte dos emails aprovados pela empresa para deixar passar possível spam.

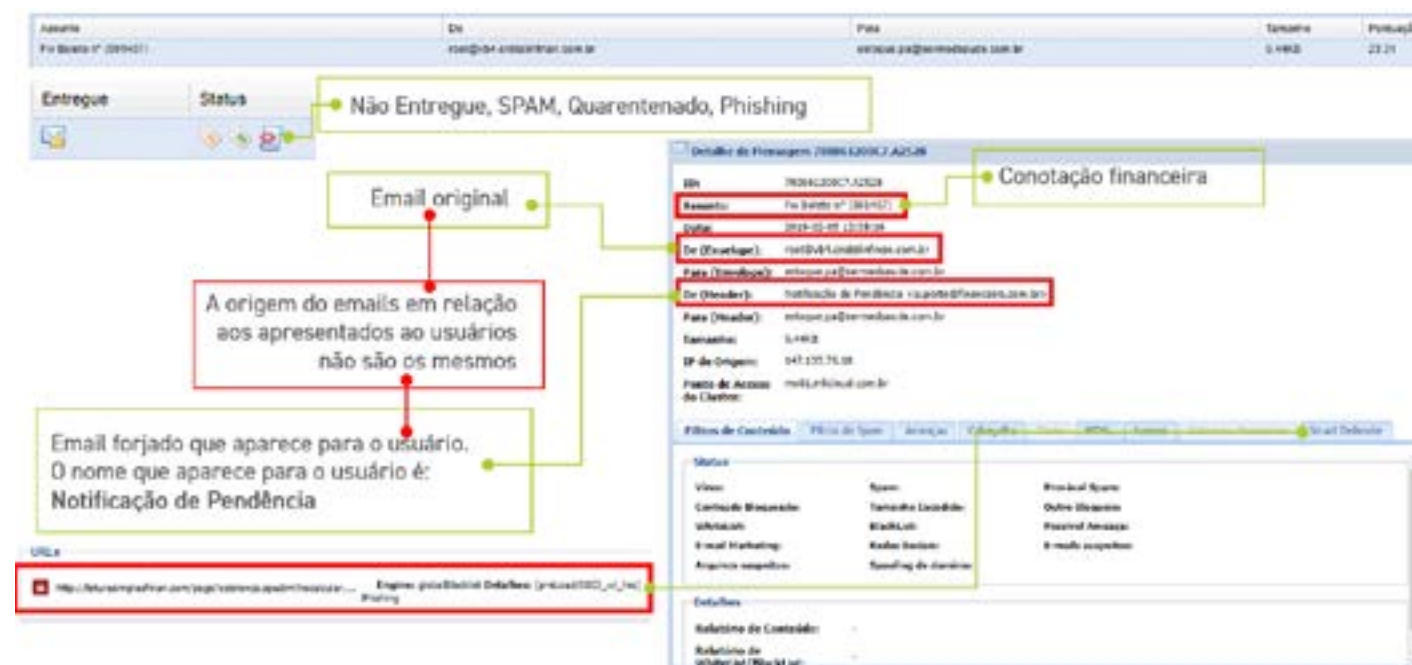
(Emails Externos Confiáveis) E (Diretoria)	(Cabeçalho) E (Cabeçalho)	Pontuação: -5
--	---------------------------	---------------

Proteção a fraude de email pela análise do Display Name

Sabendo que boa parte de fraude de email não se preocupa com o Display Name, geralmente enviando o email “padrão” em nomes dos diretores (emails de entrada), uma possível solução é:

- 1) Criar um grupo chamado Display Name e incluir os diretores/emails sensíveis nesta lista;
- 2) Efetuar a verificação do Display Name quando o email vier de “fora” e pontuar quanto a isso.

Características de Fraude de Email



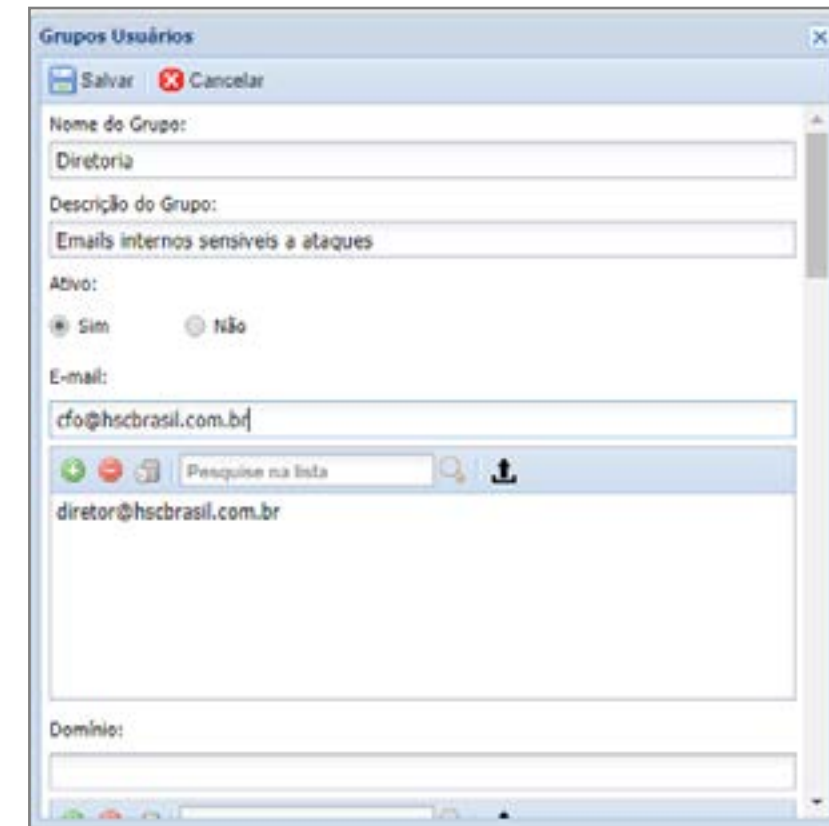
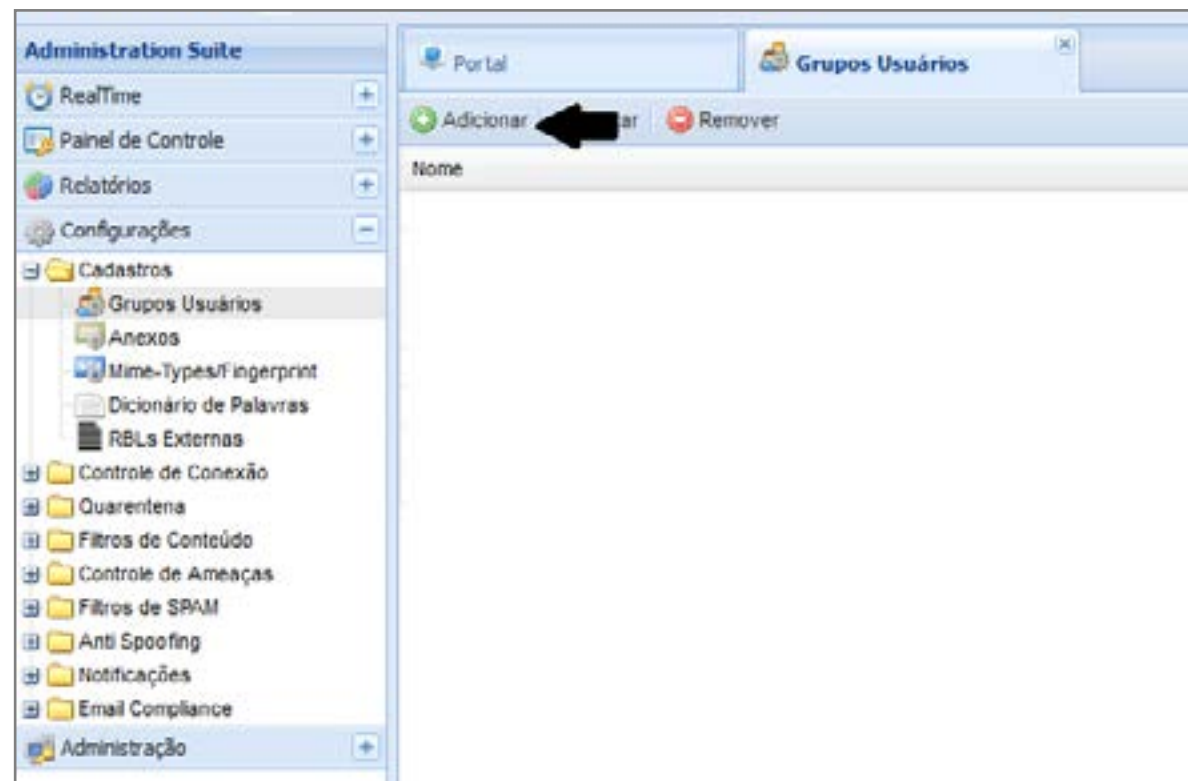
Criação de Grupo de Email dos Diretores

Configurações > Cadastro > Grupo de Usuários

Clique em **Adicionar** > Insira no nome do Dicionário (no exemplo foi Diretoria), descrição e os e-mails dos diretores/emails sensíveis a ataques.

Obs: Não esqueça de clicar em + para incluir o Email na lista.

Após inserida a lista de email da diretoria, clique em **Salvar**. Será fechada a janela de Grupos de Usuários e aparecerá na lista o grupo que você acabou de criar.

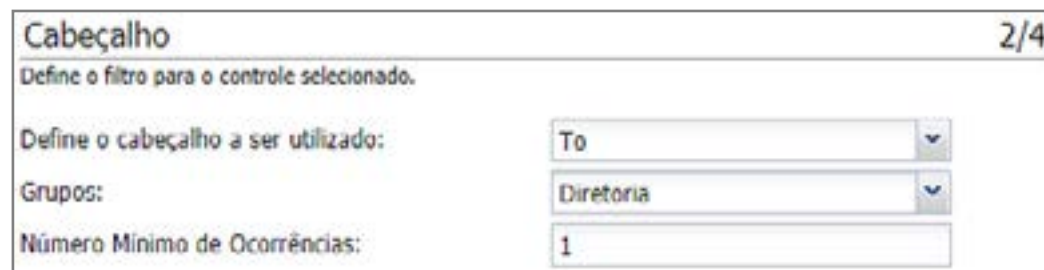


Regra de SPAM – Diretoria

Em Configurações > Filtro de SPAM > Controle Avançado

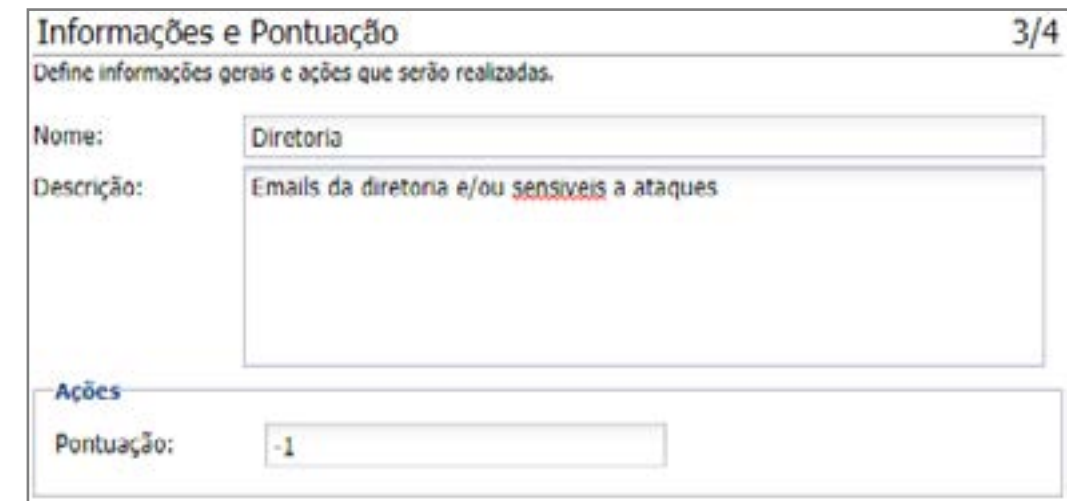
Clique em **Adicionar**

- Seleção de Controle: **Cabeçalho**
- Defina o cabeçalho a ser utilizado: **To**
- Grupos: **Diretoria**
- Número Mínimo de Ocorrências: **1**



Na etapa de **Informações e Pontuação**

- Nome: **Diretoria**
- Descrição: **Emails da diretoria e/ou sensíveis a ataques**
- Pontuação: **-1**



Clique em **Avançar** > E depois de apresentado o resumo, clique em **Salvar**.



Regra de SPAM – Display Name

Em *Configurações > Filtro de SPAM > Controle Avançado*

Clique em **Adicionar**

- Seleção de Controle: **Cabeçalho**
- Define o cabeçalho a ser utilizado: **Customizado**
- Cabeçalho Customizado: **From**
- Dicionário de Palavras: **Display Name - Diretores**
- Número Mínimo de Ocorrências: **1**

Cabeçalho 2/4

Define o filtro para o controle selecionado.

Define o cabeçalho a ser utilizado: Customizado

Cabeçalho Customizado: From

Dicionário de Palavras: Display Name - Diretores

Número Mínimo de Ocorrências: 1

Clique em **Avançar**

Na etapa de **Informações e Pontuação**

- Nome: **Display Name Diretores**
- Descrição: **Nomes de Apresentação utilizados pelos diretores em Seus Emails Profissionais**
- Pontuação: **-1**

Informações e Pontuação 3/4

Define informações gerais e ações que serão realizadas.

Nome: Diretoria

Descrição: Emails da diretoria e/ou sensíveis a ataques

Ações

Pontuação: -1

Clique em **Avançar** > E depois de apresentado o resumo, clique em **Salvar**.

Display Name Diretores	Cabeçalho	Pontuação: 1
------------------------	-----------	--------------



Casando as regras

64	Display Name Diretores	Cabeçalho	Pontuação: 1
77	PARA Diretoria	Cabeçalho	Pontuação: 1



Selecione as duas regras e clique em **Conectar**

The dialog box 'Conectar Regras' contains the following configuration:

- Display Name Diretores: Não Casar
- Operador Lógico: E
- PARA Diretoria: Casar
- Ações: Pontuação: 2

- Pontuação: 2

Resumo da regra

O que vier destinado a Diretoria, será verificado o Display Name. Caso o Display Name não case com nenhum dos nomes cadastrados pelas expressões regulares cadastradas, o sistema aumentará a pontuação de SPAM do email em 2 pontos.

{! Display Name Diretores} E {PARA Diretoria} {! Cabeçalho} E {Cabeçalho} Pontuação: 2



Sistema da Proteção a Spoofing de Domínio

O MailInspector consegue detectar quando há tentativa de envio de emails externos usando o próprio domínio da empresa. Muitos hacker utilizam dessa técnica, pois o sistema de email/MTA (por padrão) é configurado para aceitar emails do domínio utilizado, mesmo que sejam externos.

Portanto, com o MailInspector, o administrador pode configurar para barrar emails vindos de fora que estejam usando o próprio domínio da empresa.



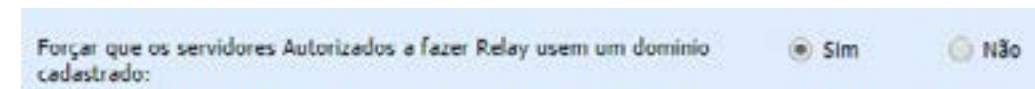
Sistema da Proteção a Spoofing de Domínio de Saída

Quando temos alguma máquina infectada na rede, muitas vezes ela caba disparando SPAM's e emails ameaçadores, sendo BOT usado pelo hacker.

Em grande maioria desses emails, o hacker utiliza de Spoofing para enganar o destinatário.

Para evitar que isso aconteça, o MailInspector possui a opção de barrar emails de saída que não tenham no seu campo de FROM o domínio da sua empresa.

Para isso, basta ativar a funcionalidade para que os servidores de relay autorizado sejam forçados a usar um domínio cadastrado no MailInspector.



Sistema de Controle de Novos Domínios

Sabendo que muitos hackers compram domínios novos e os utilizam somente para mandar spams/emails falsos, o MailInspector tem a opção do administrador escolher o que fazer com emails oriundos de novos domínios.

- **Bloquear:** Bloqueia o email com domínio considerado novo;
- **Ignorar:** Deixa passar o email, mesmo que ele tenha menos tempo de criação do que configurado pelo administrador como novo domínio;
- **Pontuar:** Aumenta a pontuação dos emails oriundos de domínios considerados novos.

Também é possível ao administrador indicar o que para ele é considerado domínio recém adquirido.



Sistema de comparação de domínios diferentes no cabeçalho



Basicamente é a comparação do campo From (Header) em relação ao From (Envelope).

O ataque por adulteração do campo From (Header) é o que está mais na moda em relação a Fraude de Email. O MailInspector possui um sistema específico para detectar esse tipo de ataque, ao qual verifica se foi adulterado o campo Mail From, permitindo ao administrador da solução rastrear a origem da ameaça.

Destinatário	E-mails	Spoofing	DKIM fail	SPF fail
contato@gtpn.com.br	10364	35	10289	366
vendas@gtpn.com.br	116	-	116	-
romulo@hscbrasil.com.br	19	-	19	-
romulo@gtpn.com.br	1	-	1	-

Ainda sabendo que muitos hackers mudam o cabeçalho do email, o MailInspector compara os domínios de origem do campo From (Envelope do email) e do campo From (Header do email) para verificação de discrepância entre eles. Sendo diferentes, é possível efetuar uma ação, como pontuar ou bloquear.

Sistema de detecção de uso de Free Mail

Outro ponto importante que o MailInspector verifica é se o email origina-se de um sistema de email grátis, como GMAIL, YAHOO MAIL, OUTLOOK (antigo HOTMAIL), etc.

Importante salientar que a verificação de uso de Free Mail, pode casar com regras de por exemplo o Sistema de comparação de domínios diferentes no cabeçalho.

Proteção e prevenção a invasão ao email interno

Quando o email em questão é originário da própria empresa por causa de um vírus ou email que foi invadido, o MailInspector possui um sistema de Controle de Fluxo de Email, ao qual o administrador pode configurar o controle de fluxo tanto para saída de emails, quanto para entrada de email.

Também conta com sistema de pontuação do email devido a reputação e proteção de ataque do tipo Outbreak, bloqueando o IP de origem quando excede uma determinada quantidade de emails com as características de:

- **Email com vírus/malware;**
- **Email de ataques de dicionário;**
- **Ataque dirigido de spam;**



Considerações Finais

Além das diversas proteções anteriormente citadas, o MailInspector utiliza BigData, com uso de assinaturas e com o uso de tecnologia fuzzy hash, garantindo detecção de variantes mesmo antes de novas assinaturas de malware e spams.

Maiores informações sobre a solução MailInspector, você poderá encontrar na nossa página:

[Saiba mais](#)

Fontes:

http://br.amadamiyachi.com/about/email_fraud

<https://www.serasaconsumidor.com.br/ensina/seu-cpf-protegido/como-saber-se-um-e-mail-e-falso-e-evitar-golpes/>

<https://ecommercenews.com.br/noticias/dicas/dicas-para-o-combate-a-fraude-de-comprometimento-do-email-empresarial-ber/>