HIGH SECURITY CENTER

Guia do Usuário Final

Junho/2019

HSC MailInspector 5

Versão do Manual 1.0

MailInspector Cloud - Manual do Usuário final

NOTA IMPORTANTE

Este manual foi desenvolvido exclusivamente para uso para revendas e/ou clientes da HSCBRASIL. Para efetuar distribuição, apresentação, cópia parcial e/ou integral dele, é necessária autorização da empresa HSCBRASIL ou do autor Roberto Chu.

O manual é destinado a USUÁRIO FINAL. Existe outro manual, que é voltado ao ADMINISTRADOR do sistema MailInspector.

Este manual foi desenvolvido baseado no produto HSC MailInspector versão 5.x, sendo utilizado para base dele a versão 5.0.

Para qualquer dúvida e/ou sugestão deve entrar em contato com HSCBRASIL, pelo email negocios@hscbrasil.com.br

DEFINIÇÕES

O que é SPAM?

Spam é o termo usado para referir-se aos e-mails não solicitados, que geralmente são enviados para um grande número de pessoas. Quando o conteúdo é exclusivamente comercial, esse tipo de mensagem é chamada de UCE (do inglês Unsolicited Commercial E-mail).

O que são spam zombies?

Spam zombies são computadores de usuários finais que foram comprometidos por códigos maliciosos em geral, como worms, bots, vírus e cavalos de tróia. Estes códigos maliciosos, uma vez instalados, permitem que spammers utilizem a máquina para o envio de spam, sem o conhecimento do usuário. Enquanto utilizam máquinas comprometidas para executar suas atividades, dificultam a identificação da origem do spam e dos autores também. Os spams Zombies são muito explorados pelos spammers, por proporcionar o anonimato que tanto os protege.

Motivadores de envio de spam

A Internet causou grande impacto na vida das pessoas, tornando-se um veículo de comunicação importante, evoluindo para revolucionar a maneira de fazer negócios e buscar e disponibilizar informações. Ela viabiliza a realidade da globalização nas diversas áreas da economia e do conhecimento. Por outro lado, esse canal acabou absorvendo diversas práticas, boas e ruins.

O spam é uma das práticas ruins. Ele ficou famoso ao ser considerado um tormento para os usuários de e-mail, impactando na produtividade de funcionários e degradando o desempenho de sistemas e redes. No entanto, poucos se lembram de que já enfrentaram algo semelhante, antes de utilizar o e-mail como ferramenta de comunicação.

As cartas de correntes para obtenção de dinheiro fácil, encontradas nas caixas de correio, as dezenas de panfletos recebidos nas esquinas e as ligações telefônicas oferecendo produtos são os precursores do spam. A principal diferença, extremamente relevante, é o fato de que para enviar cartas ou panfletos e ligar para nossas casas, o remetente tinha de fazer algum investimento. Este muitas vezes inviabilizava o envio de material de propaganda em grande escala.

Com o surgimento e a popularização da Internet e, consequentemente, do uso do e-mail, aquele remetente das cartas de corrente ou propagandas obteve a oportunidade e a facilidade de atingir um número muito maior de destinatários. Tudo isso com a vantagem de investir muito pouco ou nada para alcançar os mesmos objetivos em uma escala muito maior. Por essa razão, esse é um dos maiores motivadores para o envio de spam.

Desde o primeiro spam registrado e batizado como tal, em 1994, essa prática tem evoluído, acompanhando o desenvolvimento da Internet e de novas aplicações e tecnologias. Atualmente, o

spam está associado a ataques à segurança da Internet e do usuário, propagando vírus e golpes. Tão preocupante quanto o aumento desenfreado do volume de spam na rede, é a sua natureza e seus objetivos.

O spam ganhou popularidade, é tema tratado em vários sites e protagonista de notícias na imprensa, muitas vezes abordando mecanismos de prevenção ou defesa. O combate ao spam e o desenvolvimento de mecanismos de prevenção e proteção tornaram-se serviços de destaque oferecidos por provedores de acesso e empresas fabricantes de software/hardware.

Toda essa movimentação em torno do tema fez com que surgissem diferentes fontes de informação e muitas controvérsias a respeito do spam. Não é por acaso que tornou-se um assunto quase sempre acompanhado de polêmicas. Com o objetivo de ser uma fonte de referência idônea, imparcial e embasada tecnicamente é que foi criado o site Antispam.br. Ele tem o compromisso primordial de informar o usuário e o administrador de redes sobre o spam.

Fonte: http://www.antispam.br/

Problemas causados pelo SPAM

O spam pode afetar os usuários do serviço de correio eletrônico de diversas formas. Alguns exemplos a seguir mostram como a produtividade, a segurança, entre outros, podem ser ameaçadas.

Não recebimento de e-mails: Boa parte dos provedores de Internet limita o tamanho da caixa postal do usuário no seu servidor. Caso o número de spams recebidos seja grande, ele corre o risco de ter sua caixa postal lotada com mensagens não solicitadas. Se isto ocorrer, passará a não receber e-mails e, até que possa liberar espaço em sua caixa postal, todas as mensagens recebidas serão devolvidas ao remetente. Outro problema é quando o usuário deixa de receber e-mails nos casos em que regras anti-spam ineficientes são utilizadas, por exemplo, classificando como spam mensagens legítimas.

Gasto desnecessário de tempo: Para cada spam recebido, o usuário necessita gastar um determinado tempo para ler, identificar o e-mail como spam e removê-lo da caixa postal.

Aumento de custos: Independente do tipo de acesso à Internet utilizado, quem paga a conta pelo envio do spam é quem o recebe. Por exemplo, para um usuário que utiliza acesso discado à Internet, cada spam representa alguns segundos a mais de ligação que ele estará pagando.

Perda de produtividade: Para quem usa o e-mail como ferramenta de trabalho, o recebimento de spams aumenta o tempo dedicado à tarefa de leitura de e-mails, além de existir a chance de mensagens importantes não serem lidas, serem apagadas por engano ou lidas com atraso.

Conteúdo impróprio ou ofensivo: Como a maior parte dos spams é enviada para conjuntos aleatórios de endereços de e-mail, é bem provável que o usuário receba mensagens com conteúdo que julgue impróprio ou ofensivo.

Prejuízos financeiros causados por fraude: O spam tem sido amplamente utilizado como veículo para disseminar esquemas fraudulentos, que tentam induzir o usuário a acessar páginas clonadas de instituições financeiras ou a instalar programas maliciosos, projetados para furtar dados pessoais e financeiros. Esse tipo de spam é conhecido como phishing/scam. O usuário pode sofrer grandes prejuízos financeiros, caso forneça as informações ou execute as instruções solicitadas nesse tipo de mensagem fraudulenta.

Fonte: http://www.antispam.br/

Tipos de SPAM

Desde o aparecimento do primeiro spam, em 1994, a prática de enviar e-mails não solicitados tem sido aplicada com vários objetivos distintos e também utilizando diferentes aplicativos e meios de propagação na rede. Os tipos de spam identificados até o momento são correntes, boatos, lendas urbanas, propagandas, ameaças, pornografia, códigos maliciosos, fraudes e golpes, spIM (spam via Instant Messenger), spam via redes sociais e spit (spam over internet telephony).

Correntes (chain letters)

Um texto característico de uma corrente geralmente pede para que o usuário (destinatário) repasse a mensagem um determinado número de vezes ou, ainda, "para todos os amigos" ou "para todos que ama". O texto pode contar uma história antiga, descrever uma simpatia (superstição) ou, simplesmente, desejar sorte. Atualmente, o envio em massa de correntes diminuiu bastante, continuando frequente em grupos e listas de discussão de amigos.

Algumas correntes utilizam métodos de engenharia social para convencer o usuário a repassar a mensagem, ou seja, a "não quebrar a corrente".

Propagandas

Os spams com conteúdo de propaganda são conhecidos como UCE (Unsolicited Comercial E-mail). A publicidade pode envolver produtos, serviços, pessoas, sites etc.

Esse tipo de spam é motivo de discussão e polêmica, afinal, é possível fazer marketing na Internet sem fazer spam. No entanto, aqueles que insistem em divulgar sua imagem ou negócio por meio de mensagens não solicitadas, acabam comprometendo sua credibilidade. A solução é o marketing responsável na rede.

Por outro lado, alguns spams oferecem produtos que não existem e serviços que nunca serão entregues. Os casos mais comuns são os e-mails vendendo pílulas milagrosas para melhorar o desempenho sexual de homens e mulheres ou, ainda, para perder peso dormindo.

Ameaças, brincadeiras e difamação

Existem casos de envio de grande quantidade de e-mails ou mensagens eletrônicas contendo ameaças, brincadeiras inconvenientes ou difamação de amigos ou ex-(maridos, esposas, namorados e namoradas). O ato de enviar uma grande quantidade de mensagens, por si, já caracteriza o spam.

Quando a pessoa ou empresa envolvida nesse tipo de spam sentir-se lesada, pode registrar Boletim de Ocorrência na Polícia e, eventualmente, conduzir processo por calúnia e difamação, por exemplo.

Pornografia

O envio de material de pornografia por meio de mensagens não solicitadas é uma das modalidades mais antigas de spam. Duas questões importantes relacionadas a este tópico são: o recebimento desse tipo de spam pelas crianças e a propagação de material de pedofilia. No primeiro caso, é

importante utilizar recursos técnicos anti-spam, além de acompanhar as crianças que têm acesso ao e-mail e aos demais aplicativos da rede desde muito jovens.

Em relação à pedofilia, a orientação é clara: notificar imediatamente aos órgãos competentes, como a Polícia Federal. O e-mail para denúncias de pedofilia é dcs@dpf.gov.br

Spit e spim

O spit refere-se ao "spam via Internet Telephony". Assim, as mensagens não solicitadas também se propagam por outros meios, atingindo os usuários dos "telefones IP" (VoIP). O spim é o termo empregado para os "spams via Instant Messenge", ou seja, o envio de mensagens eletrônicas não solicitadas por meio dos aplicativos de troca de mensagens instantâneas como, por exemplo, o Microsoft Messenger e o ICQ.

Spam via redes de relacionamentos

Um dos sites de redes de relacionamentos mais populares na Internet atualmente é Facebook (www.facebook.com) ou o antigo Orkut (www.orkut.com), além do Linked In (www.linkedin.com) e outros com as mesmas características. Esses sites propiciam um terreno fértil para a propagação de spam, principalmente, de boatos e propagandas. Por outro lado, a maioria deles possui opções de configuração que permitem aos usuários protegerem-se das mensagens não solicitadas enviadas por pessoas que não estejam em suas listas de contatos, por exemplo.

Propagação de vírus e RANSOMWARE

Junto ao spam, é enviado algum arquivo contaminado, com algum título de interesse do recebedor, para que o mesmo rode o executável. Uma vez executado o programa, a máquina da pessoa é infectada e se for ransomware, é efetuada a criptografia de todos os compartilhamentos e arquivos pertinentes na máquina do usuário com senha. Após encriptado os dados, geralmente aparece uma nota na tela indicando a forma e o valor em bitcoins a ser pago ao hacker, para que o mesmo envie a senha para liberação dos dados.

Fonte: http://www.antispam.br/tipos/

O que é Filtro de ANTI-SPAM?

É um conjunto de soluções ou sistemas usados por provedores no combate ao SPAM que analisam as mensagens que chegam a um determinado usuário e, com base em regras ou em verificações de determinados ítens, tentam determinar se aquele e-mail é SPAM ou não.

A questão é que muitos filtros ou sistemas classificam como SPAM uma mensagem verdadeira ou permitem a passagem de um e-mail que realmente era SPAM. Nesse último caso, até que não se trata de um problema tão ruim, afinal, nenhum filtro é 100% eficaz. No entanto, deixar de receber uma mensagem verdadeira é o maior problema. A maioria dos sistemas de e-mail com soluções anti-spam tem uma pasta dessas. Pelo menos assim, o usuário pode ver o que foi direcionado a esses diretórios. No entanto, em muitos casos, a mensagem nem chega e retorna ao emissor.

Alguns filtros do ANTI-SPAM HSC MLI

Filtro de Endereços ou Servidor de Email

Ao enviar um spam, o spammer, ou alguém que envia spam, precisa enviá-lo a partir de um endereço de email registrado em alguma conta ou servidor. Muitos desses spammers criam seus próprios serviços de envio de spam, então fica fácil para os filtros identificarem endereços ou servidores de email que sempre enviam emails identificados como Spam pelos usuários.

Filtro de IP

Sempre que um determinado email é identificado como spam, o provedor de email marca aquele endereço de IP de quem enviou como sendo de um spammer. Assim fica mais fácil identificar spam, não necessariamente pelo endereço de email, que pode ser clonado, mas pelo endereço de IP que é muito mais preciso.

Filtro de Palavras

A grande maioria dos spams vêm com determinadas palavras-chave, para chamarem a atenção do usuário para algum serviço ou venda online. Todo servidor de email atualmente vem com um filtro que faz uma varredura preliminar no conteúdo do email que você recebe em busca dessas palavras, que geralmente são “Viagra”, “Cialis” ou algo relacionado à venda de remédios online ou práticas ilícitas. Os filtros também reconhecem mensagens escritas somente com letras maiúsculas ou escritas com palavras e caracteres aleatórios e as separam como Spam.

Filtro de Links

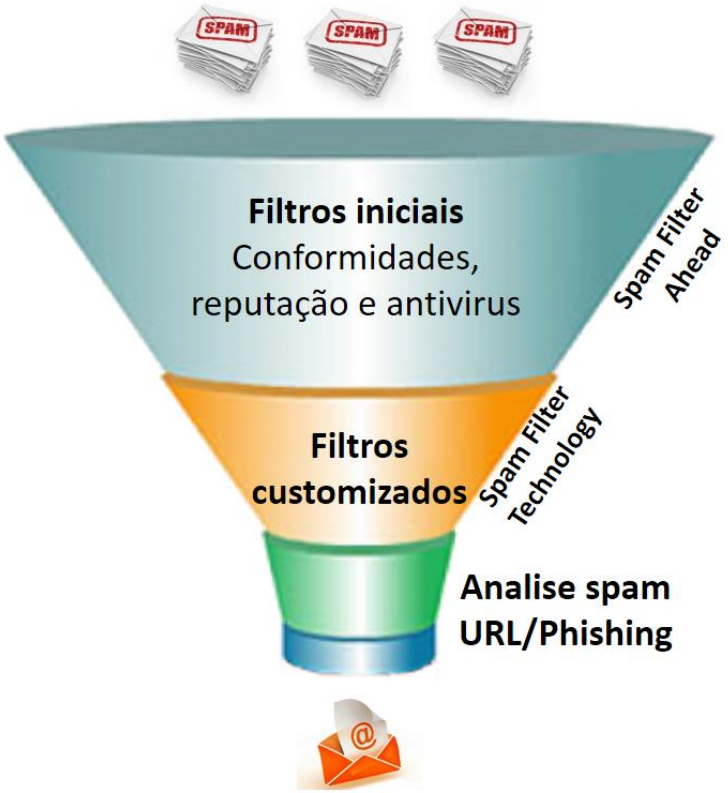
Um dos principais objetivos do spam é levá-lo a algum outro site onde ele pode vender algo a você ou pode roubar alguma informação sua através de um sistema de phishing ou instalação de vírus na sua máquina. Vários desses sites já são conhecidos e sua lista cresce a cada dia. Caso um email tenha algum link que leve a alguma dessas páginas, o filtro bloqueia automaticamente.

Filtro de Tamanho do Email e controle de anexo

Um dos ataques mais comuns é email massivo com vários anexos, dessa forma sobrecarrega-se o servidor de email e o mesmo “trava”. Para evitar isso, o HSC MLI possui filtro de controle de tamanho do email, quantidade de anexo, quantidade de arquivos compactados, quantidade de nível de compactação, filtros baseados em Mime Type, entre tantos outros filtros que protegem na entrada do email, dessa forma, muitas vezes já descartando os e-mails “perigosos” na camada de MTA (na camada de controle de conexão).

Múltiplas camadas de proteção HSC MLI

A proteção do anti-spam HSC MLI passa por múltiplas camadas de proteção, em uma espécie de funil de filtros até chegar nas últimas camadas onde são analisadas e pontuadas quanto a spam. Essa forma de análise garante melhor desempenho do produto.



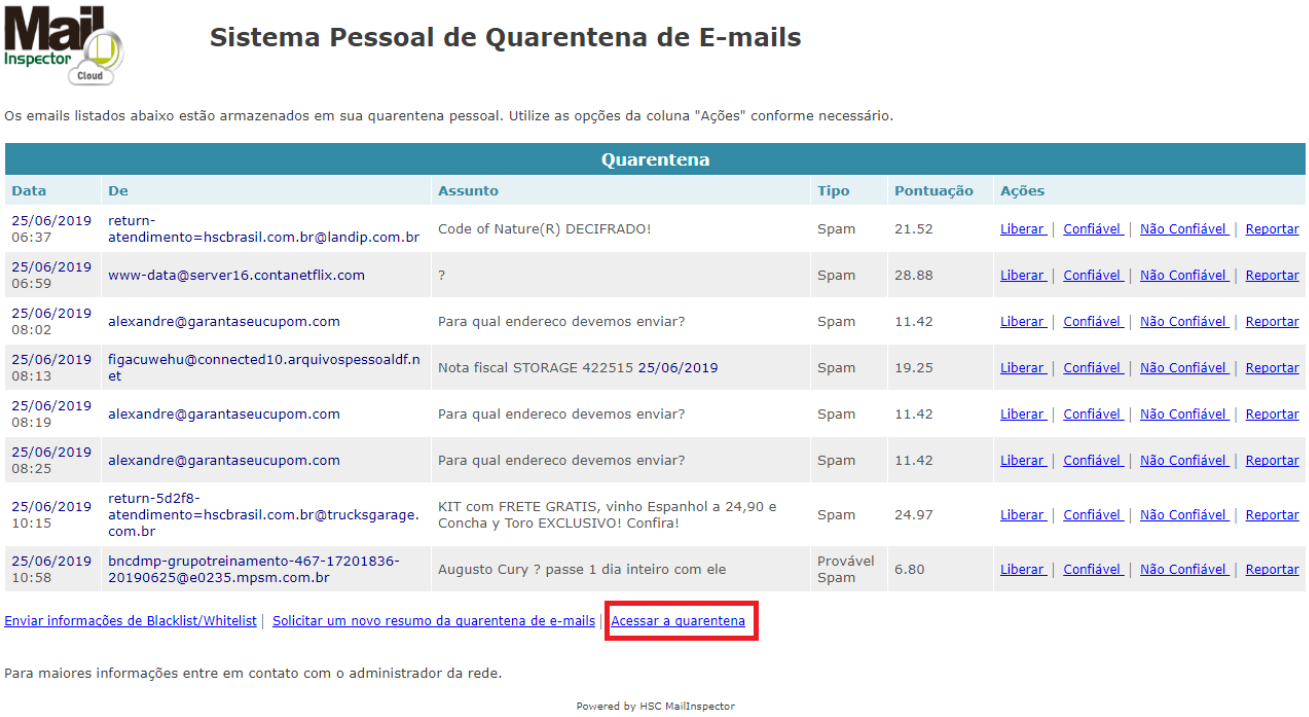
Mais proteção por menor custo de processamento.

01 | Global Threat Protection Network "Reputation Control"
02 | F-secure - Security Cloud "Reputation Control"
03 | MTA Firewall
04 | Outbreak Filter and Spam Throttling
05 | Real Time Black List
06 | Rate Controls
07 | Mail Quotas and Flow Control
08 | Criptografia de Mensagens SSL/TLS
09 | Anti DOS
10 | S. A. SPF, Domain Key, DKIM and Sender ID
11 | Greylist Filter
12 | Global Address List
13 | Bounce Control - Bounce Address Tag Verification
14 | HSC Threat Defender "Antivirus Engine"
15 | F-secure "Antivirus Engine"
16 | HTML Filter
17 | Attachment Control
18 | Fingerprint Analysis
19 | Document Inspect
20 | Image Analysis
21 | URL Intention
22 | Bayes Filter
23 | Anti-phishing
24 | User Filter
25 | URL Spam
26 | Encrypt Message
27 | DLP - Data Loss Prevention
28 | HSC Target Attack Protection

PAINEL DE CONTROLE

Primeiros passos

Ao receber o Digest (Notificação de Quarentena), o usuário final poderá acessar o MailInspector através do link contido na parte inferior do email.



Mail Inspector Cloud

Sistema Pessoal de Quarentena de E-mails

Os emails listados abaixo estão armazenados em sua quarentena pessoal. Utilize as opções da coluna "Ações" conforme necessário.

Quarentena

Data	De	Assunto	Tipo	Pontuação	Ações
25/06/2019 06:37	return-atendimento=hscbrasil.com.br@landip.com.br	Code of Nature(R) DECIFRADO!	Spam	21.52	Liberar | Confiável | Não Confiável | Reportar
25/06/2019 06:59	www-data@server16.contanetflix.com	?	Spam	28.88	Liberar | Confiável | Não Confiável | Reportar
25/06/2019 08:02	alexandre@garantaseucupom.com	Para qual endereco devemos enviar?	Spam	11.42	Liberar | Confiável | Não Confiável | Reportar
25/06/2019 08:13	figacuwehu@connected10.arquivospessoaldf.net	Nota fiscal STORAGE 422515 25/06/2019	Spam	19.25	Liberar | Confiável | Não Confiável | Reportar
25/06/2019 08:19	alexandre@garantaseucupom.com	Para qual endereco devemos enviar?	Spam	11.42	Liberar | Confiável | Não Confiável | Reportar
25/06/2019 08:25	alexandre@garantaseucupom.com	Para qual endereco devemos enviar?	Spam	11.42	Liberar | Confiável | Não Confiável | Reportar
25/06/2019 10:15	return-5d2f8-atendimento=hscbrasil.com.br@trucksgarage.com.br	KIT com FRETE GRATIS, vinho Espanhol a 24,90 e Concha y Toro EXCLUSIVO! Confira!	Spam	24.97	Liberar | Confiável | Não Confiável | Reportar
25/06/2019 10:58	bncdmp-grupotreinamento-467-17201836-20190625@e0235.mpsm.com.br	Augusto Cury ? passe 1 dia inteiro com ele	Provável Spam	6.80	Liberar | Confiável | Não Confiável | Reportar

Enviar informações de Blacklist/Whitelist | Solicitar um novo resumo da quarentena de e-mails | Acessar a quarentena

Para maiores informações entre em contato com o administrador da rede.

Powered by HSC MailInspector

Ao clicar no link, o usuário irá acessar a sua caixa de quarentena, ao qual poderá efetuar várias configurações e liberação de emails.

O processo é similar ao acesso ao portal do sistema do MailInspector, a única diferença é que no caso de clicar no link, o usuário é autenticado automaticamente, sem necessidade de login.

Acessando o Portal de Anti-Spam.

Para acessar o HSC MLI, você deve digitar o IP e/ou URL fornecido pelo administrador do MailInspector.

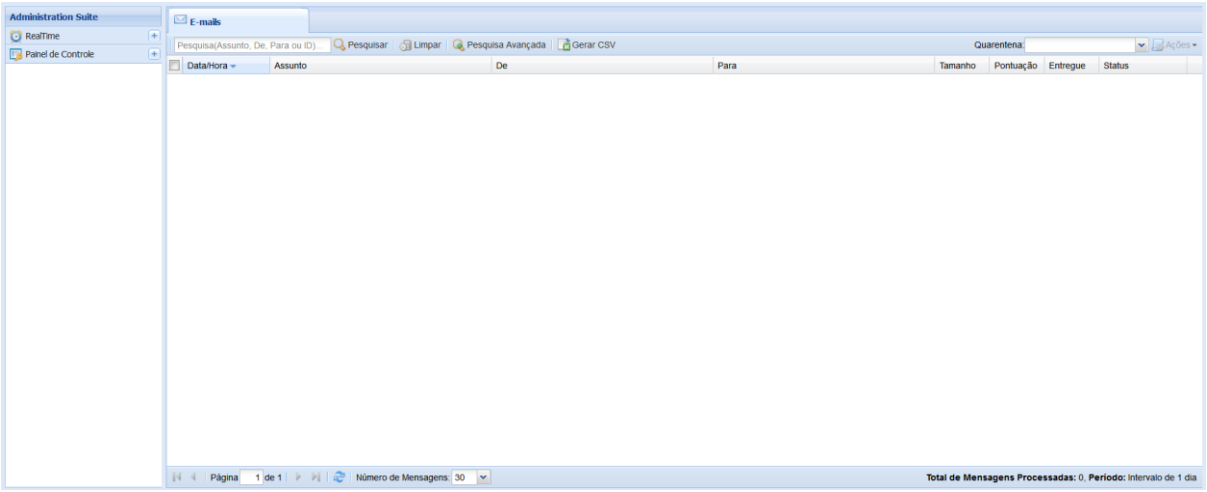
No browser deverá aparecer a tela de login:

Será necessário login com usuário e senha.

Se este for o primeiro acesso, deverá aparecer uma tela semelhante à de baixo:

Clique em Ok

Aparecerá uma tela indicando TUDO que passou de email para você nas últimas 24 horas.



Nesta tela inicial (E-mails) você poderá liberar e-mails que estão na quarentena, marcar o remetente como whitelist ou blacklist, bem como verificar o motivo do e-mail estar na quarentena e a sua pontuação.

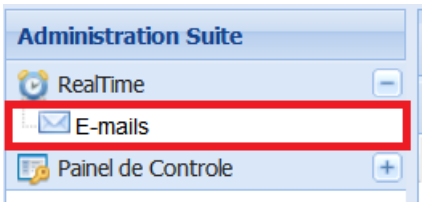
ADMINISTRAÇÃO DE EMAILS

Status do email

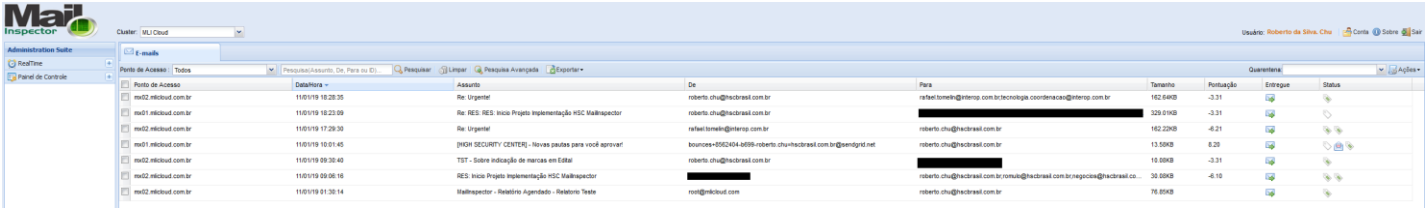
Ao entrar no Painel de Controle do MLI, você visualizará TODOS os e-mails que passaram pelo sistema (emails do dia – desde às 0h) de anti-spam referentes ao seu usuário.

Você também pode acessar esse painel de visualização indo em:

RealTime > E-mails



Nesta tela de E-mails, você visualizará as seguintes informações:



Repare que eles são indicados por colunas. Abaixo a descrição do que é cada uma delas.

Coluna	Descrição
Data/Hora	Data e hora da chegada do email
Assunto	Assunto do email
De	Remetente (quem mandou o email)
Para	Destinatário (para quem se destina o email)
Tamanho	Tamanho do email (incluindo tamanho dos anexos)
Pontuação	Quantos pontos que o email apresentou, quanto mais alto maior é o risco do email ser um SPAM.

Por padrão acima de 6 pontos já é considerado como provável spam.
Acima de 8 pontos é tratado com SPAM.

Entregue

- Indica que o email foi entregue

- Indica que o email foi bloqueado

Status

Indica o status do email, isto é, se ele foi entregue, se foi barrado e o motivo. Segue abaixo os status:

- Provável Spam

- SPAM

- Liberado para entrega pelo usuário ou administrador do anti-spam

- Está cadastrado na Whitelist da empresa

- Está cadastrado na Blacklist da empresa

- Outro bloqueio (dê duplo clique sobre o email para ver qual o motivo do bloqueio)

- Phishing

- Email limpo / Auditado

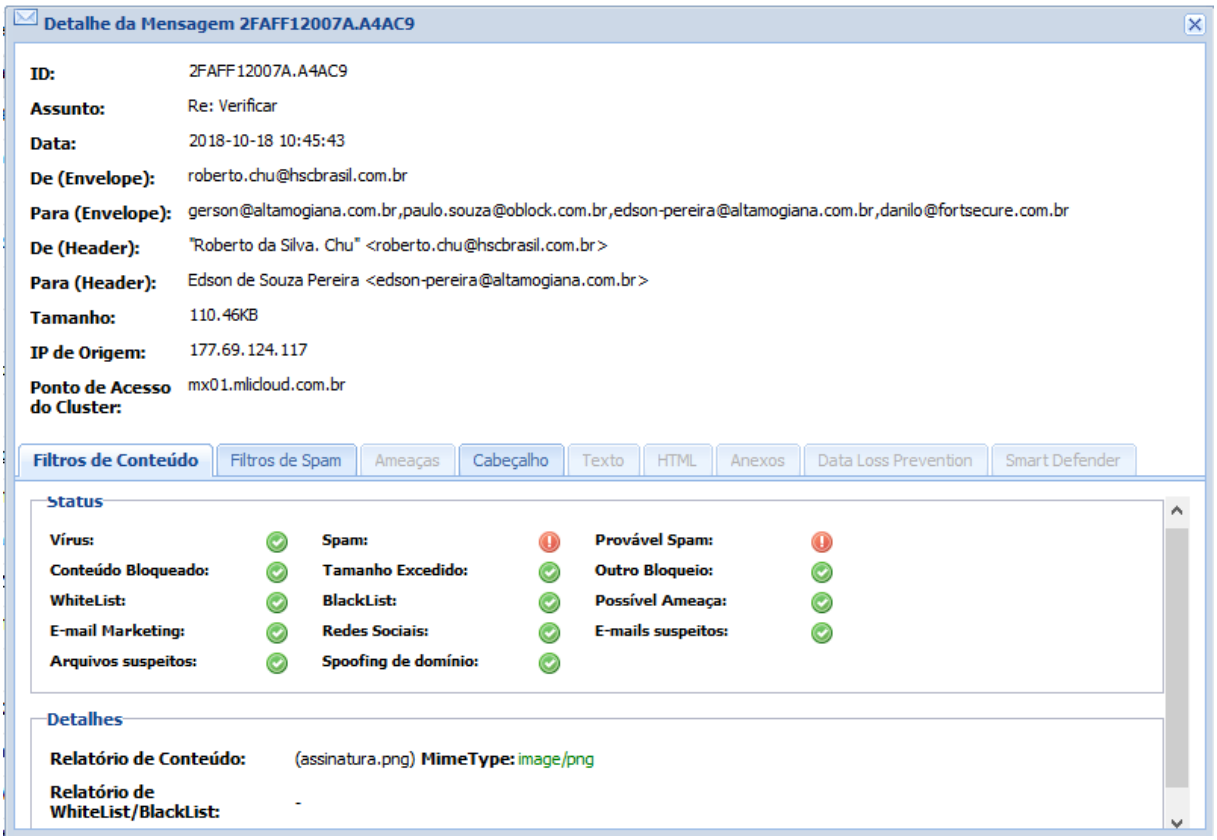
- Conteúdo malicioso

- Vírus

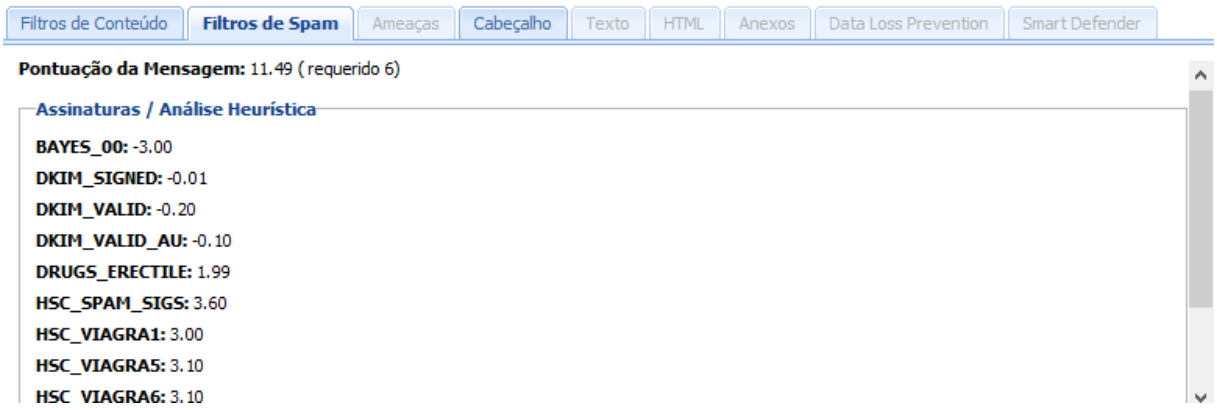
Caso você queira verificar maiores informações sobre o email, basta dar duplo clique sobre ele.

No exemplo a seguir, foi selecionado o email que havia sido barrado no anti-spam:

Ao dar duplo clique sobre o email, abrirá a janela abaixo, indicando maiores detalhes do email (neste caso do email barrado).



Você pode visualizar a pontuação dele na aba Filtros de Spam.



Você também poderá verificar outras informações em cabeçalho, Texto, HTML ou fazer download do email na aba download.

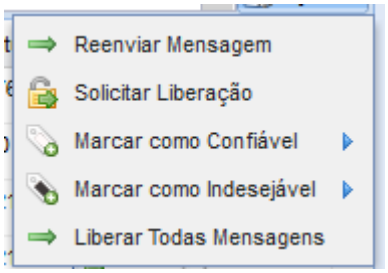
Liberar email da quarentena

Para liberar email da quarentena, você deve ir em:

RealTime -> E-mails

Selecione o email bloqueado, clique no botão Ações (

) e selecione a ação desejada.



Reenviar email: Libera o email bloqueado

Solicitar Liberação: Envia aviso ao administrador para solicitar liberação do email bloqueado. Esse processo é para emails que foram bloqueados por causa de vírus encontrado ou outro tipo de bloqueio que não seja por spam (por exemplo email continha conteúdo proibido, definido pelo administrador).

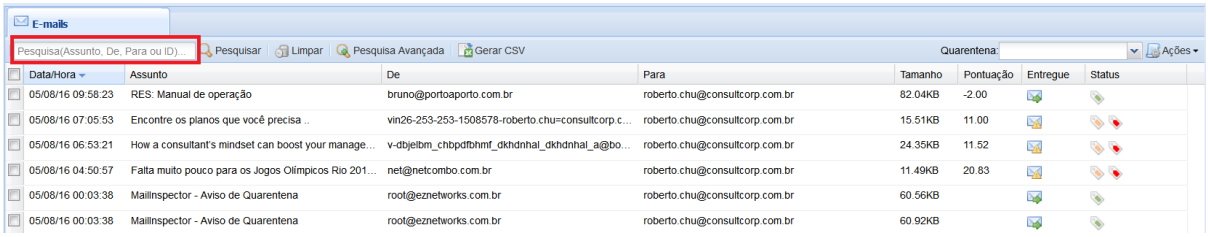
Marcar como confiável: Basicamente é colocar o email/IP/Domínio em Whitelist (os próximos emails vindo deste remetente/IP/domínio, será liberado de verificação de SPAM)

Marcar como indesejável: Basicamente é colocar o email/IP/Domínio em Blacklist (os próximos emails vindo deste remetente/IP/domínio, será automaticamente bloqueado).

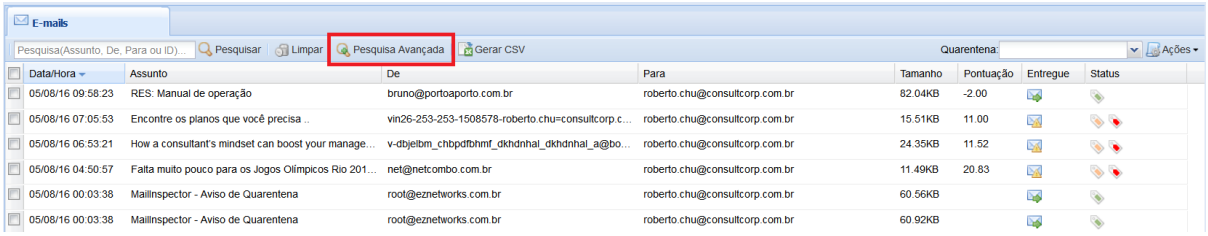
Liberar Rodas Mensagens: É o mesmo que Reenviar Email, mas com ação para múltiplas mensagens (librando as mensagens bloqueadas do dia, de acordo com a filtragem ativa).

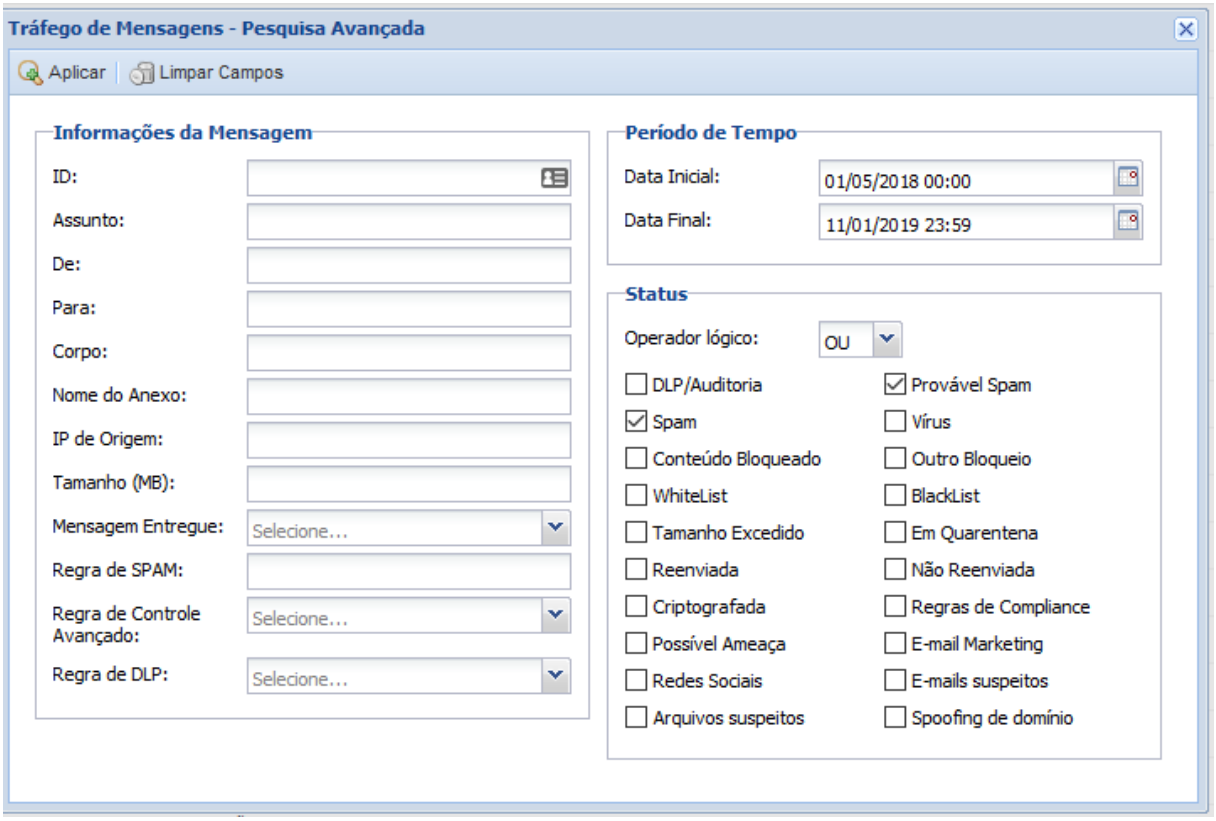
Busca de Emails

Você ainda poderá efetuar buscas mais refinadas de e-mails. Para isso basta preencher o campo Pesquisa (Assunto, De, Para ou ID)



Como neste painel inicial apresenta somente os últimos e-mails do dia (desde às 0h), para fazer pesquisas anteriores, é necessário utilizar a Pesquisa Avançada.



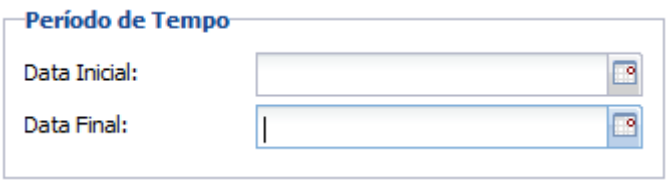


Pesquisa avançada de emails

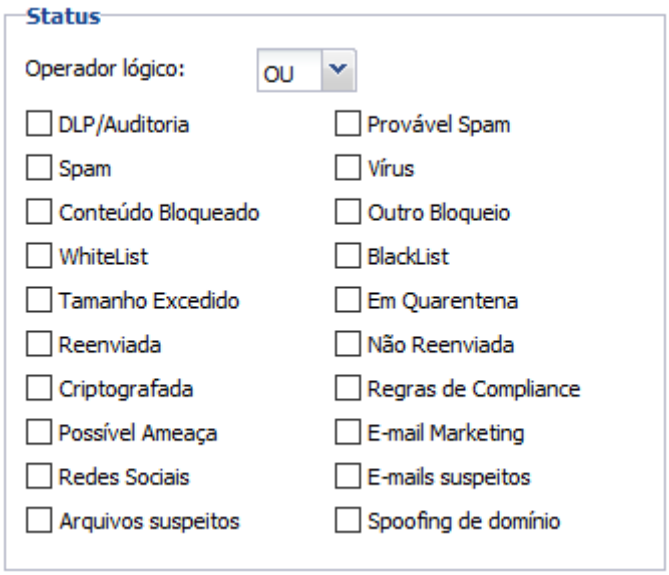
Na pesquisa avançada é possível fazer busca por:

- ID
- Assunto
- De (Origem)
- Para (Destino)
- Corpo (Algum texto que esteja no corpo do email)
- Nome do Anexo
- IP de Origem
- Tamanho (MB)
- Mensagem Entregue (Se foi entregue ou não)
- Regra de SPAM
- Regra de Controle Avançado
- Regra de DLP (caso tenha regra de DLP criada)

Também deve indicar o prazo de busca (Data inicial e data final).



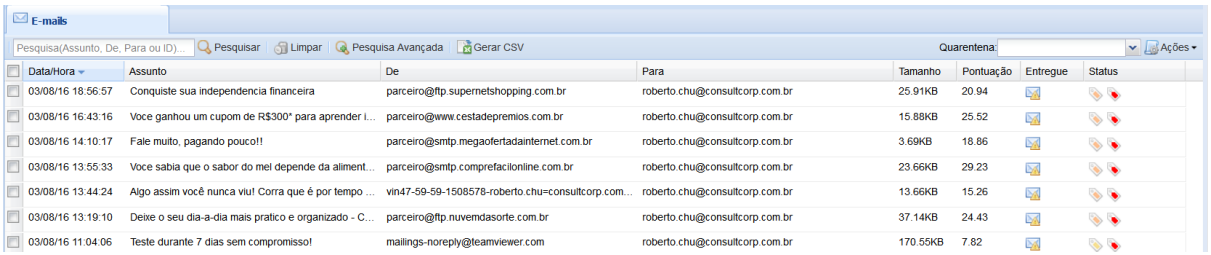
É ainda possível refinar mais ainda indicando Status da mensagem, através de operador lógico.



Após indicado os filtros, basta clicar em Aplicar. No exemplo, foram aplicados os filtros:

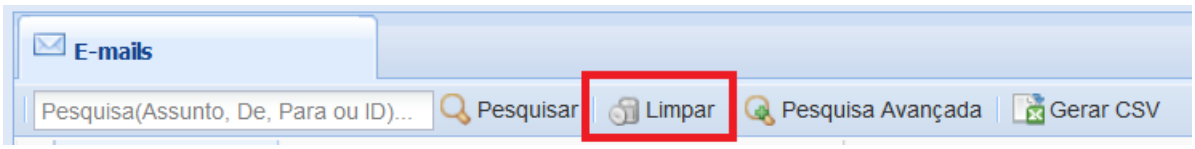
- Mensagens da data de 03/08/2016;
- Em Quarentena

Foi retornado somente os e-mails do dia 03/08/2016 que estavam em quarentena.

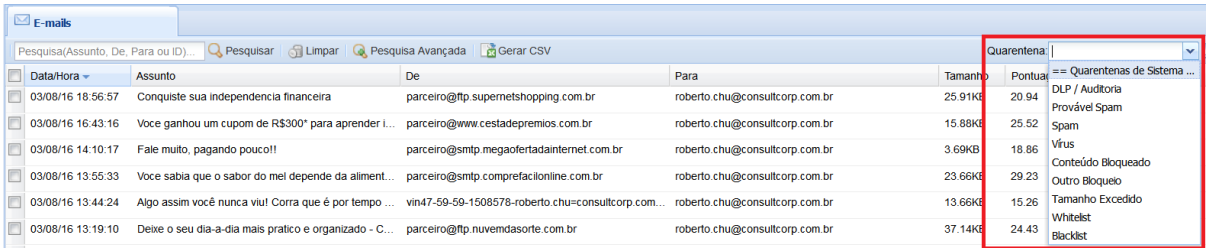


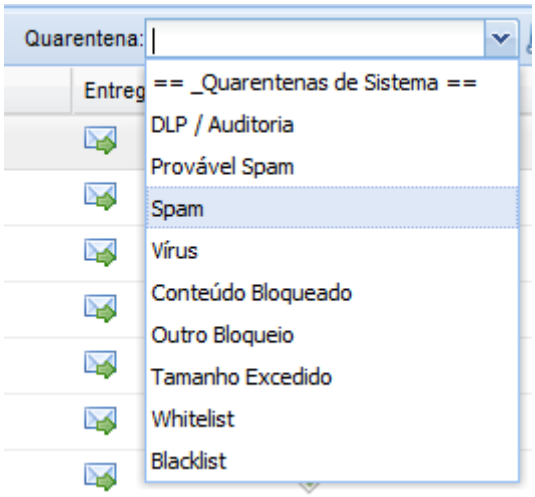
Retirada de filtro de pesquisa

Para apagar algum filtro aplicado, basta clicar no botão Limpar



Seleção por tipo de quarentena de email





Você pode escolher visualizar os e-mails em relação ao tipo:

DLP/Auditoria: São os emails considerados limpos, ou seja, os que foram entregues.

Provável SPAM: São os que possuem pontuação para serem considerados provável spam, mas não atingiram a pontuação para serem considerados SPAM.

SPAM: Emails que atingiram pontuação para serem considerados SPAM.

Vírus: Emails com anexos contaminados.

Conteúdo Bloqueado: Foi bloqueado por configuração efetuada no anti-spam. Alguma customização de bloqueio (dê duplo clique sobre o email para verificar o motivo do bloqueio).

Outro Bloqueio: Foi bloqueado por causas diversas (dê duplo clique sobre o email para verificar o motivo do bloqueio).

Tamanho Excedido: O email passou do tamanho máximo dele. O tamanho calculado, inclui imagens, anexos, etc.

Whitelist: Filtragem pelo que foi classificado como Whitelist

Blacklist: Filtragem pelo que foi detectado na Blacklist

Ações sobre email

Você pode tomar uma série de ações sobre o email, conforme imagem abaixo. Basta marcar o email e clicar no botão Ações.

Reenviar email: Libera o email bloqueado

Solicitar Liberação: Envia aviso ao administrador para solicitar liberação do email bloqueado. Esse processo é para emails que foram bloqueados por causa de vírus encontrado ou outro tipo de bloqueio que não seja por spam (por exmeplo email continha conteúdo proibido, definido pelo administrador).

Marcar como confiável: Basicamente é colocar o email/IP/Dominio em Whitelist (os próximos emails vindo deste remetente/IP/domínio, será liberado de verificação de SPAM)

Marcar como indesejável: Basicamente é colocar o email/IP/Dominio em Blacklist (os próximos emails vindo deste remetente/IP/domínio, será automaticamente bloqueado)

Libere Todas Mensagens: É o mesmo que Reenviar Mensagem, mas para múltiplas mensagens (que você pode marcar previamente na Checkbox).

Importante lembrar:

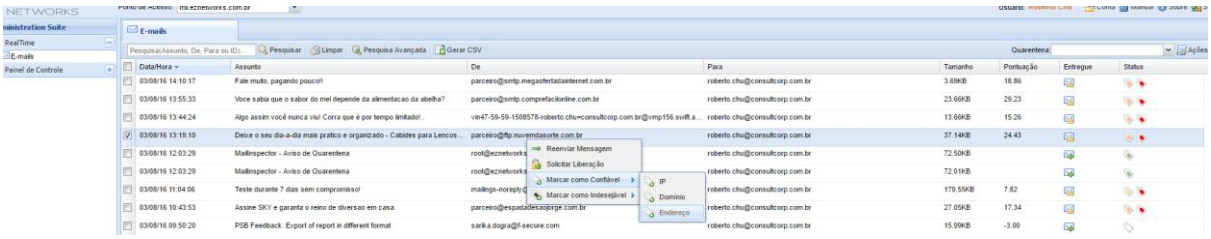
A Whitelist e Blacklist aplicados a nível de administrador do domínio, será aplicado a todo domínio indicado ou a todos domínios gerenciados. Não é individual. No caso de White e blacklist individual, terá que ser a nível de usuário.

Também é IMPRESCINDÍVEL lembrar que a **WHITELIST tem precedência sobre a BLACKLIST**, isto é TODO e QUALQUER email que estiver na Whitelist será liberada, mesmo que também esteja marcado na blacklist.

Adicionando entrada na Whitelist:

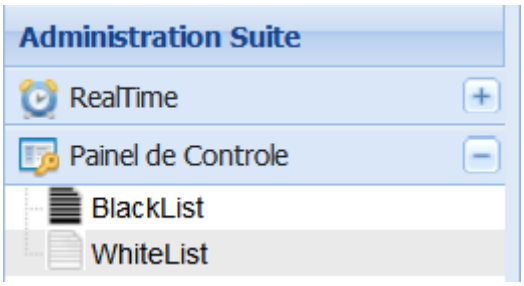
Existe dois jeitos e colocar email na Whitelist.

1. No painel de emails (RealTime > E-mails), selecione o email e clique em Ações ou o botão direito do mouse sobre o email selecionado.

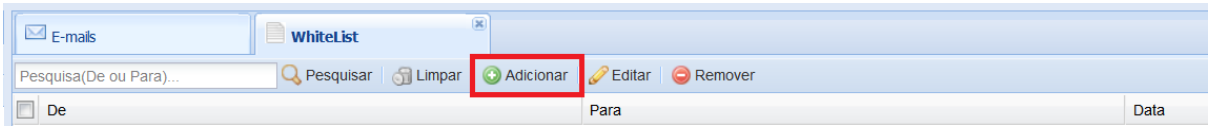


Selecione Marcar como Confiável e indique se você deseja inserir o email na Whitelist como IP/Domínio/Endereço.

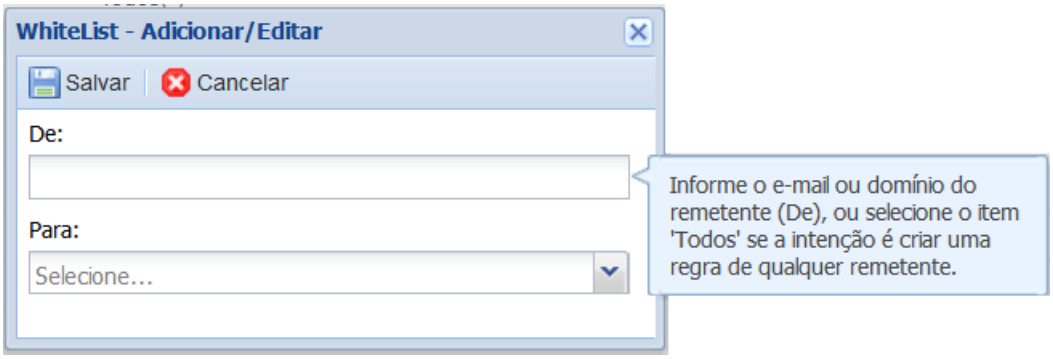
2. Através do Menu de Whitelist:
   Vá em Painel de Controle > Whitelist



Clique no botão Adicionar



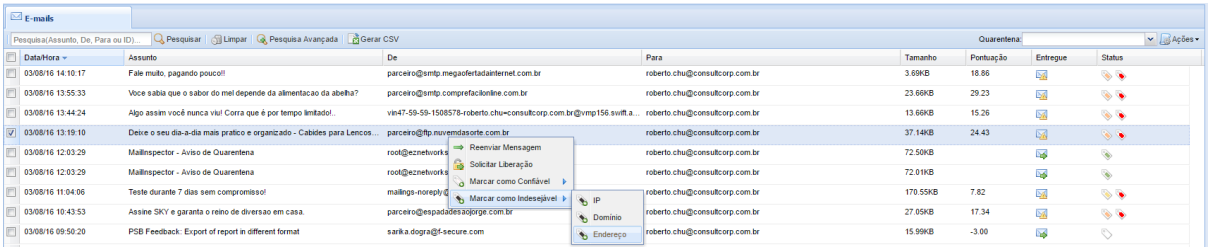
Selecione a origem (De:) e o destino (Para:)
Clique em Salvar



Adicionando entrada na Blacklist:

Existem dois jeitos e colocar email na Blacklist.

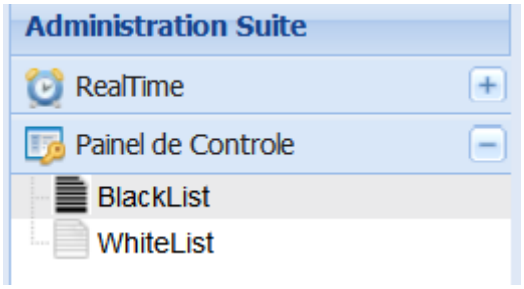
1. No painel de emails (RealTime > E-mails), selecione o email e clique em Ações ou o botão direito do mouse sobre o email selecionado.



Selecione Marcar como Indesejável e indique se você deseja inserir o email na Blacklist como IP/Domínio/Endereço.

2. Através do Menu de Blacklist:

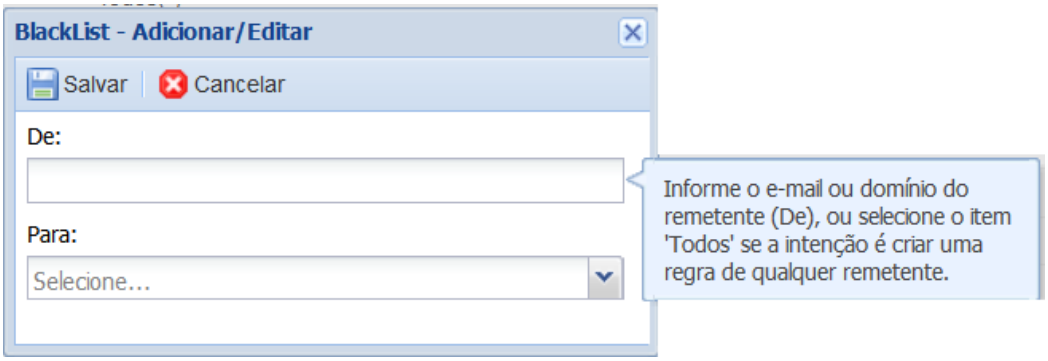
Vá em Painel de Controle > Blacklist



Clique no botão Adicionar

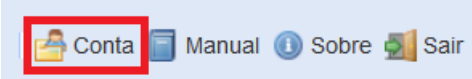
Indique a origem (De:) e o destino do email (Para:)

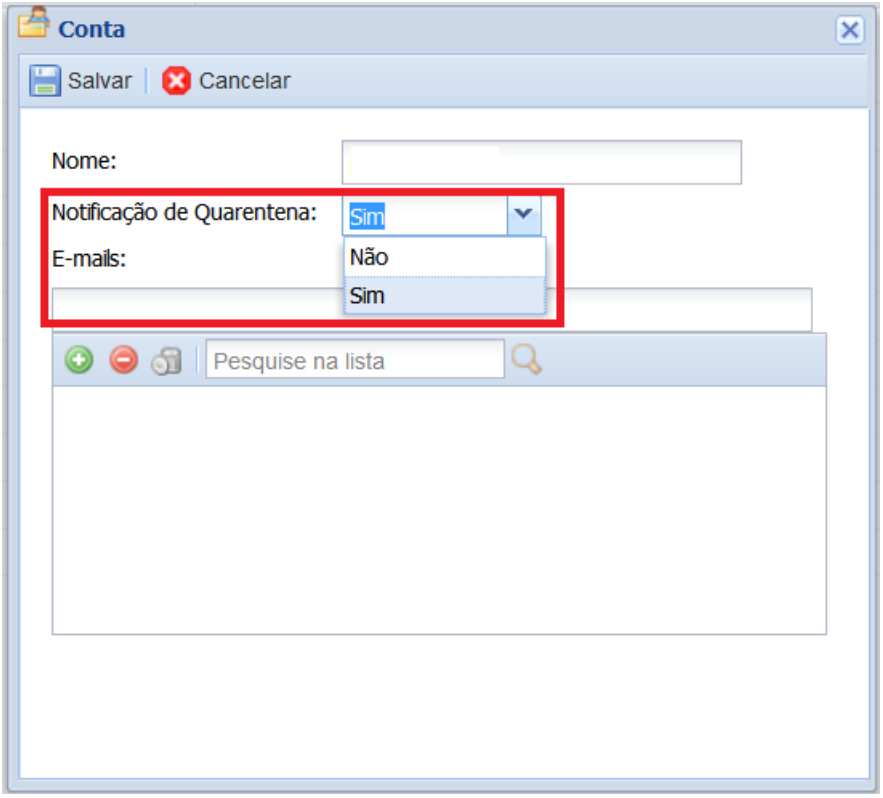
Clique em Salvar



Habilitar/Desabilitar o envio de Quarentena Individual

Você pode ativar ou desativar o envio do email de quarentena individual. Para isso vá em Conta (Canto superior direito do sistema de gerenciamento).





Na parte Notificação de Quarentena, selecione:

- Sim: Para que o email de aviso de quarentena seja enviado normalmente
- Não: Para parar o envio do email de notificação de quarentena individual.

Neste mesmo painel você ainda pode mudar o seu nome (é somente estético).

AVISOS DE QUARENTENA AO USUÁRIO FINAL

O que é Quarentena de usuário final (Digest)?

É um relatório enviado de tempos em tempos contendo a lista de e-mails que o anti-spam classificou como SPAM ou POSSÍVEL SPAM. Esse relatório é a quarentena do USUÁRIO, ou seja, as decisões tomadas somente afetarão o usuário e não TODO o domínio.

Qual a frequência do envio do aviso de Quarentena de usuário final?

A frequência do envio de notificação de quarentena individual, depende única e exclusivamente do administrador do sistema.

Como usuário final, é possível configurar se ocorrerá o envio, isto é, nas configurações do usuário, é possível ativar ou desativar este envio. Vide Habilitar/Desabilitar o envio de Quarentena Individual.

O email de Notificação de Quarentena Individual, lista o que tem de email retido (quarentenado), classificado como SPAM e/ou POSSÍVEL SPAM. Esses e-mails ficam na quarentena e pode ser liberado pelo próprio usuário. O que é SPAM para um usuário pode ser email útil para outro.

O menu da quarentena individual

Quarentena				
Data	De	Assunto	Pontuação	Ações

No menu, você verá cinco colunas:

- **Data:** Data e hora da entrada no email no sistema anti-spam.
- **De:** Quem mandou o email
- **Assunto:** Assunto pertinente ao email
- **Pontuação:** Qual a pontuação que o email recebeu. Importante lembrar que por default:
  - 10 pontos é considerado SPAM
  - Acima de 6 é considerado PROVÁVEL SPAM
- **Ações:** Indica as ações que você poderá fazer no email em quarentena
  - Liberar
  - Confiável
  - Não Confiável
  - Reportar

Ações possíveis sobre o email em quarentena

É possível marcar o email como confiável – **WHITELIST** (futuros e-mails do remetente não serão marcados como SPAM, mesmo que atinja a pontuação de SPAM) ou colocar o remetente em uma lista negra – **BLACKLIST** (ao qual futuros e-mails automaticamente serão barrados, mesmo que sejam e-mails válidos).

Segue abaixo exemplo do email do Digest (Quarentena individual):

Mail Inspector

Sistema Pessoal de Quarentena de E-mails

Os emails listados abaixo estão armazenados em sua quarentena pessoal. Utilize as opções da coluna "Ações" conforme necessário.

Quarentena

Data	De	Assunto	Tipo	Pontuação	Ações
11/01/2019 13:57	mailinspector@trt9.jus.br	biblioteca, a cota??o mais r?pida do Brasil com 30% de desconto	Spam	20.31	Liberar | Confiável | Não Confiável | Reportar
11/01/2019 13:57	mailinspector@trt9.jus.br	biblioteca Descoberto Nos Estados Unidos Um Alimento Estranho Que DerreteGordura em 24Horas !	Spam	16.25	Liberar | Confiável | Não Confiável | Reportar
11/01/2019 13:57	mailinspector@trt9.jus.br	biblioteca, a cota??o mais r?pida do Brasil com 30% de desconto	Spam	20.31	Liberar | Confiável | Não Confiável | Reportar
11/01/2019 13:57	mailinspector@trt9.jus.br	biblioteca, ex-BBB perde 8 quilos perdidos em apenas 4 semanas!	Spam	16.31	Liberar | Confiável | Não Confiável | Reportar
11/01/2019 13:57	mailinspector@trt9.jus.br	Descoberto Nos Estados Unidos Um Alimento Estranho Que Derrete Gordura em24Horas !	Spam	16.25	Liberar | Confiável | Não Confiável | Reportar
11/01/2019 13:57	mailinspector@trt9.jus.br	biblioteca, a cota??o mais r?pida do Brasil com 30% de desconto	Spam	20.41	Liberar | Confiável | Não Confiável | Reportar
11/01/2019 14:00	mailinspector@trt9.jus.br	[Exclusivo] Isso Leventa SEIOS em 30 Segundos!	Spam	17.30	Liberar | Confiável | Não Confiável | Reportar
11/01/2019 14:00	mailinspector@trt9.jus.br	OI? memorial, seu CPF ou CNPJ est?o sujos? Limpamos em at? 8 horas	Spam	13.78	Liberar | Confiável | Não Confiável | Reportar
11/01/2019 14:00	mailinspector@trt9.jus.br	sea Comece 2019 com CPF limpo. Informa??es neste e-mail.	Spam	14.08	Liberar | Confiável | Não Confiável | Reportar
11/01/2019 14:00	mailinspector@trt9.jus.br	Segue Curriculum Conforme Combinado. Grato.	Spam	13.46	Liberar | Confiável | Não Confiável | Reportar

Enviar informações de Blacklist/Whitelist | Solicitar um novo resumo da quarentena de e-mails | Acessar a quarentena

Para maiores informações entre em contato com o administrador da rede.

Powered by HSC MailInspector

Os links disponíveis no email são:

Liberar: Libera o email sem incluí-lo em whitelist ou blacklist.

Confiável: Coloca o remetente do email em uma whitelist (os próximos emails vindos deste remetente serão automaticamente liberados da verificação de SPAM).

Não confiável: Coloca o remetente do email em uma blacklist (os próximos emails vindos deste remetente serão automaticamente bloqueados).

Reportar: Reporta para HSCBRASIL o email quarentenado, como FALSO POSITIVO, isto é, email classificado erroneamente como SPAM/PROVÁVEL SPAM.

Outros links que tem no email de quarentena individual

Enviar informações de Black/Whitelist: Você receberá um email com a lista do que já foi inserido na lista de whitelist e na lista de blacklist por você no anti-spam.

Abaixo imagem do modelo de email de Whilist/Blacklist:

Gestão da Whitelist e Blacklist

Os registros abaixo fazem parte das suas listas de remetentes confiáveis e não confiáveis. Utilize o botão "Apagar" caso deseje remover determinado remetente de uma das listas.

Endereços confiáveis

Data	Remetente	Destinatário	Ação
Não existem registros			

Endereços não confiáveis

Data	Remetente	Destinatário	Ação
27/07/2018	return-conto-8krqyb@supernotadez.com.br	atendimento@hscbrasil.com.br	Apagar
27/07/2018	zdydtewfgpo@liseberg.se	atendimento@hscbrasil.com.br	Apagar

Para maiores informações entre em contato com o administrador da rede.

Powered by HSC MailInspector

Para excluir um remetente da whitelist/blacklist basta clicar no botão Apagar (Apagar).

Solicitar um novo resumo da quarentena de e-mails: Solicita novo digest (relatório de quarentena)

Acessar a quarentena: Acessa o sistema de gerenciamento da sua quarentena individual

Liberar email da quarentena individual

Se você quiser liberar um email da quarentena e que futuros e-mails enviados por esta conta de email passe direto, você deve efetuar os dois passos a seguir:

1. Clicar no link **Confiável**
2. Clicar no link **Liberar**

Dessa forma futuros e-mails deste mesmo remetente passarão a ser ignorados pelo módulo de análise de SPAM.

Importante salientar que é somente o módulo de anti-spam, o resto continua sendo avaliado, por exemplo se ele mandar no email um anexo com vírus, o email será barrado.