

Resolvendo Problemas de Métricas de Reputação do Email



Resolvendo Problemas de Métricas de Reputação do Email

Escrito por Dale Langley



Dale atua na Return Path para ajudar empresas a melhorarem suas taxas de entregabilidade de email e taxas de resposta, além de liderar o desenvolvimento de sistemas de email marketing, atendendo a clientes na Europa há mais de 7 anos.

Como desenvolvedor, Dale tem amplo conhecimento prático de como as empresas projetam sistemas e armazenam dados. Como consultor, entende como implementar uma arquitetura robusta, analisar dados, segmentar, desenhar e entregar para os melhores resultados possíveis.

Essa combinação de experiência significa que Dale sabe como resolver os problemas enfrentados pelos profissionais de Marketing responsáveis por aumentar suas listas de assinantes e maximizar o ROI.

Quem deve ler este eBook?



Iniciantes

Conteúdo Iniciante é destinado a profissionais de marketing iniciantes ou para aqueles que apenas precisam de uma reciclagem.



Intermediário

Conteúdo intermediário é destinado a profissionais de marketing com alguma experiência no assunto, incluindo estratégias e táticas.



Avançado

Conteúdo avançado é para os profissionais de marketing que têm um nível avançado de compreensão do email marketing e estão à procura de estratégias e táticas avançadas.

Este e-book:



Produtos Return Path



Placement.EQ

Maximize a entrega em caixa de entrada com precisão superior e visibilidade dos dados de assinantes ativos, listas de seeds e reputação de envio.



Certification.EQ

Aumente o impacto na caixa de entrada, aumentando a velocidade de entrega e evitando o bloqueio do email com a whitelist mais respeitada da indústria.



Insight.EQ

Faça do seu programa de email o melhor da indústria, vendo como os assinantes se envolvem com a sua marca, como o conteúdo renderiza e comparando as principais métricas lado a lado com concorrentes e benchmarks.



Protect.EQ

Proteja seus usuários e sua marca, ganhando visibilidade total do tráfego de email conhecido, desconhecido e potencialmente fraudulento.



Secure.EQ

Mantenha a confiança em sua marca por meio do monitoramento e bloqueio de phishing e integrando as mais recentes informações sobre ameaças de email em seu programa de segurança.



Serviços Profissionais

Soluções de consultoria personalizadas de especialistas em Email Intelligence que impulsionam o desempenho do email, geram resultados mensuráveis e melhoram o seu ROI.



Conteúdo:

Aumento no número de reclamações de assinantes	Pág 5
Spam traps no mailing	Pág 6
Taxas de Devolução em Provedores de email específicos	Pág 7
Elevado número de hard bounces de “usuários desconhecidos” (> 10%)	Pág 8
Falha repentina de DNS reverso	Pág 9
Os endereços IP são listados em blacklists	Pág 10
Aumento de emails rejeitados	Pág 11
Autenticação DKIM está falhando	Pág 12
Aumento das mensagens filtradas para a pasta de spam	Pág 13



O que está acontecendo



Aumento no número de reclamações de assinantes

Possível causa

- Políticas de Permissão ruins
- Mudança na frequência
- Servidor de email comprometido
- A fonte de aquisição da lista é ruim

Próximos passos...

1. Cadastre-se ou certifique-se de que está inscrito em todos os feedback loops (ISP FBLS), que incluem: Yahoo!, Microsoft / Outlook.com (chamado JMR), AOL, Comcast, Cox, BlueTie, United Online / Netzero / Juno (UOL), Rackspace (Mailtrust), Road Runner, OpenSRS (Tucows) e USA.net.
2. Estas contagens de reclamações podem ser usadas ao longo do tempo para identificar possíveis problemas com suas práticas de envio. As rápidas mudanças no número de reclamações que não correspondem aos seus volumes de disparo ou escalonamentos ao longo do tempo são indicadores de um problema de reclamações, que pode afetar sua entregabilidade e devem ser abordados.
3. Use um cabeçalho List-Unsubscribe para ajudar a facilitar os pedidos de descadastramento nos provedores de email que usam o cabeçalho. Por exemplo, enquanto o Gmail não oferece um feedback loop, vão perguntar a seus assinantes se eles gostariam de descadastrar quando relatam seu email como spam - mas só se você tiver um cabeçalho list-unsubscribe. Leia mais sobre o Gmail e o cabeçalho list-unsubscribe neste [guia](#).
4. Monitore as fontes de aquisição de lista que geram o maior número de reclamações, e implemente formas de reduzi-las ou remova essas fontes completamente. Fontes comuns de aquisição de lista incluem a aquisição paga, listas afiliadas e formulários web de parceiros.
5. Faça auditoria em seus servidores SMTP para verificar open relays e impeça que terceiros explorem e enviem email através deles.



O que está acontecendo



Spam traps no mailing

Possível causa

- Muitos inativos no arquivo
- Estratégia de email para inativos inexistente ou ineficaz
- Enviar raramente para toda lista
- Más práticas de aquisição de lista

Próximos passos...

Verifique os seus pontos de aquisição para se certificar de que está validando os endereços de email cadastrados. Considere pedir para assinantes inserirem seu endereço de email duas vezes para evitar erros de digitação. Também avalie verificar o domínio do endereço de email em tempo real, usando scripts ou serviços de validação.

Depois que os dados entram em sua lista, certifique-se de enviar um email de boas-vindas e confirmação e remova quaisquer bounces imediatamente. Verifique se o seu email de boas-vindas permite que os destinatários cancelem a inscrição, apenas no caso de um endereço de email incorreto ter sido cadastrado no ponto de de aquisição.

Por último, verifique se você está executando as boas práticas de higiene de lista e está removendo tanto bounces quanto endereços inativos.

O que está acontecendo



Taxas de Devolução em Provedores de email específicos

Possível causa

- Endereço IP com pouco ou nenhum histórico de envio
- Configurações incorretas de conexão / throughput
- ISP emprega técnicas de greylisting
- Excedeu nível aceitável de usuário desconhecido ou taxa de reclamação

Próximos passos...

Consulte o código específico localizado dentro de seus registros de bounce. Esta informação pode dizer especificamente qual o seu problema e como resolvê-lo. Se você estiver enviando a partir de um novo endereço IP, é necessário aquecer este endereço IP através do envio de pequenos volumes e aumento gradativo do volume, mantendo as reclamações e usuários desconhecidos no mínimo.

Se as devoluções se devem à reclamações, consulte a seção Complaints. Se as devoluções resultam da existência de muitos usuários desconhecidos, consulte a seção Unknown User.

O que está acontecendo



Elevado número de hard bounces de “usuários desconhecidos” (> 10%)

Possível causa

- Envio para uma lista antiga ou ruim
- Envio de email para uma lista de opt-out
- Provedor de Email está desativando endereços de email inativos ou antigos

Próximos passos...

Um código de erro de usuário desconhecido é gerado quando um remetente envia um email para um endereço que não existe mais. Isto pode acontecer porque o endereço de email nunca existiu, não está mais ativo por opção, ou foi abandonado pelo usuário final.

Quando os provedores de email observam uma alta taxa de usuário desconhecido num endereço IP, eles podem suspeitar que está ocorrendo um “ataque de dicionário” ou que o remetente não tem práticas sólidas de higiene de dados. Um ataque de dicionário é quando um spammer usa combinações de palavras no dicionário para criar combinações aleatórias de endereços de emails e depois dispara spam para esses endereços, com a finalidade de encontrar endereços de email válidos. Esses endereços são então recolhidos, vendidos e recebem mais spam. Para evitar mais usuários desconhecidos, você deve:

1. Verificar se o seu sistema de processamento de bounces está funcionando e removendo bouncebacks de usuário desconhecido imediatamente.
2. Enviar email para todos os seus usuários de email pelo menos uma vez por trimestre.
3. Envie uma amostra para listas antigas ou opt-out antes de enviar para todos a fim de mensurar o nível de risco.



O que está acontecendo



Falha repentina de DNS reverso

Possível causa

- O servidor DNS está inoperante
- Problemas de conectividade de rede
- Uma alteração incorreta de seu registro de DNS foi feita

Próximos passos...

1. Validar que o seu DNS está acessível através das ferramentas da Return Path, MX Toolbox ou DNS Stuff.
2. Entre em contato com o engenheiro de rede para verificar se foram feitas alterações em seu DNS e para verificar se o host DNS não está enfrentando problemas de conectividade.



O que está acontecendo



Endereços IP são listados em blacklists

Possível causa

- Spam traps foram adicionados à sua lista de email
- Não Processamento de Reclamações ou Bounces

Próximos passos...

A blacklist é uma lista de endereços IP que ISPs, empresas de filtragem de spam ou organizações anti-spam criam e mantêm para ajudar com a filtragem ou bloqueio de spam. O proprietário da blacklist publicará a lista e permitirá que outras organizações a utilizem para ajudá-los a filtrar ou bloquear email. Para garantir a entregabilidade do email, é importante manter-se fora de blacklists amplamente utilizadas como Spamhaus, SpamCop, CBL e a blacklist Return Path.

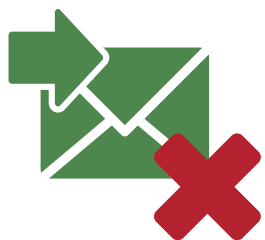
Um endereço IP pode estar listado em uma blacklist quando um email enviado atinge uma spam trap (consulte a seção spam traps) ou gera reclamações de usuários finais (consulte a seção Complaints).

Se um proprietário de blacklist observa o atingimento frequente de spam traps e/ou reclamações, pode colocar o endereço IP em sua blacklist.

Para algumas blacklists, a inclusão se baseia em falhas de infraestrutura, como open relay. Para evitar a inclusão nessas blacklists, certifique-se de que a infraestrutura de implantação esteja seguindo as melhores práticas e padrões da indústria.



O que está acontecendo



Aumento de emails rejeitados

Possível causa

- Um provedor de email incluiu seu endereço IP de envio numa blacklist
- O seu endereço de IP apareceu em uma blacklist
- Você está enfrentando problemas de reputação com as reclamações, spam traps e/ou usuários desconhecidos

Próximos passos...

Uma queda repentina na entregabilidade geralmente indica uma mudança em suas práticas de envio, então pense sobre o que mudou na sua empresa recentemente.

Você mudou de fornecedor de hospedagem para seu site ou domínios corporativos? Se sim, todas as entradas DNS para a sua autenticação de email atual estão corretas?

Você lançou templates com novo design, como parte de um exercício de rebranding ou uma atualização de conteúdo? Se você vai passar por esse processo, deve testar novos modelos para garantir que as suas taxas de resposta não caiam. Se os assinantes não reconhecerem a marca ou linguagem usada em seus emails, é provável que não engajem com o seu conteúdo, o que é uma má notícia para a entrega em caixa de entrada.

Você incluiu um novo grupo de dados à sua lista recentemente, talvez como parte de uma aquisição ou uma tentativa de reconquistar assinantes antigos? A qualidade destes dados vai afetar sua capacidade de chegar à caixa de entrada da lista inteira, portanto fatores como higiene de dados e engajamento do assinante devem ser priorizados quando passar por este processo.

Depois de identificar a mudança que contribuiu para uma queda na entrega em caixa de entrada, você pode colocar um plano em prática para lidar com isso.

O que está acontecendo



Autenticação DKIM está falhando

Possível causa

- Checar comprimento da chave
- Chave pública inválida / inexistente

Próximos passos...

Embora as chaves de 512 bits estejam sendo usadas por um tempo, elas já não são recomendadas devido a uma facilidade com que podem ser hackeadas. Mais tarde, em 2012, o Gmail começou a recusar emails assinados com chaves de menos de 1024 bits.

Também é possível que você tenha um problema com o que é conhecido como chave pública. Este é um registro de DNS que é “emparelhado” com o hash incluído no email de saída para validar seus fluxos de email. Parte da chave pública é uma sequência de caracteres aleatórios, se você copiou isso de um gerador de registro DKIM em seu DNS, é possível que possa haver alguns caracteres inválidos no registro.

Dependendo do seu host DNS, você também pode descobrir que certos caracteres de escape são necessários ao adicionar o registro, verifique com seu provedor se você não tiver certeza de como atualizar seu registro. Finalmente, se você quiser testar seus registros, envie um email de seu domínio assinado com DKIM para checkmyauth@auth.returnpath.net e você receberá um relatório detalhando todos os problemas.



O que está acontecendo



Aumento das mensagens que estão sendo filtradas para a pasta de spam

Possível causa

- Um aumento no número de reclamações, spam traps ou usuários desconhecidos
- Falta de programa de win-back
- Faltam feedback loops
- Palavras-chave de spam ou estrutura da mensagem de emails estão falhando nas verificações de filtros de spam

Próximos passos...

Ter uma queda no engajamento do assinante pode realmente afetar sua capacidade de chegar à caixa de entrada, é importante, portanto, tentar voltar a engajar esses assinantes antes que se tornem um problema. Você deve saber definir o que é um assinante inativo, esta definição varia de empresa para empresa e depende da compreensão do ciclo de vida do seu cliente.

Depois de ter esta definição, tente trabalhar com o que vai voltar a engajá-los. Talvez seja um benefício adicional ou oferta especial, poderia ser o conteúdo ou informações mais relevantes, que não podem obter em nenhum outro lugar. Você também deve saber quando abandonar, se alguém realmente se converte em usuário desengajado, em seguida, enviar-lhes mais e mais emails não vai reconquistá-los, é provável que os faça apertar o botão "Spam", que poderia ser muito pior do que apenas deixá-los ir.

Se alguém está marcando seu email como spam ou lixo eletrônico, então é importante ter certeza de que você não está mais enviando email a estas pessoas. Seu email não só será filtrado para a pasta Lixo, como sua capacidade de entrega como um todo irá cair. Então, certifique-se de que você está inscrito em todos os feedback loops disponíveis para que o ISP envie notificações de reclamações, de modo que você possa remover os assinantes da sua lista. Existem alguns requisitos para a aceitação em feedback loops (FBLS) que envolvem adoção de melhores práticas, como SPF, DKIM e reputação de IP, mas os requisitos são facilmente alcançados pela maioria dos profissionais de Marketing.

Sobre a Return Path

A Return Path é líder mundial em Email Intelligence. Nós analisamos mais informações a respeito de emails do que qualquer outra empresa no mundo e usamos os dados para reforçar os produtos, garantindo que somente os emails que os destinatários desejam receber cheguem à caixa de entrada. Nossas soluções de Email Intelligence, líderes de mercado, utilizam o mais abrangente conjunto de dados do mundo para maximizar o desempenho e a responsabilidade de cada email, além de construir relações de confiança por todo ecossistema de email e proteger os usuários contra spam e outros abusos. Como consequência, ajudamos a construir melhores relacionamentos com seus clientes e a aumentar seu ROI e, ao mesmo tempo, damos suporte aos ISPs e outros provedores de serviços de email para aumentar o desempenho das redes e incrementar a retenção de clientes. Informações sobre a Return Path podem ser encontradas em:

br.returnpath.com

Canadá

rpinfo-canada@returnpath.com

Estados Unidos

rpinfo-uk@returnpath.com

Alemanha

rpinfo-germany@returnpath.com

França

rpinfo-france@returnpath.com

Estados Unidos

rpinfo@returnpath.com

Brasil

rpinfo-brazil@returnpath.com

Austrália

rpinfo-australia@returnpath.com



