pmweb

Guia de Entregabilidade

2022

pmweb

Relacionamentos únicos em escala

2022

Guia de Entregabilidade

Desenvolvido pelo setor de
Entregabilidade da Pmweb.

pmweb

Índice

1. Entrega e entregabilidade

Antes de começarmos, primeiro precisamos compreender a diferença entre **entrega e entregabilidade**.

Entrega

A entrega se refere ao **e-mail que sai da ferramenta de disparo e chega ao provedor**. Logo, esse e-mail pode ir para a caixa de entrada ou para a caixa de spam, sem retornar como bounce. Essa métrica é fornecida pelo **ESP** *(Email Service Provider)*, com isso, o e-mail enviado com erro é subtraído na contabilização.

Entregabilidade

Já a entregabilidade, é o **gerenciamento do disparo do e-mail para que ele chegue à caixa de entrada do usuário**. Entretanto, até que isso aconteça de fato, o e-mail passa por várias etapas, e tudo o que acontece durante o percurso pode influenciá-lo. A métrica de entregabilidade pode ser definida pelo número de e-mails que caem na caixa de entrada dividido pelas entregas realizadas.

Vale ressaltar que uma boa taxa de entrega não significa que a entregabilidade também esteja, pois a entrega do e-mail é apenas uma parte de todo o processo. Porém, com uma boa taxa de entregabilidade, certamente a entrega também estará.

2. Autenticações necessárias para evitar problemas de envios

Realizar o disparo de e-mails exige uma série de questões **estratégicas e técnicas**. Para iniciar os envios, são necessárias algumas autenticações que funcionam como documento de identificação para os provedores. Ao apresentar essa "prova" de identificação, o e-mail não será confundido com *spammers*.

As autenticações necessárias são:

SPF (Sender Policy Framework)

Responsável por certificar o IP que fará o envio do e-mail através de um determinado domínio. O **SPF** **checa e confirma a identidade de quem fará o disparo**, assim como avalia se o e-mail from é válido. Logo que a mensagem chega ao provedor, ele verifica no domínio se o IP está autorizado a realizar o envio.

DKIM (Domain Keys Identified Mail)

Um mecanismo de validação que permite o remetente **transmitir uma mensagem ao destinatário**. O **DKIM** adiciona os envios em uma chave pública, que é verificada pelos provedores no momento em que o e-mail chega até eles, assim ele confirma a autenticidade do disparo pelo cabeçalho do e-mail.

DMARC (Domain-Based Message Authentication, Reporting and Conformance)

Reforça a **segurança e a proteção** realizando o **relatório e diagnóstico sobre a legitimidade do remetente**, com base nas duas autenticações anteriormente mencionadas (SPF e DKIM). Através do **DMARC**, facilmente conseguimos ter feedbacks de possíveis e-mails falsos, mantendo a reputação do domínio e garantindo a **boa entregabilidade dos e-mails**.

3. O que é reputação?

O trabalho da entregabilidade é “convencer” os provedores de que o IP e o domínio são bons remetentes e merecem entregar e-mails na caixa de entrada do usuário. Contudo, para conquistar essa confiança é preciso realizar um trabalho cuidadoso de acordo com o que é exigido por eles. Quando conseguimos cumprir as exigências dos ISPs e vemos boas métricas, pode-se dizer que conquistamos uma boa reputação.

A reputação é a forma do provedor reconhecer o remetente como legítimo. É difícil de criar, fácil de perder e deve ser trabalhada ao longo do tempo. Várias métricas de e-mail marketing podem influenciar para que uma reputação seja boa ou ruim.

Abaixo, listamos as métricas que podem **influenciar positivamente e negativamente na reputação do remetente**:

Métricas de influência positiva

Entrega | **Inbox** | **Open Rate** | **CTR** | **CTO**

Métricas de influência negativa

Soft Bounce | **Hard Bounce** | **Spam Complaint** | **Spam Trap** | **SNDS**

Até agora vimos que diversos fatores podem **contribuir ou dificultar** todo o processo dos e-mails, e não apenas influenciar em taxas altas ou baixas. Os provedores adotam critérios de avaliação de reputação que não são possíveis de mensurar, como por exemplo, quando o usuário marca um e-mail como lido sem de fato ter aberto. Não é possível saber quantos usuários fazem isso em uma campanha, mas os provedores usam esse tipo de informação para entender o comportamento do remetente.

Essa é uma ação do usuário que pode afetar negativamente a reputação do remetente, assim como outras que também **não são possíveis mensurar: adicionar aos remetentes confiáveis (positiva), responder o e-mail (positiva) e deletar sem abrir (negativa).**

Se não é possível mensurar alguns critérios, como saber se a reputação está boa?

Existem dois serviços muito importantes nas análises de entregabilidade que auxiliam na leitura da reputação: o **SNDS (Smart Network Data Service) e o GPT (Google Postmaster Tools)**.

Veja como cada um deles atua e contribui na verificação de reputação:

SNDS (Smart Network Data Service)

Fornece dados de reputação de IP, exclusivamente de provedores **Microsoft (Outlook, Hotmail, Live e MSN)**.

GPT (Google Postmaster Tools)

Oferece dados sobre reputação de IP e domínio, taxas de spam, erros de entrega, entre outros dados exclusivos de Gmail.

Ambas são ferramentas extremamente úteis e de uso nas rotinas diárias de análise. Parte dos dados de SNDS e GPT completam informações de Open Rate, CTR e assim por diante. **Com o entendimento de todas as métricas, dos comportamentos não mensuráveis e dos dados fornecidos pelas ferramentas de reputação, conseguimos entregar um diagnóstico de E-mail Deliverability.**

4. Aquisição

Conhece a citação **“os fins justificam os meios”**? Essa citação se tornou uma frase clássica, mas que se adequa quando o assunto é e-mail marketing. Boa parte do trabalho assertivo de entregabilidade, onde o maior interesse é que o e-mail chegue à caixa de entrada do usuário, passa pela qualidade dos endereços que serão usados nas campanhas. Quando falamos em qualidade, nos referimos a endereços que não sejam devolvidos como soft ou hard bounce, que não sejam de usuários com status de opt-out ou que não estejam diretamente ligadas à marca que está enviando a comunicação. Por essa razão, o resultado começa lá atrás, ainda nos meios de aquisição de e-mail.

Existem várias formas diferentes de captação de e-mail, mas todas devem seguir as mesmas regras: **solicitar a permissão do usuário para enviar e-mails** (opt-in: é a permissão prévia concedida pelo destinatário e comprovável pelo remetente, autorizando o envio de e-mail marketing) e **informar o que será enviado a partir de então**.

Confira os **três métodos** mais comuns entre as empresas que adotam boas práticas na captação de e-mail:

1. Double Opt-in (alta segurança)

Nesse método, o usuário entra no site, insere seu endereço de e-mail no campo indicado e envia. Depois, recebe uma mensagem de ativação com um link para confirmar sua inscrição e assim, passa a receber os e-mails da marca.

2. Single Opt-in (média segurança)

O processo inicial é parecido com o Double Opt-in, onde o usuário entra no site da marca e insere seu endereço de e-mail. Quando clica em enviar, automaticamente se torna opt-in, sem receber uma mensagem com link de confirmação.

3. Soft Opt-in (baixa segurança)

Essa é uma forma implícita de conseguir crescer a base de e-mails, onde o mais comum são os envios de comunicações empresariais, considerando que já exista um relacionamento pré-estabelecido entre as partes. Segundo o **CAPEM**, soft opt-in é o envio de mensagens sem opt-in, porém sempre a partir da prévia e comprovável relação comercial ou social entre remetente e destinatário. Além disso, existe a LGPD (Lei Geral de Proteção de Dados) onde exige que as comunicações sejam enviadas apenas com a autorização e consciência do usuário.

As formas de aquisição de e-mails não precisam necessariamente ser pela internet com campos de inscrição nos sites. É possível captar esses dados em eventos, feiras, palestras, sorteios, entre outros. Todavia, dificilmente teremos a garantia de que esses endereços serão fornecidos da forma correta, a fim de reduzir o número de hard bounces. A partir do momento em que uma pessoa precisa escrever seu e-mail, sem nenhum tipo de validação, pode haver erros.

Existem no mercado uma série de ferramentas para validar endereços de e-mail, que basicamente verificam a existência da conta extraindo os registros MX e se conectando com o endereço via SMTP, simulando um envio real. Isso reduz significativamente as chances das listas possuírem endereços nocivos à reputação. Entretanto, o resultado nunca será 100% positivo, pois nem todos os ISPs colaboram com o fornecimento dessas informações.

5. IP dedicado e compartilhado

Quais as diferenças entre IP dedicado e compartilhado? O IP dedicado é exclusivo para o subdomínio do cliente, com isso, é possível controlar e monitorar o IP para que a sua reputação não seja afetada.

O IP compartilhado é utilizado para mais de 1 subdomínio, ou seja, o risco de afetar a reputação do IP é maior, já que não é controlado e monitorado de forma exclusiva.

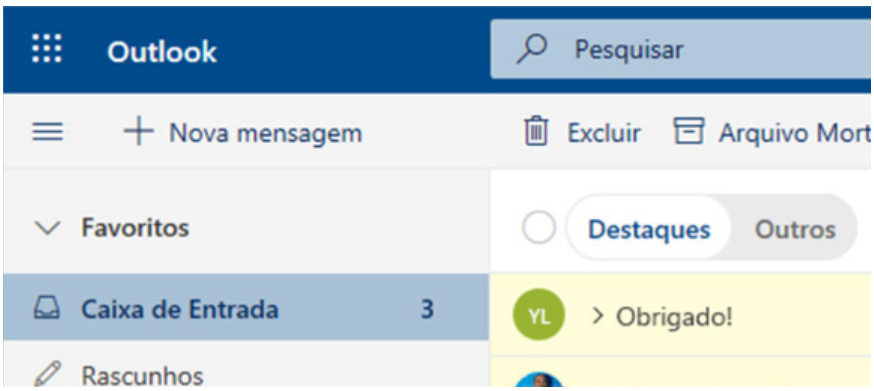
6. Internet Service Provider (ISP)

Um ISP é um provedor de internet que oferece vários serviços como conteúdo, notícias, hospedagem de sites, blogs e e-mail. Existem vários ISPs no mercado que oferecem o serviço de e-mail, cada um com sua própria característica e exigência para fornecer o melhor serviço ao cliente.

Os três principais ISPs são **Outlook (Microsoft), Gmail (Google) e Yahoo (Apollo)**, por se tratar de serviços de e-mail antigos e possuírem muitos usuários pelo mundo, o que é muito importante para estratégias de entregabilidade. A seguir, confira as características de cada um deles:

1. Outlook

O Hotmail foi lançado em 1996 pela Microsoft, passando a ser o domínio de maior expressão e dominando rapidamente o mercado global. Em 2013 passou a ser chamado Outlook.com. Desde 2017, a Microsoft consolidou todos os e-mails em uma só plataforma, inserindo os domínios @hotmail, @outlook, @msn e @live dentro das mesmas regras internas da Microsoft de reputação e regras antispam. Hoje, o Outlook oferece aos seus usuários uma categorização da caixa de entrada, onde o provedor divide entre “Destaques” (e-mails promocionais que o usuário mais interagiu) e “Outros” (e-mails promocionais e transacionais que não tem tanta aderência dos seus usuários).



O Outlook oferece algumas ferramentas úteis para análise de reputação:

Postmaster

Esse recurso auxilia os remetentes em questões relacionadas a problemas com as entregas. Quando isso acontece, a Microsoft fornece um formulário onde deve ser preenchido com os detalhes do caso, e após a análise, retornam com as orientações para o chamado aberto. Além disso, sempre apresentam todas as políticas e diretrizes de envio.

Políticas e Diretrizes de Envio

São procedimentos que visam proteger os usuários contra e-mails abusivos, indesejados ou mal-intencionados. O rigor contra spam é uma medida de garantia para que os remetentes sigam as diretrizes do Outlook e protejam as caixas de e-mail dos usuários.

Feedback Loop (FBL)

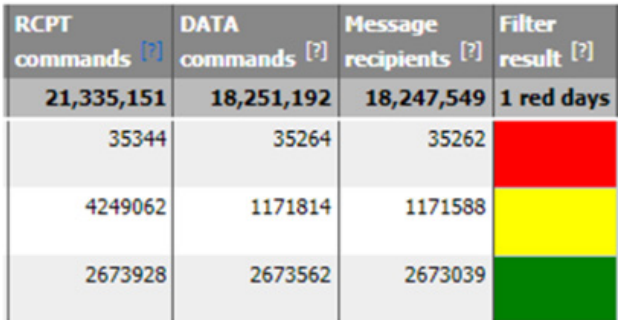
Quando o usuário marca o e-mail como spam, o remetente recebe essa informação do ISP informando qual endereço fez a reclamação. Essa informação é útil para retirar o endereço de e-mail das audiências e cancelar a assinatura da base. Além de mostrar quem fez a reclamação, os FBLs informam sobre problemas de segurança que os IPs possam apresentar, com ID de campanhas e header da mensagem.

Junk Mail Reporting Program (JMRP)

Um programa do Outlook que fornece informações sobre usuários que marcam as mensagens como lixo ou phishing. Essas informações partem de marcações de e-mail como spam, ou encaminhamentos diretos para a pasta de spam ou lixo eletrônico.

Smart Network Data Services (SNDS)

É um serviço gratuito prestado pelo Outlook que fornece informações sobre como os usuários classificam o remetente. Esses dados são apresentados de forma bastante visual, classificando o IP com status de reputação alta (verde), média (amarela) e baixa (vermelha). A definição de como o IP será classificado depende de uma série de fatores, como marcações spam, trap hits e engajamento, dentro daquele período de atividade.



RCPT commands [?]	DATA commands [?]	Message recipients [?]	Filter result [?]
21,335,151	**18,251,192**	**18,247,549**	**1 red days**
35344	35264	35262	
4249062	1171814	1171588	
2673928	2673562	2673039	

Além disso, a Microsoft também disponibiliza a opção de suporte, onde é possível enviar qualquer tipo de solicitação ou dúvida para os serviços do Outlook.

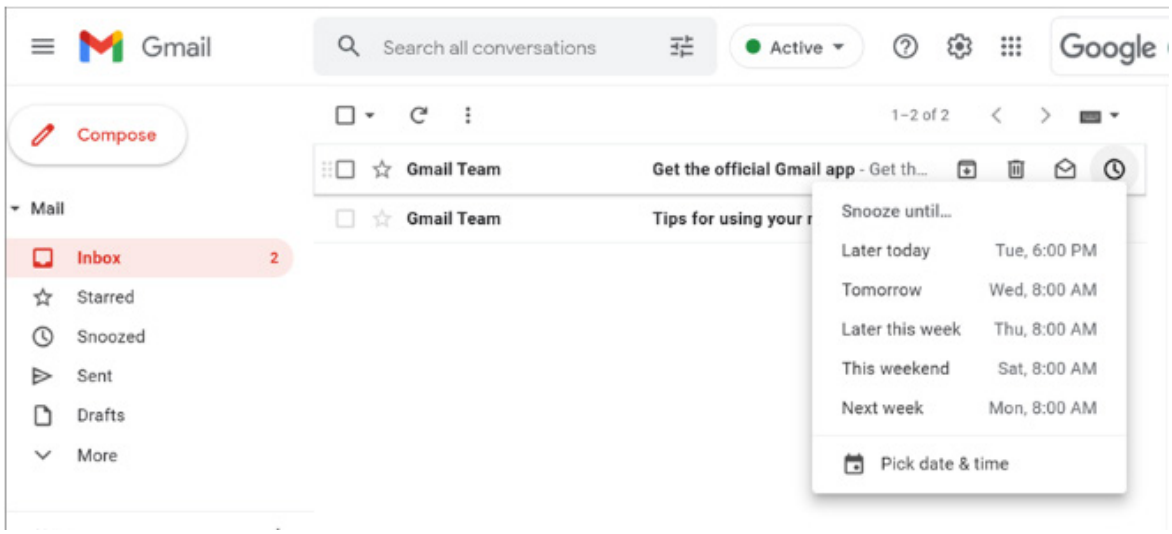
2. Gmail

O Gmail foi anunciado pelo Google oficialmente em 1º de abril de 2004 e venceu seus concorrentes da época (Hotmail e Yahoo) logo na sua criação. Ficou em versão beta até 2009, quando foi anunciado o fim do período de testes.

Em 2012 o Gmail tornou-se o provedor de e-mail mais usado na internet, ultrapassando a marca de 2 bilhões de usuários por mês em 2020. A integração com o Google e com vários recursos como calendário, tarefas, vídeos-chamadas, telefonemas, armazenamento em nuvem, personalização de prioridade de mensagens, entre outros, faz o Gmail ser hoje um dos melhores serviços de e-mail para o usuário.

O Gmail também possui o Feedback Loop para fornecer dados sobre as reclamações de spam dos usuários. A segurança adotada por essa plataforma funciona da seguinte maneira: o remetente precisa assinar o domínio como propriedade e verificar na ferramenta de postmaster, assim, obtém acesso ao FBL. Além disso, existe uma segmentação de mensagens, que facilita a localização dos e-mails na caixa de entrada e na pasta de spam.

As mensagens são classificadas da seguinte forma:



As mensagens são classificadas da seguinte forma:

Principal: aba que prioriza conversas e mensagens entre pessoas, com e-mails pessoais;

Social: atualizações de redes sociais e outros sites de compartilhamento de mídia;

Promoções: e-mails promocionais com ofertas e estímulos à compra.

Atualizações: notificações, como confirmações, recibos, faturamentos e demonstrativos.

Fóruns: mensagens de grupos on-line, fóruns e listas de e-mails.

Google Postmaster Tools (GPT)

Uma ferramenta utilizada para análises de entregabilidade que mostra algumas informações importantes sobre a reputação. Alguns dados são parecidos com o que o SNDS apresenta para o Outlook, mas alguns pontos são únicos do Gmail.

Veja abaixo o que é possível captar de dados através do GPT:

a) Taxa de spam reportado pelo usuário;

b) Reputação de domínio e de cada intervalo de IP em 4 níveis: ruim, baixa, média e alta;

c) Taxa de spam identificado pelo FBL;

d) Taxas de sucesso das autenticações de SPF, DKIM e DMARC;

e) Criptografia do tráfego e possíveis erros de entrega.

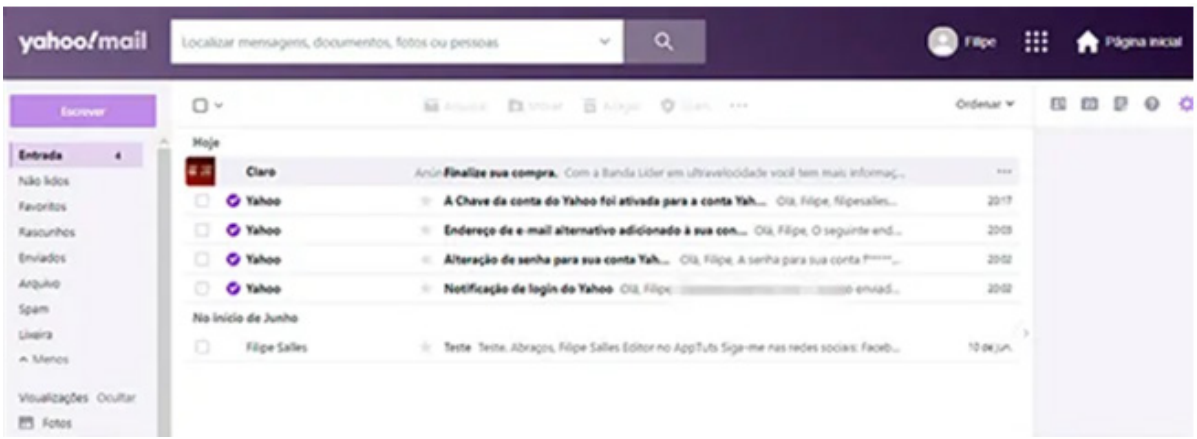
Além disso, também existe um formulário para envio de solicitações de análise para problemas caso o remetente não tenha acesso às informações.

O Gmail tem suporte ao BIMI (*Brand Indicators for Message Identification*), novo padrão de autenticação de mensagens que ajuda a eliminar possíveis spammers, aumentando a segurança das entregas do remetente às caixas de entrada. Com o BIMI, as empresas podem ser identificadas facilmente pelos usuários quando recebem suas mensagens, mostrando seu logotipo na caixa de entrada do usuário, gerando uma experiência mais próxima com a marca.

3. Yahoo

O Yahoo foi fundado em 1994 como um portal da internet para compilar links de outros sites e facilitar as buscas dos usuários. Rapidamente se tornou o maior buscador da internet, criando vários produtos próprios. Em 1997 comprou a RocketMail, um dos serviços mais conhecidos de e-mail gratuito que concorria diretamente com o Hotmail na época. Assim, passou a chamar esse serviço de Yahoo Mail.

Quando o Gmail surgiu em 2004, o Yahoo precisou fazer várias alterações para conseguir concorrer, como mudanças no layout e aumento da capacidade de armazenamento. Em 2017 sua independência chegou ao fim, quando foi comprado pela Oath Inc., empresa da companhia Verizon. Um ponto importante nessa transição é que a Verizon também era detentora da AOL, porém, ambas foram vendidas em 2021 para a *Apollo Global Management*.



Apesar de ser um dos gigantes dos ISPs e possuir uma grande estrutura, o Yahoo não fornece tantas opções para análise ou captação de dados sobre reputação. O ponto de contato mais usado é o formulário de postmaster, onde é possível informar possíveis problemas de entrega, solicitando auxílio mais profundo.

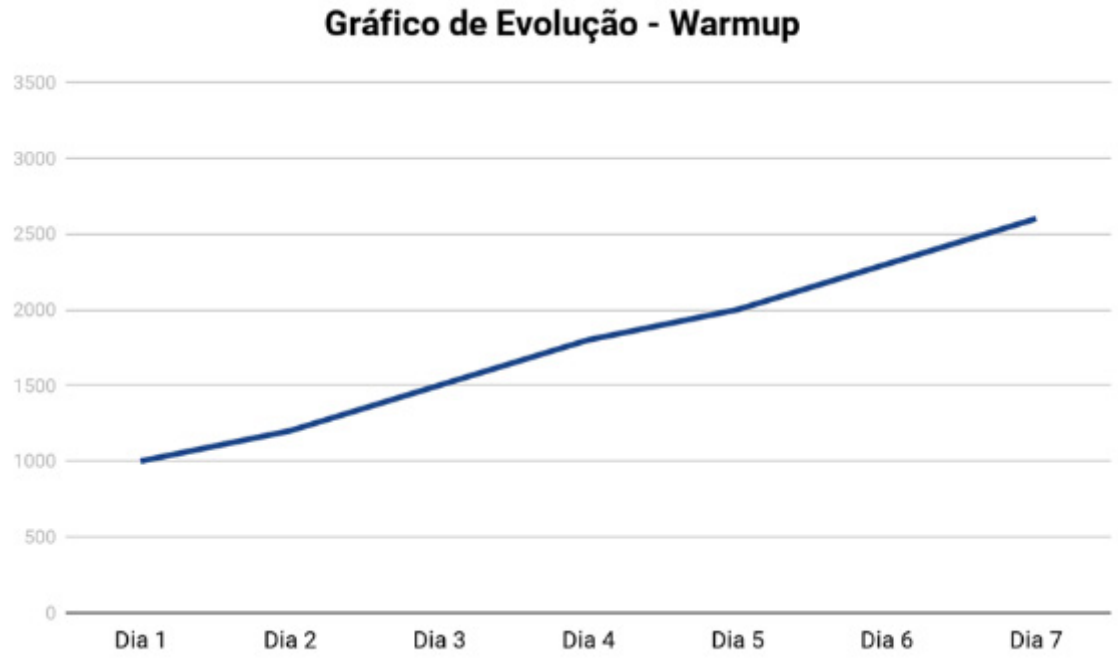
Existem diversos provedores de e-mail no mercado, cada um com suas características. Embora sejam importantes por terem um grande volume de usuários ativos, em termos de estrutura, são bem fracos. Não possuem gratuitamente capacidade grande de armazenamento, ficam sobrecarregados quando há disparos em massa, muitas vezes impedindo de ser entregue a mensagem nesses provedores. De qualquer forma, não podemos descartá-los em hipótese alguma, pois complementam as bases de e-mails e ajudam nas vendas e obtenção de receita.

7. Warmup e Rampup

Sempre que uma marca precisa fazer a troca de um IP para envios promocionais em massa, é necessário que seja feito o aquecimento desse novo IP. O conceito de “IP aquecido”, significa que está apto para enviar um grande volume de envios sem que as métricas e a reputação sejam prejudicadas.

Para alcançar êxito nesse processo, os envios do warmup e rampup são feitos apenas para usuários com histórico recente de interação com os e-mails da marca. Esses disparos iniciam com uma volumetria baixa, até chegar ao volume médio feito pelo cliente. Sendo assim, o warmup é o início dos envios qualificados com volume baixo, enquanto o rampup, é o crescimento gradual dessa volumetria de disparos.

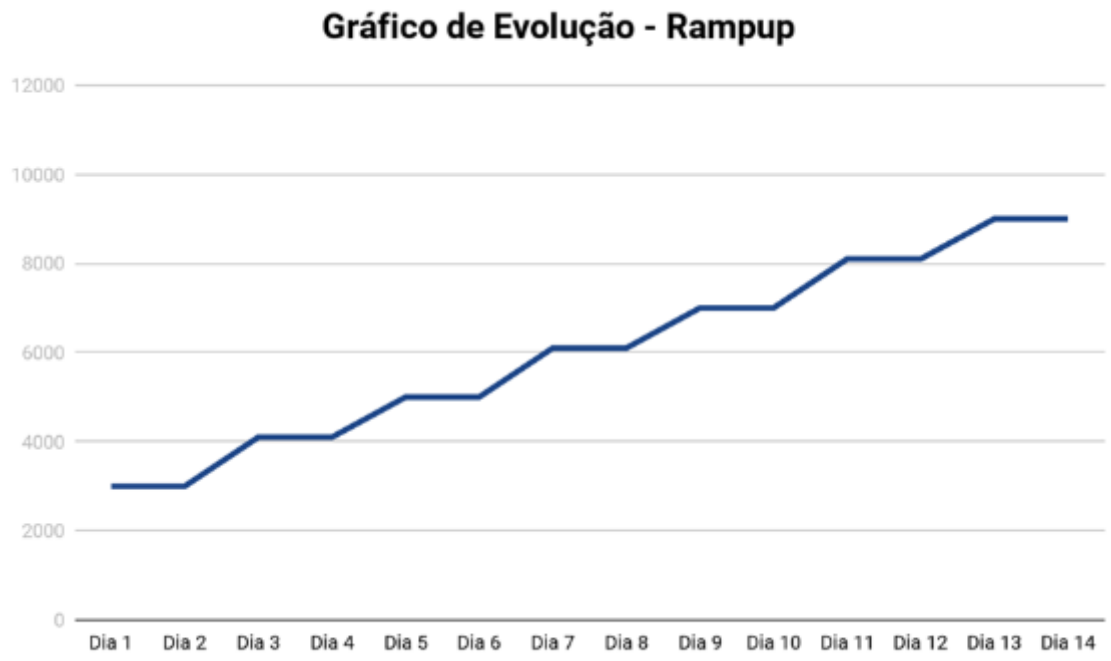
Nessa lógica, o gráfico do primeiro estágio de warmup ganha o seguinte formato:



Nota-se que nesse exemplo, o dia 1 começa com 1.000 envios e chega até pouco mais de 2.500 no dia 7. É um crescimento moderado, onde a prioridade é o início dos envios qualificados.

A fase do Rampup é semelhante ao Warmup, porém, o crescimento volumétrico é mais acentuado e pode ser feito de dois em dois dias ou diariamente com acréscimos. Nessa fase mostramos para os provedores a rotina que se pretende ter nos dias normais.

A evolução ocorre conforme o gráfico:



Início: média de 2.500 envios no dia 1.

Término: média de 9.000 envios dia 14.

Como sabemos, cada ISP tem as suas próprias características na formação de reputação. Por isso, é importante que os principais provedores de e-mail sejam trabalhados de forma individual, analisando a performance de cada um deles. Sendo assim, quando estiver disponível a base que será usada no aquecimento, ela pode ser dividida inicialmente nos principais ISPs e posteriormente os provedores menores são incorporados nos envios.

É imprescindível que sejam realizadas análises diárias de cada disparo, com atenção na volumetria enviada, no horário de disparo (de preferência pela manhã entre 8h e 10h), entregas vs bounces, spam complaints e, finalmente, aberturas. Esses são os critérios que os provedores irão avaliar.

Passando por cada uma dessas etapas, mantendo bom desempenho, certamente o aquecimento do IP será um sucesso.

8. Análise

Para construir uma análise de e-mail marketing, é necessário entender o principal objetivo de fazer esses envios. Partindo disso, precisamos conhecer os três principais tipos de e-mail: transacional, promocional e newsletter. Ao definir o tipo de email, definimos também o objetivo da análise que faremos.

Transacional

É um e-mail de resposta sobre alguma ação feita pelo usuário. Quando precisamos solicitar novas senhas de acesso, recebemos um e-mail com link de confirmação e reset de senha, ou quando efetuamos alguma compra pela internet e recebemos um e-mail de confirmação de pagamento, atualização de entrega, entre outros. Para esse tipo de e-mail não é necessário ser opt-in, ou seja, não é preciso solicitar o recebimento dessas comunicações. Entende-se que ao solicitar algum retorno por e-mail, você autoriza o envio daquela informação.

Análise: **% de entrega**, **% de bounces** e **% spam** são os pontos principais para e-mails transacionais com o objetivo de que a informação solicitada pelo cliente chegue até ele.

Promocional

Esse tipo de e-mail é fundamental para qualquer porte de empresa. O envio tem como objetivo principal vender os produtos ou serviços ofertados pela marca. No layout destaca-se características, preço, condições de pagamento, call to action escrito “Comprar”, “Compre agora” ou “Eu quero”. Cupom de desconto, banners promocionais, etc. Tudo o que possa facilitar a comunicação com o usuário, garantindo a abertura, clique em alguma oferta e conversão no site.

Análise: as métricas principais são **% entrega**, **% bounces, % aberturas**, **% cliques**, **sessões** e **receita**. Apesar de falarmos dessas taxas como principais, não podemos de forma alguma manter fora disso as demais métricas de e-mail para garantir a reputação da conta.

Newsletter

E-mail do tipo informativo, para comunicar novidades da marca, conteúdos ou notícias importantes.

Por exemplo, um e-commerce de calçados irá fazer um evento em uma praça e pretende expor alguns modelos de tênis, aproveitando a oportunidade para comercializá-los. Para garantir que mais pessoas sejam avisadas desse evento, a marca envia um e-mail com todos os detalhes do evento: localização, datas, horários e qualquer dado importante pertinente sobre o evento.

Análise: **% entrega**, **% bounce**, **% spam** e **% aberturas** são as principais métricas para esse tipo de e-mail.

9. Conclusão

Podemos concluir que entregabilidade envolve diversos fatores, desde as autenticações até as análises. Entretanto, com uma boa performance de entregabilidade, você terá engajamento dos usuários, poderá elaborar uma boa estratégia de e-mail marketing através das análises e até aumentar a receita por este canal.

Guia de Entregabilidade

2022

pmweb

Relacionamentos únicos em escala.