

ENTREGABI- LIDADE DE E-MAIL



A entregabilidade de e-mail é a **eficácia de enviar mensagens** para a caixa de entrada do destinatário sem que acabem no spam.

SUMÁRIO

O que é a entregabilidade de e-mail	3
Dois termos que você deve distinguir: entrega e entregabilidade	4
Reputação do domínio e do IP como elementos chave da entregabilidade	4
Aprenda 12 passos para aumentar e manter a entregabilidade	7
Passo 1: higiene da base	8
Passo 2: cuide da autenticação	14
Passo 3: construa seu banco de dados com responsabilidade	26
Passo 4: aquecimento do endereço de IP e infraestrutura	30
Passo 5: analise e otimize	33
Passo 6: para aumentar o engajamento, envie para clientes engajados	35
Passo 7: use a segmentação	41
Passo 8: cuide do conteúdo	43
Passo 9: envie regularmente	45
Passo 10: faça testes A/B	47
Passo 11: garanta facilidade para o descadastro	48
Passo 12: acompanhe mudanças nas tendências de entregabilidade	49
Resumo	51

© que é a entregabilidade de e-mail

A entregabilidade de e-mail é a eficácia de enviar mensagens para a caixa de entrada do destinatário sem que acabem no spam. Isso envolve manter uma reputação positiva do remetente e implementar melhores práticas, como o uso de medidas de segurança DKIM, SPF e DMARC. No contexto do marketing, uma alta entregabilidade impacta na eficácia das campanhas e na construção de uma relação de confiança com o cliente. **Não é apenas uma ferramenta de marketing**, mas também um meio de criar relacionamentos duradouros e alcançar o sucesso nos negócios.



No mundo de hoje, onde bilhões de e-mails são enviados diariamente, a entregabilidade se torna um elemento crucial da estratégia de marketing por e-mail. O número de usuários de e-mail ultrapassou **4,4 bilhões** em 2023 (Influencer Marketing Hub), com projeção de crescimento para **4,6 bilhões** até 2025, representando mais da metade da população global. Até 2025, a previsão é de que **376,4 bilhões** de e-mails sejam disparados por dia.

De acordo com dados de abril de 2022, a taxa média de entregabilidade de e-mail foi de **84,2%**, indicando uma queda de **4,7%** em comparação com o ano anterior.

Curiosamente, **20,4% dos e-mails acabam na caixa de spam ou não são entregues**. Isso levanta uma discussão sobre o sucesso da entrega de e-mails e estratégias para melhorar a entregabilidade. Questões sobre os fatores que afetam a reputação do remetente e práticas para evitar armadilhas que levam a uma baixa entregabilidade são consideradas essenciais.

Dois termos que você deve distinguir: **entrega e entregabilidade**

Entrega e entregabilidade de e-mails são dois conceitos distintos frequentemente confundidos na linguagem do dia a dia. A entrega refere-se à quantidade de e-mails enviados aceitos pelos servidores dos provedores de e-mail dos assinantes. Isso confirma que as mensagens alcançaram seu destino. Por outro lado, a entregabilidade é onde os e-mails terminam - se na caixa de entrada ou no spam. É um elemento crucial que determina a posição de uma mensagem na consciência do destinatário.

Por exemplo, quando vamos enviar uma carta para um amigo, a entrega é a confirmação de que a carta física chegou à caixa de correio, equivalente a colocar um pacote na porta do destinatário. Já a entregabilidade é o que acontece após abrir a caixa do correio - se a carta é notada e apreciada ou ignorada.

Em resumo, entrega é a fase inicial que garante a chegada física da mensagem ao destinatário, enquanto entregabilidade é a segunda fase que verifica se a mensagem não apenas chegou, mas também foi recebida e notada. Tanto entrega quanto entregabilidade são cruciais para uma comunicação por e-mail eficaz, e manter a reputação do remetente influencia ambos elementos.

Reputação do domínio e do IP como elementos chave da entregabilidade

A reputação do domínio e do IP impacta significativamente a entregabilidade de e-mails. Tanto os provedores de e-mail quanto os filtros anti-spam consideram esses elementos ao avaliar se um e-mail deve ser entregue na caixa de entrada ou classificado como spam.

Nossos especialistas em entregabilidade enfatizam que os provedores de serviços de e-mail, como o Gmail, atribuem maior importância à reputação do domínio. Isso ocorre porque a reputação do domínio está mais focada em remetentes específicos e está intimamente ligada a uma empresa ou marca. A reputação do IP influencia diretamente na avaliação feita pelos provedores de serviços de e-mail, como a Microsoft. A Microsoft, sendo proprietária de um dos provedores de caixa de correio mais populares (por exemplo, Outlook, Hotmail), utiliza filtros anti-spam rigorosos e mecanismos para avaliar os provedores de e-mail.

O que é a reputação do domínio?

Reputação do domínio refere-se a como os provedores de serviços de e-mail, como Outlook, Yahoo ou Gmail, percebem o seu domínio. Quanto melhor a reputação, menor a probabilidade de seus e-mails serem rejeitados, pois os provedores de e-mail o consideram um remetente confiável.

Provedores de serviços de internet e de caixa de correio influenciam se seus e-mails serão entregues na caixa de entrada dos destinatários ou redirecionados para a pasta de spam. A reputação do domínio é um dos principais fatores que afetam essa decisão. No contexto do e-mail, a reputação do domínio é semelhante a uma pontuação de crédito, fornecendo uma avaliação geral de um determinado domínio com base na quantidade e qualidade de links que o direcionam. Os provedores de serviços de e-mail avaliam a reputação do domínio em uma escala de 0 a 100. Servidores que recebem e-mails tendem a confiar mais em mensagens de um domínio que alcança uma pontuação mais alta na avaliação.

Verificando a reputação do domínio

O processo de monitoramento e avaliação da reputação do domínio no marketing por e-mail é crucial, mas é essencial entender que cada provedor de serviços de e-mail (ESP, sigla em inglês) emprega seu próprio sistema de pontuação de reputação para o seu domínio de e-mail. Isso significa que cada provedor, como Gmail, Yahoo ou Microsoft, atribui pontuações de reputação únicas para o seu domínio.

Por que isso acontece? A razão é simples: os provedores de serviços de e-mail só podem avaliar a reputação do domínio com base nos e-mails que recebem desse domínio específico. Isso implica que cada provedor tem sua própria perspectiva e dados para avaliar a reputação.

Para simplificar essa situação complexa, existem ferramentas como:

- Google Postmaster Tools que permite monitorar e verificar a reputação de domínios que enviam e-mails para caixas de entrada do Gmail;
- Microsoft SNDS (Smart Network Data Services), uma ferramenta oferecida pela Microsoft que permite aos provedores de e-mail verificarem estatísticas de entrega e reputação para seus IPs;
- Spamhaus DBL (Domain Block List), um banco de dados que rastreia domínios considerados como abuso de e-mails. Verificar se seu domínio está nesta lista pode fornecer insights sobre sua reputação.

Reputação de IP

Ao comparar a reputação de domínio com a reputação de IP, é possível observar que a reputação de IP se refere à avaliação da credibilidade dos dispositivos atribuídos a um endereço de IP específico.

A reputação de IP tem um impacto negativo quando suas mensagens de e-mail são classificadas como spam. Vários outros fatores influenciam a reputação de IP, como a localização do endereço IP, o tipo de atividades associadas a ele e se o endereço de IP está em uma lista negra. Provedores de serviços de e-mail monitoram constantemente a reputação de IP dos remetentes.

Se um remetente possui uma reputação alta, é mais provável que os e-mails sejam entregues nas caixas de entrada de usuários que utilizam serviços da Microsoft, por exemplo. Os provedores implementam filtros avançados anti-spam que analisam vários aspectos dos e-mails, incluindo conteúdo, cabeçalhos, links e endereços IP associados. A Microsoft atribui uma pontuação de “reputação do remetente”. Essa pontuação leva em consideração vários fatores, como histórico de envio de e-mails, taxas de retorno, reclamações de spam, atividade dos assinantes e conformidade com as melhores práticas de envio de e-mails. Os ESPs exigem que os remetentes sigam padrões da indústria, como DKIM (DomainKeys Identified Mail), SPF (Sender Policy Framework) e DMARC (Domain-based Message Authentication, Reporting, and Conformance). Sua implementação e configuração corretas são cruciais para manter uma reputação de IP positiva.

Aprenda 12 passos para aumentar e manter a entregabilidade

A entregabilidade é um assunto sério, mas o que você pode fazer para garantir que esteja em seu nível mais alto? Descubra os 12 passos mais importantes para aumentar e manter a entregabilidade:

Passo 1: higiene da base

Por que cuidar da qualidade da lista de e-mails é crucial?

Uma estratégia ideal requer manter uma lista de assinantes limpa e engajada, que constitui a base de uma campanha de e-mail eficaz. Ter uma lista bem organizada com assinantes engajados é fundamental para combater o crescente problema de spam.

O estado da sua lista de e-mails é significativo por várias razões importantes.

Principalmente, pois impacta sua reputação como remetente e se seus e-mails alcançarão as caixas de entrada dos assinantes que utilizam serviços de marketing por e-mail. É essencial perceber que o simples envio de e-mails não garante a entrega perfeita do remetente ao destinatário.

Verificando a reputação do domínio

O e-mail é rejeitado pelo servidor de e-mail do destinatário.

Provedores de serviços de e-mail bloqueiam ou marcam o e-mail como spam.

O e-mail é entregue na caixa de entrada do destinatário.

É crucial ressaltar que o controle sobre se seus e-mails chegam ao destino não é aleatório, mas depende da sua reputação como remetente. Uma reputação alta significa que os provedores de e-mail o consideram um remetente confiável, entregando seus e-mails diretamente nas caixas de entrada dos assinantes. No entanto, uma reputação ruim aumenta o risco de seus e-mails serem marcados como spam.

Provedores de serviços de e-mail, como Gmail ou Outlook, utilizam vários indicadores para avaliar a reputação do remetente. Esses fatores incluem o número de e-mails rejeitados (tanto hard bounces quanto soft bounces), reclamações de spam dos destinatários, o histórico de cancelamentos de assinatura e a verificação se o remetente envia e-mails para endereços que são armadilhas de spam.

Portanto, manter a higiene da lista de e-mails é crucial. Imagine uma parte significativa de seus assinantes tendo endereços de e-mail incorretos ou perdendo o interesse em suas mensagens. Todos esses aspectos impactam negativamente sua reputação como remetente. Com base nesses fatores, os provedores podem decidir bloquear seus e-mails, o que significa que eles nem mesmo alcançarão as caixas de entrada ativas usando o mesmo provedor de serviços de e-mail. É uma penalidade severa que poderia ser evitada mantendo a limpeza e a qualidade da lista de e-mails. Portanto, vale a pena dedicar tempo e esforço para garantir a higiene da lista de e-mails, preservando uma excelente reputação como remetente e alcançando o sucesso no marketing por e-mail.

Cuidado com as armadilhas de spam (anti-spam traps)

As armadilhas de spam são frequentemente utilizadas por provedores de caixa de correio e listas de bloqueio para capturar remetentes mal-intencionados, mas remetentes legítimos com baixa higiene de dados também podem acabar na lista de bloqueio (por isso a importância de manter a limpeza de dados!). As armadilhas de spam se assemelham a endereços de e-mail regulares, mas seu propósito real é identificar spammers/organizações com higiene de dados inadequada. Enviar e-mails para um endereço de armadilha de spam pode impactar a reputação do remetente e afetar a entrega de mensagens de e-mail na caixa de entrada do assinante.

Tipos de endereços de armadilhas de spam:

Armadilhas de Spam Pristine (ASP):

Armadilhas de Spam Pristine são endereços de e-mail recém-criados intencionalmente gerados por provedores de serviços de internet ou organizações anti-spam. Esses endereços nunca foram usados por usuários regulares de e-mail e muitas vezes são acessíveis publicamente online. Spammers podem inadvertidamente encontrar essas armadilhas de e-mail quando um banco de dados contendo esses endereços é vendido a um comprador.

Armadilhas de Spam Recicladas (ASR):

Armadilhas de Spam Recicladas são endereços de e-mail que eram originalmente legítimos, mas foram abandonados (por exemplo, endereços de ex-funcionários, caixas de correio de pessoas que mudaram de provedores). Após 12 a 18 meses, eles são reativados e transformados em armadilhas. Eles frequentemente atraem remetentes regulares e legítimos, especialmente aqueles que tiveram contato anterior com o proprietário original. Essas armadilhas de spam são comumente encontradas em grupos de contatos mais antigos usados para envios de e-mails pouco frequentes ou campanhas de reativação.

Armadilhas de Spam por Erro de Digitação (EST):

As Armadilhas de Spam por Erro de Digitação, também conhecidas como Armadilhas por Erro de Digitação, se assemelham às Armadilhas de Spam Recicladas (ASR) ao se passarem por endereços de e-mail válidos. No entanto, elas diferem sutilmente por terem um domínio ligeiramente alterado, o que pode ser enganoso, por exemplo, gmai.com em vez de gmail.com. Sua presença em um banco de dados pode ser acidental, talvez devido a erros de registro. Ao contrário das Armadilhas de Spam Pristine (ASP), mais prejudiciais, as Armadilhas de Spam por Erro de Digitação são menos danosas, mas enviar mensagens para esses endereços pode sugerir falta de cuidado com a higiene da lista de contatos. Isso, por sua vez, pode levar os provedores de serviços de e-mail a tomar medidas restritivas. Para evitar Armadilhas de Spam por Erro de Digitação, é importante usar confirmação de registro (double-opt-in) no formulário de registro.

Armadilhas de Spam Inativas (ASI):

Embora usadas com menos frequência, este tipo de armadilha de spam ainda representa uma ameaça potencial para remetentes cujos bancos de dados de contatos não são verificados regularmente. Endereços de e-mail incorretos, conhecidos como Armadilhas de Spam “esquecidas”, permanecem não utilizados por um período prolongado, às vezes por mais de um ano, mas não foram fechados ou desativados pelos provedores de serviços de internet.

Semelhantes às Armadilhas de Spam Recicladas (ASR), elas se originam de contas muito antigas que se tornaram armadilhas de spam. Embora menos comuns do que outros tipos de Armadilhas de Spam, é essencial prestar atenção a elas durante a limpeza do banco de dados.

Higiene do banco de dados: impacto na entregabilidade e influência positiva nos seus resultados

Um banco de dados saudável garante resultados mais precisos para campanhas de marketing por e-mail. Assinantes não engajados podem impactar negativamente métricas como a taxa de abertura (TA) e a taxa de cliques. Limpar regularmente o banco de dados permite a medição precisa da eficácia, facilitando o planejamento de futuras atividades de marketing. Taxas mais altas de abertura e cliques confirmam a eficácia na entrega de e-mails para o público certo, aumentando as chances de conversões e aprimorando o valor do marketing por e-mail.

Higiene: impacto na entregabilidade e efeitos positivos nas economias de marketing e ROI

Uma lista de e-mails saudável reduz os custos de marketing, especialmente com encargos para e-mails enviados. Manter uma lista limpa elimina gastos desnecessários com assinantes não engajados, melhorando a lucratividade das campanhas. Focar nos destinatários que desejam receber suas mensagens aumenta as chances de conversões e um melhor retorno sobre o investimento em marketing por e-mail. Assinantes engajados são cruciais para o sucesso. Uma lista limpa não apenas melhora a qualidade dos contatos, mas também economiza nos custos associados a problemas de entregabilidade de e-mails, minimizando bloqueios de caixa de correio e garantindo uma entrega tranquila nas caixas de entrada.

Passo a passo: limpeza da lista de e-mails

Limpar uma lista de e-mails é um processo crucial que serve para manter a alta qualidade dos bancos de dados e melhorar a eficácia das campanhas de e-mail.

Agora que você entende por que é essencial cuidar de uma lista de e-mails saudável, vamos discutir como conduzir o processo de limpeza em alguns passos simples.

1 **Elimine endereços de e-mail inválidos e desatualizados**

Identifique hard bounces (problemas permanentes) e remova-os. A Edrone pode ajudar automaticamente a bloquear endereços de e-mail após a primeira ocorrência de um hard bounce. Não enviaremos uma mensagem a esse destinatário novamente.

Soft bounces requerem uma resposta, como o desenvolvimento de procedimentos de resposta e limpeza potencial. Eles indicam dificuldades temporárias na entrega de e-mails, que podem resultar de vários motivos, como uma caixa de entrada cheia, indisponibilidade do servidor de e-mail ou tamanho excessivo da mensagem. Para soft bounces, a remoção imediata da lista nem sempre é necessária; em vez disso, vale a pena desenvolver um procedimento para a resposta e limpeza potencial.

2 Identifique perfis não engajados na lista de e-mails

Você já entende que alguns assinantes podem perder o interesse em seus e-mails.

- Defina critérios para assinantes não engajados.
- Estabeleça quando um assinante se torna não engajado, por exemplo, falta de interação por um período prolongado.
- Crie segmentos para assinantes não engajados antes de considerar a remoção deles.

3 Tentando campanhas de reativação de e-mails

Antes de remover clientes não engajados da lista de e-mails, é aconselhável implementar campanhas de reativação. Essas ferramentas eficazes ajudam a restabelecer contato com clientes que perderam o interesse nas ofertas. Etapas-chave incluem:

Segmentação da lista:

Segmentar a lista identificando clientes não engajados sem atividade, aberturas ou cliques.

Personalização de conteúdo:

Personalizar e-mails de reativação para grupos específicos de clientes. Ofertas e conteúdo devem ser personalizados, focando nas necessidades do público.

Ofertas e incentivos:

Utilizar vários incentivos, como códigos de desconto, frete grátis, apresentações de novos produtos. Persuadir clientes a reacender o interesse na marca.

Monitoramento de cronogramas:

Definir cronogramas para campanhas de reativação. Enviar e-mails iniciais, seguidos por lembretes eventuais. Campanhas de reativação permitem reter clientes à beira do desengajamento enquanto economizam nos custos de envio para assinantes não engajados. Experimentar diferentes estratégias, monitorar resultados e ajustar campanhas às necessidades do público são cruciais.

Dicas adicionais para a limpeza da lista de e-mails incluem:

Monitorar o engajamento e enviar mensagens para assinantes ativos. Ajustar a frequência para assinantes menos ativos, otimizando custos. Manter promoções-chave para todos os assinantes.

4 **Facilitar o processo de cancelamento da inscrição, impactando positivamente a reputação do remetente.**

Como reconhecer quando é necessário limpar sua lista de e-mails?

Uma diminuição no engajamento, como baixas taxas de abertura e cliques.

- Aumento nas taxas de retorno.
- Aumento nos pedidos de cancelamento de inscrição e nos relatórios de spam.

Com que frequência você deve limpar sua base?

Se você tiver menos de 50.000 contatos, uma vez por ano deve ser suficiente. No entanto, se sua lista estiver crescendo dinamicamente, é recomendado limpá-la a cada seis meses. Além disso, lembre-se de verificar antes de eventos de compras significativos, como a Black Friday e a Cyber Monday.

MOSQUITO



CO U CIEBIE
SŁYCHAĆ?

Cześć **first_name_test!**

Jesteś na naszej liście subskrybentów, dzięki czemu na bieżąco dostajesz od nas informacje o aktualnych promocjach. Również dzielimy się z Tobą inspiracjami i ciekawostkami, które mogą okazać się przydatne przy wyborze produktów.

Niestety widzimy, że już od dłuższego czasu nie otwierasz naszych newsletterów. 😞

Jeśli chcesz nadal otrzymywać od nas treści i być subskrybentem, kliknij poniższy przycisk:

Chcę pozostać subskrybentem



ODKRYJ WIĘCEJ

PRZEJDŹ DO SKLEPU >>

MOSQUITO



Administratorem Twoich danych osobowych, podanych przy zapisie do naszego newslettera jest firma MOSQUITO COMPANY ALICJA KOMAR ul. Piława 8, 97-200 Tomaszów Mazowiecki, NIP: 773232310, REGON: 100740521. Wszelkie informacje związane z przetwarzaniem danych osobowych i Twoich prawach z tym związanych znajdziesz w naszej Polityce Prywatności, a więcej pytań możesz zadać, pisząc pod adres: GDRO@mosquito.pl. Jeśli nie chcesz otrzymywać od nas więcej podobnych wiadomości, kliknij [tutaj](#).

Uma campanha de reativação da marca polonesa Mosquito para assinantes que não abriam uma mensagem há mais de seis meses. Os clientes inativos foram filtrados e marcados, e seu status de assinatura foi substituído por desconhecido antes do envio. Um botão de ação de assinatura SUBSCRIBE foi usado na mensagem, para que os clientes que quisessem permanecer no banco de dados tivessem a chance de responder. A campanha foi enviada para mais de 50.000 usuários inativos, 700 usuários abriram e 113 usuários expressaram o desejo de permanecer no banco de dados. Quando clicados, os clientes tiveram seu status de assinatura alterado para SUBSCRIBE e voltaram a receber comunicação regular.

*campanha traduzida para o português.

Passo 2: cuide da autenticação

Medidas de segurança como SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail), DMARC (Domain-based Message Authentication, Reporting, and Conformance) e BIMl (Brand autenticidade das mensagens de e-mail transmitidas). Todos esses mecanismos têm um impacto positivo na entregabilidade das mensagens, aumentando a autenticidade, construindo a confiança do destinatário e reduzindo o risco de os e-mails serem classificados como spam. Graças a essas medidas, as organizações podem proteger mais efetivamente sua reputação online e manter a segurança da comunicação eletrônica.

O que é SPF?

SPF (Sender Policy Framework) é um recurso de segurança usado para autenticar o remetente de uma mensagem de e-mail. Essa segurança declara quais servidores de e-mail têm permissão para realizar envios a partir do seu domínio - dessa forma, o servidor de e-mail do destinatário “sabe” que a mensagem foi enviada de um servidor autorizado. Em resumo, é uma tecnologia para prevenir spam e a possibilidade de falsificação.

No SPF, incluímos o IP ou o nome (no qual determinados IPs são armazenados) do servidor que queremos autorizar a enviar mensagens sob um determinado domínio, por exemplo, como aqui: `v=spf1 mx ip4:196.137.0.5 -all`. Se a mensagem for enviada de outro servidor, cujo IP não estiver incluído no SPF, será considerada suspeita pelos servidores de e-mail do destinatário.

Cada mensagem de e-mail contém os dois endereços de envio indicados no campo ‘from’ e o ‘return_path’ (ou seja, o chamado caminho de retorno). O return_path é o endereço para o qual as mensagens devem ser enviadas de volta ou devolvidas se não puderem ser entregues. Ele é incluído no cabeçalho oculto do e-mail. Não é o mesmo que o endereço “reply to” (responder para) (o endereço para o qual você pode responder a uma mensagem recebida). O SPF é definido para o domínio contido no endereço “return_path”.

Como é um registro SPF e como adicioná-lo?

Um registro SPF é simplesmente um registro DNS. O registro pode ser adicionado ou modificado na hospedagem de um determinado domínio. Se um SPF para um domínio já existe, você não adiciona outro (só pode haver um SPF para um domínio), mas pode modificá-lo adicionando outra parte que conterà os IPs ou nomes dos servidores que você deseja autorizar a enviar mensagens desse domínio.

O registro SPF está sempre no formato TXT ou, em alguns hosts, simplesmente SPF.

Um exemplo de registro SPF se parece com isso:

```
v=spf1 a mx include:spf.protection.outlook.com include:_spf.edrone.me ~all
```

Aqui está uma explicação do que cada elemento do registro significa:

v=spf1 - o início do registro SPF e indica a versão do SPF que está atualmente em uso. Neste caso, "spf1" significa que você está usando a versão 1 do protocolo SPF.

a - este elemento significa que os servidores cujos endereços IP estão associados ao registro A raiz do domínio (ou seja, aqueles que servem o próprio site) estão autorizados a enviar e-mails em nome desse domínio.

mx - significa que servidores especificados como servidores de e-mail (registros MX) para um domínio também estão autorizados a enviar e-mails em nome desse domínio.

include:spf.protection.outlook.com - este elemento indica que os servidores incluídos no registro SPF chamado 'spf.protection.outlook.com' estão autorizados a enviar e-mails desse domínio. Este é um exemplo de uso de um registro SPF externo que especifica que os servidores Microsoft Outlook estão autorizados.

include:_spf.edrone.me - este é outro exemplo de uso de um registro SPF externo. Neste caso, servidores do domínio "_spf.edrone.me" estão autorizados a enviar e-mails em nome desse domínio.

~all - esta é a parte que determina como lidar com e-mails que foram enviados sob um determinado domínio, mas seus servidores não estão incluídos no SPF. "~all" significa que tais e-mails são tratados como suspeitos.

Os finais do SPF podem variar, podem ser 'all' ou '~all' ou '-all'. Diferenças explicadas a seguir:

"all" - significa que mensagens que não correspondem ao registro SPF devem ser rejeitadas. Esta é a opção mais restrita e significa que apenas servidores listados no registro SPF estão autorizados a enviar e-mails em nome do domínio.

"~all" - esta é uma opção mais flexível e permite a entrega de e-mails de servidores que não estão incluídos no registro SPF, mas os marca como potencialmente suspeitos.

"-all" - também significa que mensagens que não correspondem ao registro SPF devem ser descartadas, semelhante a "all", no entanto, "-all" é uma notação mais antiga e menos comumente usada, "all" é mais comum.

“?all” - significa que a autenticação incorreta não afeta o recebimento da mensagem. A escolha entre essas opções depende de sua preferência e estratégia de segurança. Pode levar até 48 horas antes que um registro SPF esteja totalmente operacional, então aguarde e verifique após esse tempo.

Como funciona a verificação SPF?

Ao enviar, o servidor de e-mail para o qual a mensagem será enviada verifica o endereço contido no “return_path”. Ele então valida o registro SPF, ou seja, verifica se a mensagem foi enviada de um servidor que está incluído no registro DNS do domínio (o domínio do endereço do ‘return_path’).

Se o domínio for validado - o servidor de envio está incluído no registro SPF do domínio - então a mensagem é entregue.

Se não for - o servidor de envio não está incluído no registro SPF - então, dependendo do sufixo do registro SPF (-all, ~all, etc.), a mensagem pode ser rejeitada ou recusada, mas marcada como suspeita, ou ir para o SPAM.

No contexto de um servidor usando o protocolo SPF (Sender Policy Framework), o processo funciona da seguinte maneira:

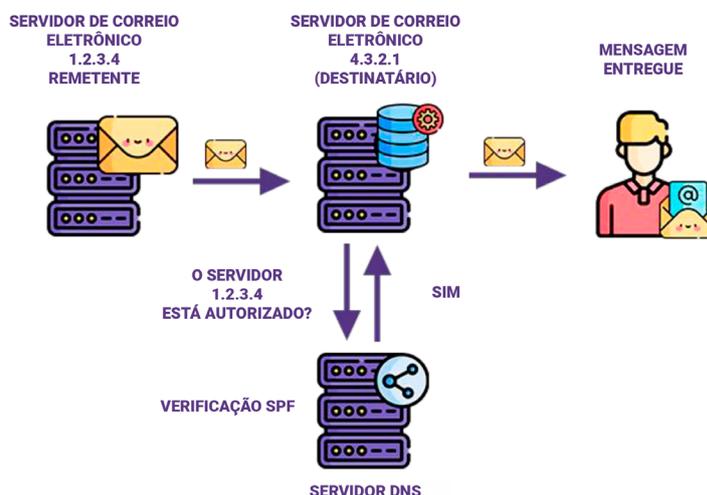
O servidor receptor extrai o domínio fornecido no campo MAIL FROM (localizado no envelope SMTP) da mensagem de e-mail.

O servidor receptor acessa a configuração SPF armazenada nos registros DNS do domínio do remetente.

A verificação é realizada para determinar se o endereço IP do qual o servidor receptor recebeu o e-mail está autorizado a usar o domínio especificado.

- A No caso de verificação negativa, ou seja, o endereço IP não está autorizado, a mensagem de entrada é rejeitada.
- B No caso de verificação positiva, ou seja, o endereço IP está autorizado, o servidor aceita a mensagem para processamento adicional.

Esse esquema permite que o protocolo SPF verifique efetivamente a autenticidade do remetente, impedindo assim transmissões não autorizadas e aprimorando a segurança e credibilidade do



hostido.pl/blog/mechanizmy-zabezpieczajace-poczte-e-mail-spf-dkim-dmarc/

Por que o DMARC é tão importante e quais são os benefícios de configurar o DMARC corretamente?

Proteção contra fraudes

O DMARC ajuda a verificar que o e-mail é de um remetente genuíno e não foi adulterado durante a transmissão. Isso aumenta a credibilidade do remetente.

Redução de spam:

O SPF ajuda a combater o spam porque permite que servidores de e-mail verifiquem se os e-mails são de fontes genuínas. Se um e-mail não atender aos critérios de um registro SPF, o servidor de e-mail pode bloquear a entrega.

Melhoria na entrega de e-mails:

Um registro SPF corretamente configurado pode melhorar a entrega de e-mails. Servidores de e-mail têm mais probabilidade de entregar e-mails de remetentes que possuem o registro SPF correto, pois isso é um sinal de que o remetente é genuíno.

Suporte a outras tecnologias anti-spam:

O SPF pode ser usado em conjunto com outras tecnologias anti-spam, como DKIM e DMARC, para aumentar o nível de segurança dos e-mails.

Proteção da reputação do domínio:

Um registro SPF corretamente configurado ajuda a manter uma boa reputação do domínio no mundo dos e-mails. Domínios que não protegem seus e-mails com SPF podem se tornar um alvo atrativo para golpistas e spammers, o que pode afetar negativamente sua reputação.

Em resumo, configurar um registro SPF ajuda a proteger seu domínio contra abusos de e-mail, spam e fraudes. É um passo importante para manter a segurança (incluindo destinatários) e a credibilidade do seu domínio.

No entanto, garantir a segurança do SPF não é suficiente, então também vale a pena cuidar do DKIM, a autenticação de domínio do endereço 'from'.

O que é o DKIM?

O DKIM (DomainKeys Identified Mail) é outra tecnologia usada para verificar a autenticidade de uma mensagem de e-mail e do remetente, e para prevenir fraudes e phishing. O DKIM é uma assinatura digital de uma mensagem de e-mail que permite aos servidores do destinatário verificarem a autenticidade do remetente.

Se a assinatura DKIM for válida e corresponder à chave DKIM do registro DNS do domínio do remetente, o remetente e a mensagem são considerados autênticos. Este registro DNS refere-se ao domínio contido no endereço 'from', ou seja, o domínio do remetente.

Aqui está um exemplo de registro DKIM em formato TXT:

nome do host: selector._domainkey.example.com

valor: "v=DKIM1; k=rsa; p=MIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC..."

Neste exemplo:

- nome do host é o nome do host DKIM, que geralmente segue o formato "selector._domainkey.example.com", onde:
 - "selector" é o identificador de um servidor específico, que especifica o conjunto de chaves usadas para assinar e-mails em um domínio específico
 - "_domainkey" é a parte fixa
 - "example.com" é o domínio do remetente
- value é o valor real do registro DKIM, que contém informações sobre a versão, o algoritmo criptográfico e a chave pública DKIM

O registro DKIM é sempre gerado pelo provedor do servidor remetente. Ele é adicionado como outro registro DNS selecionando o formato TXT ou CNAME (dependendo do formato em que foi gerado) e especificando o nome e o valor. É possível ter vários registros DKIM (não apenas um, como o SPF). Dependendo do provedor, o nome do host e o valor podem ter nomes um pouco diferentes, então verifique como o DKIM está configurado em seu provedor de hospedagem.

Você também deve aguardar até 48 horas após adicionar o DKIM, pois pode levar esse tempo para estar completamente operacional.

DKIM

Como funciona a verificação do DKIM?

Quando o remetente envia um e-mail, ele usa sua chave privada DKIM para gerar uma assinatura digital. O remetente envia um e-mail com esta assinatura DKIM para o destinatário.

Quando o servidor de e-mail do destinatário recebe a mensagem, ele verifica os registros DKIM do domínio e verifica se há um com o identificador de domínio do remetente da mensagem, ou seja, se essa assinatura corresponde a algum dos registros DNS (qualquer registro DKIM) do domínio do remetente.

Se a verificação for bem-sucedida, ou seja, a assinatura concordar com o registro DKIM do domínio, a mensagem e o remetente são considerados autênticos. Se esse registro não existir ou não for válido, a mensagem pode ser considerada suspeita ou pode ser rejeitada pelo servidor de e-mail do destinatário, dependendo da política do servidor de e-mail.

Na prática, esse processo ocorre da seguinte forma:

A chave pública para um determinado domínio é armazenada nos registros DNS.

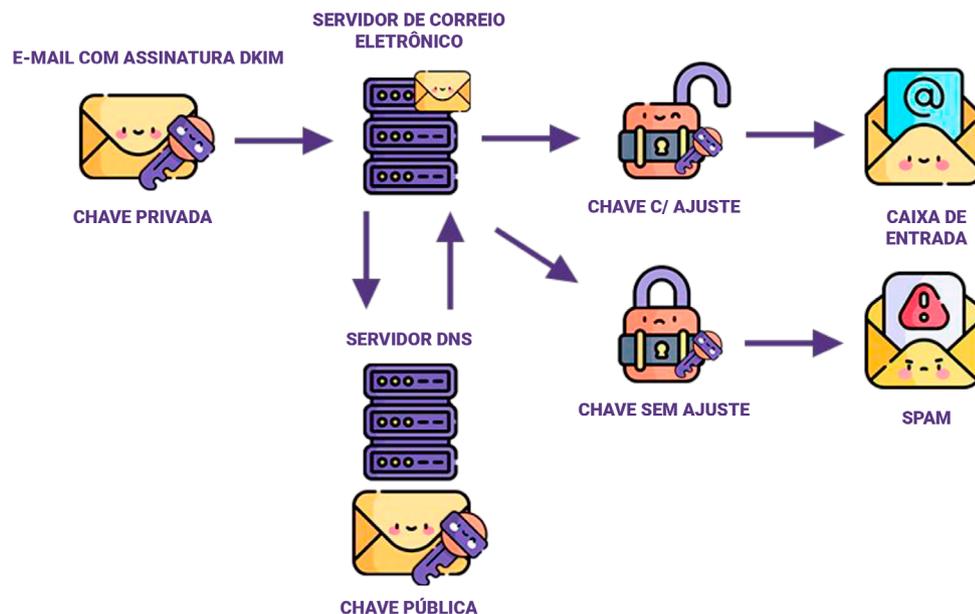
Ao enviar uma mensagem de e-mail, uma assinatura digital criada usando a chave privada é adicionada aos cabeçalhos da mensagem.

O servidor receptor obtém o registro DKIM contendo a chave pública para o domínio especificado.

A verificação é realizada para checar se a assinatura digital da mensagem corresponde à chave pública.

- A Em caso de não correspondência, ou seja, se a assinatura não corresponder à chave pública, a mensagem é rejeitada.
- B Em caso de correspondência, ou seja, se a assinatura corresponder à chave pública, o servidor aceita a mensagem para processamento adicional.

Através desse mecanismo, o DKIM confirma efetivamente a autenticidade da mensagem, eliminando o risco de falsificação e aumentando o nível de segurança na transmissão de e-mails.



hostido.pl/blog/mechanizmy-zabezpieczajace-poczte-e-mail-spf-dkim-dmarc/

Como funciona a verificação do DKIM?

Na prática, esse processo ocorre da seguinte forma:

O DMARC ajuda a verificar que o e-mail é de um remetente genuíno e não foi adulterado durante a transmissão. Isso aumenta a credibilidade do remetente.

Proteção contra phishing:

O DMARC ajuda a combater o phishing porque facilita para os servidores de e-mail identificarem os verdadeiros remetentes dos e-mails. Isso dificulta que os fraudadores se passem por marcas conhecidas ou individuais.

Melhoria da entregabilidade de e-mails:

E-mails assinados com o DMARC são mais confiáveis aos olhos dos servidores de e-mail, o que aumenta as chances de entrega nas caixas de entrada dos destinatários.

Proteção contra modificações:

O DMARC protege contra modificações acidentais ou intencionais no conteúdo da mensagem durante a transmissão, garantindo a integridade das informações transmitidas.

Suporte para outras tecnologias:

O DMARC pode ser usado em conjunto com outros mecanismos anti-spam, como SPF e DKIM, para aprimorar a proteção e a segurança dos e-mails.

Reputação do remetente:

Enviar e-mails usando DMARC ajuda, assim como com o SPF, a manter a boa reputação do domínio do remetente, o que é importante para a confiabilidade e entregabilidade a longo prazo dos e-mails.

Como funciona a verificação do DMARC?

O proprietário do domínio define regras determinando como lidar com mensagens que não atendem aos requisitos de SPF e DKIM. O DMARC também permite receber relatórios sobre as ações tomadas pelos servidores de e-mail que recebem as mensagens. Essas regras fazem parte dos registros DNS de um domínio específico.

Quando um servidor de e-mail recebe uma mensagem, ele verifica os registros DNS do domínio do remetente para verificar a política do DMARC e avalia a mensagem com base em três diretrizes:

- Se o DKIM é válido.
- Se o SPF contém o IP do servidor de envio.
- Se os domínios nos cabeçalhos (from e return_path) correspondem ao domínio no endereço do remetente (no campo “from”).

Após a verificação, com base na política do DMARC estabelecida pelo remetente, o servidor “decide” o que fazer com a mensagem e envia um relatório ao remetente.

Por que vale a pena configurar o DMARC?

Enquanto o SPF e o DKIM se concentram na autenticação das mensagens em termos de origem e integridade do conteúdo, o DMARC agrega esses mecanismos, permitindo o estabelecimento de políticas para o manuseio de mensagens e ações de relatórios realizadas pelos servidores de e-mail. Configurar o SPF e o DKIM de acordo com o DMARC pode aprimorar a eficácia das defesas contra falsificações e ataques de phishing.

O que é BIMi?

BIMI (Brand Indicators for Message Identification) é um padrão que permite às empresas verificarem sua identidade em mensagens de e-mail usando logotipos. O principal objetivo do BIMi é combater o phishing, permitindo que os destinatários verifiquem se um e-mail realmente vem de uma empresa específica.

Quando uma empresa implementa o BIMl, ela pode configurar seu servidor de e-mail para incluir um cabeçalho especial (VBR-Info) em cada mensagem, contendo informações sobre onde o logotipo original da empresa pode ser encontrado. A empresa então coloca os dados relevantes no registro DNS para confirmar sua identidade.

Especificamente, isso envolve adicionar um “registro BIMl” às configurações de DNS do domínio. Este registro contém informações usadas para configurar o logotipo da empresa sob o padrão BIMl. Abaixo está uma descrição geral dos dados geralmente incluídos em um registro BIMl:

- **localização:** Especifica onde está localizado o logotipo da empresa, que pode ser um URL para a imagem do logotipo em um servidor web.
- **formato:** Especifica o formato do arquivo de imagem, como SVG, PNG ou outro formato suportado.
- **hash:** Um hash criptográfico da imagem do logotipo, atuando como uma “impressão digital” única para o arquivo. No BIMl, é usado para verificar se a imagem do logotipo não foi manipulada durante a transmissão do e-mail.

Um exemplo de registro BIMl no DNS pode se parecer com isso:

```
default._bimi.example.com IN TXT "v=BIMl1; l=https://example.com/logo.svg; h=sha256:abcdef123456..."
```

Neste exemplo:

- **v=BIMl1** indica que este é um registro compatível com a versão 1 do padrão BIMl.
- **l=https://example.com/logo.svg** aponta para a localização do logotipo da empresa (ou seja, a localização).
- **h=sha256:abcdef123456...** é o hash da imagem do logotipo

Esses dados permitem que os servidores de e-mail do destinatário verifiquem se o logotipo recebido é autêntico e se originou da empresa legítima.

Como funciona a verificação do BIMl?

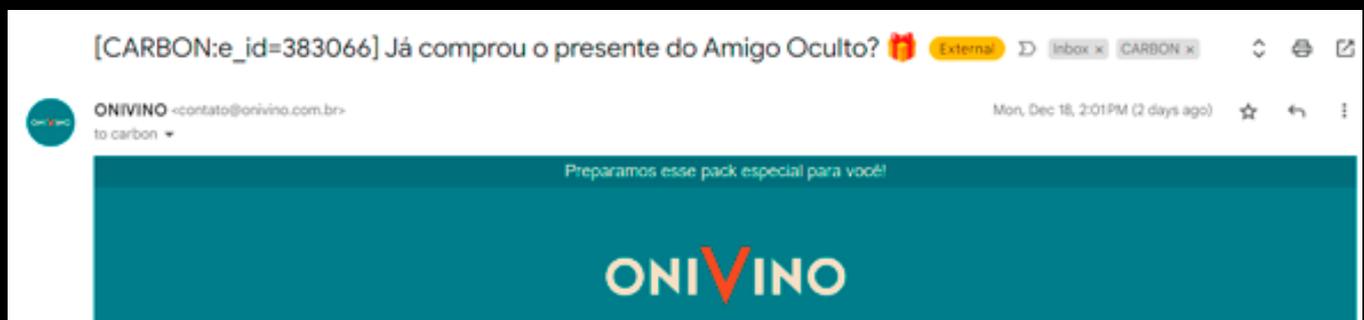
Quando o servidor receptor recebe um e-mail, ele analisa os cabeçalhos da mensagem, incluindo o cabeçalho VBR-Info adicionado pelo servidor de envio de acordo com o protocolo BIMl, e extrai informações sobre a localização, formato e hash do logotipo da empresa.

O servidor receptor pesquisa o DNS do domínio do remetente e compara com o cabeçalho contido no e-mail.

Se tal registro não existir ou se os dados não coincidirem com o cabeçalho no e-mail, a verificação pode falhar. Se a verificação DNS for bem-sucedida, o servidor receptor tenta buscar o logotipo no local especificado no registro BIML.

O servidor receptor então calcula o hash do logotipo baixado e compara com o valor de hash no registro de domínio DNS do endereço do remetente. Se esses dois valores coincidirem, significa que o logotipo não foi alterado e o e-mail está em conformidade com o padrão BIML implementado, indicando autenticidade.

Se todo o processo de verificação for bem-sucedido, a caixa de correio do destinatário pode exibir o logotipo da empresa próximo da mensagem de e-mail, auxiliando na identificação de remetentes genuínos e reduzindo o phishing.



Por que configurar o BIML?

Existem vários benefícios associados ao uso do BIML:

Construção de confiança

O BIML ajuda a aumentar a confiança dos destinatários nos e-mails, permitindo que as empresas confirmem sua identidade por meio da exibição do logotipo ao lado das mensagens de e-mail. Isso facilita a distinção de mensagens genuínas de possíveis golpes.

Identificação de remetentes confiáveis

Com o BIML, os destinatários podem identificar mais facilmente mensagens de e-mail de remetentes confiáveis, o que pode ser especialmente significativo no contexto de e-mails de marketing ou comunicações comerciais. Os usuários têm mais probabilidade de abrir um e-mail que não pareça suspeito.

Redução do risco de phishing

Ao permitir que os destinatários reconheçam rapidamente remetentes genuínos, o BIMl ajuda a reduzir o risco de ataques de phishing. Os destinatários estão mais inclinados a confiar em mensagens respaldadas por um logotipo visível da empresa.

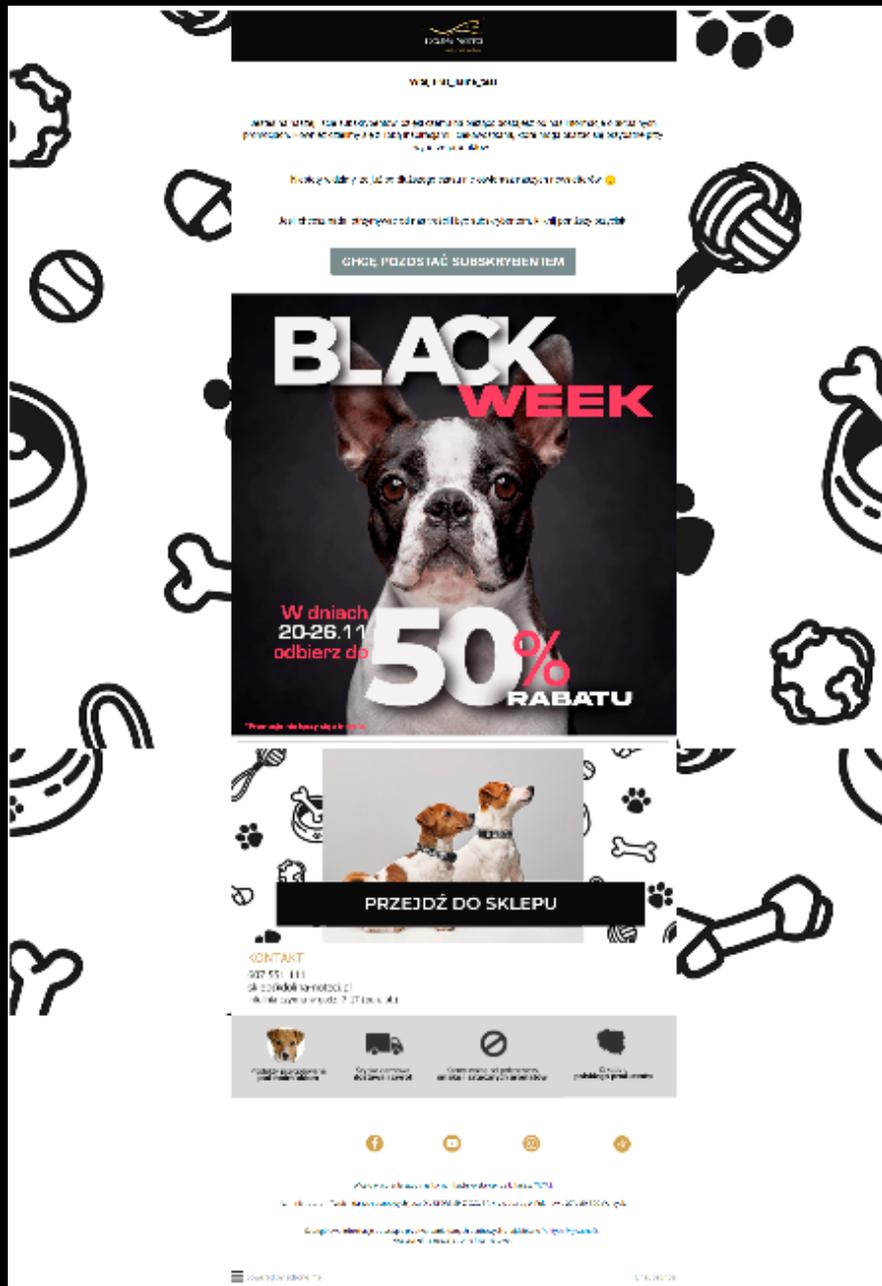
Melhoria na experiência do usuário

Adicionar um logotipo às mensagens de e-mail pode aprimorar a experiência geral do usuário, tornando-a mais atraente para os destinatários. Isso, por sua vez, torna a empresa mais reconhecível.

Padrão de segurança

O BIMl introduz um padrão para verificação e autenticação de mensagens de e-mail, aumentando a confiança geral na origem das mensagens. À medida que mais empresas implementam esse padrão, ele pode se tornar uma expectativa do setor, e a falta de tais medidas de segurança pode ser percebida como um risco potencial.

Vale ressaltar que a eficácia do BIMl depende se os remetentes de e-mail implementam esse padrão e se os destinatários usam clientes de e-mail que o suportam. Na prática, isso pode exigir colaboração entre diferentes empresas e provedores de serviços de e-mail.



Uma campanha de reativação do fabricante polonês de alimentos para cães e gatos Dolina Nocteci, no mercado há mais de 15 anos. O cliente decidiu usar a exportação do banco de dados CUSTOMERS FOR HIGIENCY oferecido pela edrone. Esses são clientes que não abrem uma mensagem há mais de 6 meses.

O cliente importou esse banco de dados exportado alterando o status da assinatura para desconhecido. Em seguida, ele preparou uma mensagem de botão com a ação de assinatura SUBSCRIBE, para que os clientes que quisessem permanecer no banco de dados tivessem a chance de responder. A campanha foi enviada para mais de 26.000 usuários inativos, foi aberta por 1.150 usuários e 250 usuários expressaram o desejo de permanecer no banco de dados.

Uma vez clicados, os clientes tiveram seu status de assinatura alterado para SUBSCRIBE e voltaram a receber comunicações regulares.

Passo 3: construa seu banco de dados com responsabilidade

Não compre - construa seu próprio banco de dados!

Comprar um banco de dados, apesar de parecer a maneira mais rápida e fácil de adquirir destinatários, é a pior opção e pode causar mais problemas do que benefícios.

Por que não comprar um banco de dados?

Existem pelo menos 5 razões para desencorajar isso:

SPAM e altas taxas de rejeição

Os destinatários de um banco de dados comprado podem considerar mensagens de uma fonte desconhecida como spam, levando a cancelamentos de inscrição ou marcando mensagens como suspeitas. Isso pode resultar em altas taxas de rejeição e, em última análise, até mesmo no bloqueio de mensagens do remetente.

Baixa qualidade dos bancos de dados comprados

Bancos de dados comprados de fontes desconhecidas frequentemente contêm informações de baixa qualidade, desatualizadas ou imprecisas, incluindo endereços de e-mail inativos. Isso pode levar a uma baixa eficácia nas campanhas de marketing e ao desperdício de recursos.

Armadilhas de spam

Tais bancos de dados podem conter armadilhas de spam, endereços inativos ou pouco utilizados criados para capturar remetentes que não verificam seus destinatários, compram bancos de dados ou não mantêm a higiene. Mensagens enviadas para esses endereços são marcadas como spam, e o endereço IP do remetente pode ser incluído em uma lista negra, danificando severamente a reputação.

Pouco interesse dos destinatários

Mesmo se forem evitados conflitos legais e armadilhas de spam, os destinatários podem simplesmente não se interessar pelo produto ou serviço descrito na mensagem. Há uma alta probabilidade de que tais mensagens sejam consideradas indesejadas, tornando as campanhas de marketing ineficazes na geração de leads reais e podendo prejudicar a reputação da marca.

Conflito legal e LGPD

A compra de um banco de dados de e-mails frequentemente viola princípios éticos e leis (LGPD), especialmente se os dados forem obtidos sem o consentimento explícito dos destinatários. Enviar um e-mail a um cliente que nunca se inscreveu voluntariamente no banco de dados pode acarretar em consequências legais - é simplesmente ilegal.

Em vez de comprar um banco de dados, é recomendado focar na construção de sua própria lista de assinantes por meio de práticas éticas de marketing, entregando conteúdo valioso e envolvendo regularmente os destinatários. Embora seja um processo mais desafiador, leva à fidelidade do cliente e a um marketing mais eficaz a longo prazo.

Como construir um banco de dados corretamente e de forma eficaz?

A maneira mais simples é usar um formulário de inscrição na newsletter no site. Ele deve ser visualmente atrativo e projetado para chamar a atenção do cliente. Um formulário cativante é fundamental, mas também é importante prestar atenção a certos problemas para coletar o banco de dados correta e eficazmente.

Em primeiro lugar, a conformidade com a LGPD é essencial:

- Deve-se fornecer informações claras sobre o que a inscrição implica.
- Deve-se fornecer informações claras sobre o que a inscrição implica.
- O formulário deve incluir uma caixa de seleção para consentimento em receber conteúdo de marketing.
- Se um formulário no site servir a um propósito diferente de assinatura, por exemplo, registro, mas também puder ser usado para coletar potenciais destinatários, é aconselhável adicionar uma caixa de seleção OPCIONAL com consentimento de marketing e informações sobre os benefícios da assinatura.
- As informações sobre o processamento de dados devem estar incluídas na política de privacidade e serem facilmente acessíveis e compreensíveis para os destinatários.
- É uma boa prática informar quem é o controlador de dados.
- É recomendado usar o modelo de confirmação dupla - um e-mail de confirmação é enviado para o endereço fornecido, e somente após expressar consentimento nesse e-mail é que o destinatário se torna um assinante.
- Os clientes também devem ter permissão para cancelar a inscrição quando não estiverem mais interessados no conteúdo.

Além disso, uma boa maneira de incentivar a inscrição é fornecer informações sobre a frequência das newsletters e o conteúdo específico que será entregue. Você também pode aprender com seu público quais tópicos especificamente os interessam e, em seguida, segmentar o banco de dados e enviar mensagens diferentes com base nos interesses dos destinatários - informações sobre essa personalização de conteúdo são valiosas, incentivadoras e ajudam a construir o banco de dados.

É importante lembrar que quanto mais curto o formulário, ou seja, exigindo o mínimo de dados do cliente, melhor. Hoje em dia, nem todos compartilham voluntariamente todas as informações sobre si mesmos, então vale a pena perguntar ao usuário apenas o que for necessário.

Incentivar o cliente com um pequeno presente no início, como um desconto, um ebook ou frete grátis, também é uma ótima ideia. Adquirir um destinatário de e-mail é uma transação - o destinatário compartilha seus dados (endereço de e-mail) e, em troca, recebe um bônus prático. Usar formulários dedicados, como pop-ups ou banners (por exemplo, Web layer), também é uma boa ideia. Quando exibidos em locais e horários específicos para não desencorajar os usuários, a inscrição por meio deles deve ser percebida como valiosa.

Coletar um banco de dados não é apenas possível no site; outras fontes, como as mídias sociais, também devem ser consideradas. Seguidores no Facebook ou Instagram nem sempre são assinantes de e-mail, então vale a pena incentivá-los por meio de campanhas apropriadas ou redirecioná-los para formulários de inscrição. Criar páginas de destino especiais para a assinatura de newsletters também é uma excelente ideia.

Uma ótima maneira de construir um banco de dados é por meio de indicações. Você pode usar um programa dedicado e envolver os assinantes existentes nesse processo. O destinatário atual, em troca de um bônus, recomenda a loja ou o site aos amigos, potenciais assinantes. É uma oportunidade perfeita para facilitar a inscrição de novos usuários.

A coleta offline de banco de dados também é possível, por exemplo, em uma loja física usando códigos QR. Escanear esses códigos levará o cliente para o mundo online, para uma página de inscrição dedicada. Eventos nos quais novos assinantes podem ser incentivados a se inscrever também são úteis.

Existem muitas maneiras de construir um banco de dados; no entanto, é essencial lembrar-se dos princípios básicos e recomendações para tornar esse processo eficaz e garantir que os assinantes estejam cientes, sejam voluntários e ansiosos para se inscreverem na newsletter.



5% OFF no seu primeiro vinho!

Faça parte da nossa Newsletter para ficar atualizado nas nossas novidades e receber ofertas.

Nome

Email

CADASTRAR!

Aceito a política de privacidade.

Pop-Up de Inscrição de Newsletter do cliente **CIA DO VINHO**



Descubra o mundo da moda sustentável

Inscreva-se para receber

10% OFF

E novidades exclusivas

Email

Nome

INSCREVER

Eu aceito a política de privacidade.

Pop-Up de Inscrição de Newsletter do cliente **RESERVA NATURAL**

Passo 4: aquecimento do endereço de IP e infraestrutura

Os provedores de serviços de e-mail são cautelosos quando se trata de atividade de e-mail de novos endereços IP. Os spammers frequentemente criam novos endereços IP e imediatamente começam a enviar grandes volumes de e-mails. Além disso, os provedores de serviços de e-mail continuamente desenvolvem e aprimoram seus mecanismos antispam. **Adotar uma abordagem excessivamente agressiva ao enviar grandes volumes de e-mails de um novo endereço IP ou com um novo provedor pode resultar em perda de confiança e inclusão em listas negras, levando a baixa entregabilidade.** Aquecer um endereço IP é o processo de aumentar gradualmente o número e a frequência de e-mails enviados a partir de um endereço IP específico. O objetivo é construir a reputação deste endereço aos olhos dos provedores de serviços de e-mail.

Por que isso deve te preocupar?

Se você estiver mudando de ferramentas, por exemplo, fazendo a transição para a edrone, e sua base de assinantes for superior a 10.000 contatos, você deve aquecer adequadamente sua infraestrutura de envio para garantir a entregabilidade de seus e-mails. O mesmo princípio se aplica se você optar por enviar via um IP dedicado. Novos clientes da edrone, tanto na infraestrutura compartilhada quanto na dedicada, devem seguir as recomendações e passar pelo processo de aquecimento. O mesmo processo deve ser aplicado se você registrou recentemente seu domínio

Como realizar o aquecimento?

O processo de aquecimento do IP é uma sequência cuidadosamente planejada de ações destinadas a construir gradualmente a reputação do remetente antes de enviar um grande volume de e-mails. O aquecimento da infraestrutura é um processo gradual que pode ser dividido em etapas:

1 Comece com baixo volume:

Comece limitando o número de e-mails enviados. Escolha um pequeno segmento de assinantes ou os destinatários mais importantes e altamente ativos. Envie conteúdo de alto valor que você espera que receba uma resposta positiva.

2 Aumento gradual de volume:

Aumente gradualmente o número de e-mails enviados ao longo do tempo. Evite aumentos súbitos, mas aumente constantemente a quantidade. Monitore a atividade dos assinantes, as reações aos e-mails e as métricas de entregabilidade. Recomenda-se que a primeira campanha seja enviada para menos de 10.000 destinatários. Aumente lentamente o número de e-mails enviados a cada campanha subsequente. Dobre a quantidade de mensagens enviadas a cada três ou quatro dias até atingir a quantidade máxima diária.

3 Foque no engajamento do assinante:

Concentre-se em manter um alto nível de engajamento dos assinantes, incluindo aberturas, cliques e evitando marcações como spam. Evite enviar para assinantes que não reagem aos seus e-mails para evitar um impacto negativo na reputação do remetente.

4 Monitoramento de métricas e reputação:

Verifique regularmente métricas de entregabilidade, como % de entregabilidade, retornos e reclamações de spam.

5 Ajuste o ritmo com base nos resultados:

Se perceber problemas de entregabilidade ou reações negativas dos assinantes, ajuste o ritmo de crescimento. Tome ações corretivas, se necessário, como identificar e remover assinantes problemáticos.

6 Qualidade do conteúdo do e-mail:

Garanta um conteúdo de e-mail de alta qualidade. Evite o uso de palavras e frases frequentemente associadas a spam. Certifique-se de que o conteúdo seja personalizado e adaptado às expectativas dos assinantes.

7 Consulta com especialistas:

É aconselhável consultar especialistas em implementação ou Gerentes de Sucesso do Cliente para adaptar a estratégia de aquecimento de acordo com suas necessidades.

8 Otimização de conteúdo para caixas de entrada:

Garanta que o conteúdo do e-mail seja otimizado para exibição em várias caixas de entrada de diferentes provedores. A consistência no conteúdo pode impactar positivamente a classificação de qualidade de seus e-mails.

9 Planejar o processo de aquecimento:

O processo de aquecimento provavelmente levará cerca de 30 dias, mas pode variar com base na:

- quantidade de e-mails enviados,
- qualidade da lista de assinantes,
- frequência de envio.

AOL, Outlook.com e Gmail geralmente exigem um período de aquecimento mais longo.

10 Esperar desafios iniciais:

Esteja preparado para resultados potencialmente mais baixos inicialmente.

Durante a primeira ou segunda semana, podem ocorrer desafios de entrega à medida que a nova infraestrutura de envio constrói sua reputação. Isso depende da qualidade dos assinantes e das práticas de marketing por e-mail. Alguns provedores verificam se os assinantes estão recebendo e marcando e-mails como “não spam”. Assinantes que marcam e-mails como “não spam” são um indicador positivo usado pelos provedores de e-mail para percebê-lo como um remetente legítimo. Portanto, enviar e-mails envolventes para quem os deseja é crucial.

Se surgirem problemas de entregabilidade, pause ou reduza os volumes para permitir que os filtros antispam se ajustem aos novos endereços IP. Suspenda o envio para provedores com bloqueios de política, resolva os problemas e elimine a causa. Retome o envio somente após resolver o problema. Certifique-se de que o processamento de reclamações e retornos estejam funcionando corretamente.

Verifique se você enviou acidentalmente para toda a lista ou para um grande número de assinantes não engajados. Se sim, mantenha os volumes nos níveis atuais por alguns dias e, em seguida, reinicie conforme o plano original de aquecimento, garantindo que você envie imediatamente para os assinantes engajados.

RESUMO

O processo de aquecimento de endereços IP e infraestrutura é um elemento chave de campanhas eficazes de marketing por e-mail. Compreender e seguir este processo pode impactar significativamente a reputação do remetente e melhorar a entregabilidade de e-mails, resultando em sucesso de comunicação e de marketing. O aquecimento da infraestrutura é um processo crucial e negligenciá-lo pode levar à perda de confiança dos provedores de serviços de e-mail e à baixa entregabilidade.

Passo 5

Passo 5: aquecimento do endereço de IP e infraestrutura

As métricas de entrega de e-mail desempenham um papel crucial na avaliação da eficácia das campanhas de e-mail. Elas informam ao remetente se suas mensagens estão alcançando os destinatários pretendidos ou acabam na pasta de spam. Compreender essas métricas permite ajustes estratégicos, aumentando assim as chances de alcançar os objetivos de marketing.

Nesse contexto, indicadores como Taxa de Abertura, Taxa de Cliques, Taxa de Reclamação de Spam e Taxa de Rejeição se tornam partes integrantes das estratégias de marketing. Essas métricas não são apenas números na tela; elas servem como um mapa orientando o caminho para uma comunicação eficaz. A Taxa de Abertura revela o apelo e a eficácia das linhas de assunto do e-mail, a Taxa de Cliques indica o engajamento da audiência, a Taxa de Reclamação de Spam reflete a qualidade do conteúdo e a Taxa de Rejeição significa a limpeza da lista.

Quais métricas analisar:

Taxa de entrega:

A taxa de entrega refere-se ao percentual de mensagens entregues com sucesso entre todas as enviadas. Ela representa o número de e-mails que chegaram às caixas de entrada dos destinatários em comparação com o número de e-mails enviados pelo remetente. No marketing por e-mail, a taxa de entrega é a porcentagem de mensagens que você envia e são recebidas pelos provedores de serviços de e-mail dos seus destinatários. A taxa de entrega de e-mail é calculada dividindo o número de mensagens enviadas para assinantes pelo número total de e-mails enviados.

Taxa de abertura:

Esta é uma métrica que mede o percentual de destinatários que abriram uma mensagem de e-mail específica em relação ao número total de destinatários que receberam essa mensagem. É uma medida importante, pois indica o quão efetivamente o conteúdo dos e-mails captura a atenção dos destinatários. No entanto, vale ressaltar que alguns programas de e-mail não registram aberturas de mensagens se o destinatário não baixar o conteúdo do e-mail (por exemplo, exibir imagens em HTML), então a Taxa de Abertura pode não ser um reflexo totalmente preciso do engajamento ou interesse real no conteúdo. A taxa de abertura média para a maioria das indústrias está dentro da faixa de 15% a 25%. No entanto, existem indústrias, como e-commerce, educação ou estilo de vida, onde taxas mais altas podem ser alcançadas, chegando até mesmo a 30-40%.

Taxa de cliques (CTR):

A Taxa de Cliques (CTR) é uma medida que determina o percentual de destinatários que clicaram em links ou botões em uma mensagem de e-mail em relação ao número total de destinatários que receberam essa mensagem. A CTR é calculada como o número de cliques dividido pelo número de e-mails enviados, depois multiplicado por 100 para obter a porcentagem. O valor da CTR pode variar significativamente dependendo da indústria, tipo de oferta ou clareza das ações a serem realizadas pelos destinatários. Geralmente, uma boa CTR em uma campanha de e-mail pode variar de 2% a 5%, mas em alguns casos, especialmente com conteúdo bem otimizado e ofertas precisamente adequadas, pode ser mais alta.

Taxas de reclamação de spam:

Essa métrica identifica o percentual de destinatários que relataram ter recebido um e-mail específico como spam em relação ao número total de destinatários que o receberam. Uma boa Taxa de Reclamação de Spam geralmente se mantém em um nível baixo, frequentemente abaixo de 0,1% ou até mesmo menor. Taxas altas podem levar a problemas de reputação do remetente e impactar negativamente a eficácia da campanha de e-mail.

Taxas de cancelamento de inscrição:

Esse indicador determina o percentual de destinatários que optaram por cancelar a inscrição na lista de e-mails após receberem uma mensagem específica. É uma métrica importante porque mostra quantas pessoas consideram o recebimento de mais mensagens como desinteressante ou que não estão mais alinhadas com suas expectativas. Existem muitos fatores que podem influenciar a taxa de cancelamento de inscrição, como a frequência de envio de e-mails, a qualidade e relevância do conteúdo para os destinatários ou o momento da entrega. Portanto, monitorar esse indicador e analisar os motivos pelos quais os destinatários optam por cancelar a inscrição na lista de e-mails é crucial. Uma boa taxa de cancelamento de inscrição depende da indústria e das especificidades de uma campanha específica, mas geralmente, uma taxa baixa variando de 0,1% a 0,5% é considerada satisfatória.

Taxas de rejeição:

A taxa de rejeição no contexto de uma campanha de e-mail refere-se ao percentual de mensagens de e-mail que não foram entregues nas caixas de entrada dos destinatários devido a vários problemas.

As rejeições podem ser divididas em dois tipos principais: rejeições “rígidas” e rejeições “suaves” (hard bounces e soft bounces).

Hard bounces ocorrem quando uma mensagem não pode ser entregue devido a problemas permanentes, como um endereço de e-mail inexistente ou bloqueado pelo servidor como inválido. Esses erros são permanentes e exigem intervenção, como remover o endereço incorreto da lista de e-mails.

Soft bounces são problemas temporários de entrega que podem ser causados por uma caixa de entrada cheia, problemas temporários com o servidor de destino, etc. Essas mensagens às vezes podem ser entregues após uma tentativa subsequente.

Uma taxa de rejeição baixa é desejável porque uma taxa alta de rejeição pode impactar negativamente a reputação do remetente e a eficácia da campanha de e-mail. Os padrões aceitos frequentemente sugerem que a taxa de rejeição deve ficar abaixo de 2-3%. No entanto, esse valor pode variar dependendo da indústria ou das especificidades da lista de destinatários. Monitorar e gerenciar a taxa de rejeição são essenciais para manter a limpeza da lista de destinatários e melhorar a eficácia da campanha, eliminando endereços de e-mail incorretos e diagnosticando problemas na entrega de mensagens.

Passo 6

Passo 6: para aumentar o engajamento, envie para clientes engajados

O que é engajamento e por que é tão importante?

Nas redes sociais, os usuários se engajam com publicações quando interagem com uma marca específica. Essas interações podem ser medidas por meio de “curtidas”, “comentários” e “compartilhamentos”. Da mesma forma, em e-mails, o engajamento é entendido de maneira comparável. O engajamento por e-mail é medido por provedores de serviços de e-mail como Gmail, Outlook e Yahoo, usando métricas como aberturas, cliques e respostas, entre outros dados comportamentais, para filtrar mensagens que chegarão ou não às caixas de entrada dos usuários. Os servidores de e-mail têm mecanismos para monitorar o comportamento do usuário, aprendendo mais sobre suas preferências conforme enviam e recebem e-mails. Eles também incorporam recursos anti-spam para “proteger” os usuários de conteúdos indesejados. Por exemplo, se um usuário habitualmente exclui e-mails sobre tópicos específicos mesmo antes de abri-los, o serviço de e-mail entende que deve bloquear essas mensagens. Essas informações são armazenadas pelo servidor para personalizar cada vez mais o serviço.

Como medir o engajamento em campanhas de e-mail?

Fala-se muito sobre engajamento do usuário, mas como você o mede e observa no marketing por e-mail? Monitore indicadores específicos como:

Taxa de abertura

Esta métrica indica a porcentagem de e-mails abertos em relação ao total entregue. A taxa média de abertura de e-mails varia por setor (educação, construção, saúde, etc.), mas essa porcentagem mostra quantas pessoas estão interessadas no seu conteúdo.

Taxa de cliques (CTR)

Esta é a proporção de cliques em links nos criativos de e-mail em relação a todas as mensagens entregues corretamente. Indica o número de cliques em links nos e-mails entregues. Cada clique significa interesse, permitindo o ajuste das estratégias de marketing. Sem acompanhar a CTR, você não consegue identificar o impacto da sua campanha de e-mail na sua audiência.

Taxa de cancelamento de inscrição

Mede a porcentagem de usuários que decidiram sair da sua lista de e-mails. Uma alta taxa de cancelamento sinaliza os provedores de serviços de e-mail e pode ter consequências negativas. Nem todos os interesses dos usuários podem ser atendidos; a taxa de cancelamento esperada é de 0,5% e 0,2% ou menos é considerado bom. Se o número for maior, sua estratégia de marketing precisa de melhorias. No entanto, isso não deve ser levado muito radicalmente para uma empresa nova ou uma nova lista de e-mails, já que os relacionamentos com os destinatários estão se desenvolvendo nesses casos.

BOAS PRÁTICAS E DICAS PARA MELHORAR O ENGAJAMENTO POR E-MAIL

Fale sobre o que é interessante para o cliente

Enviar conteúdo personalizado e relevante para assinantes pode incentivá-los a interagir com sua marca. Isso pode levar a um aumento nas taxas de cliques, visitas ao site e engajamento nas redes sociais. Segundo pesquisas, 70% das pessoas afirmam sempre ler e-mails de suas empresas favoritas. Em outras palavras, é um método eficaz para manter um bom relacionamento com sua audiência.

Preste atenção ao assunto do e-mail

O assunto do e-mail não é apenas um título. Ele é responsável pelas aberturas, uma das primeiras métricas a serem analisadas. Ao criar um assunto, considere o que seus assinantes realmente querem ou precisam. Por que eles se inscreveram na sua newsletter? O que despertaria o interesse deles? Comunique claramente sobre o que é o e-mail, mas evite revelar detalhes impactantes. Dê aos seus assinantes um pequeno trecho de informação que os faça abrir sua mensagem por curiosidade. Em resumo: o assunto deve ser claro, curto, adaptado aos destinatários e despertar curiosidade. Não há uma regra específica, então você precisa testar diferentes opções e analisar os resultados das suas campanhas para descobrir quais assuntos geraram a maior Taxa de Abertura. Os títulos de e-mail são uma ótima variável para experimentar em testes A/B. Mudar alguns detalhes muitas vezes resulta em resultados surpreendentes!

Além disso:

- Evite usar mais de 50 caracteres.
- Evite o uso excessivo de pontuação e emoticons.
- Evite gritar! Evite o uso de letras maiúsculas.
- Prefira emoticons que façam sentido para o seu negócio.
- Use variáveis, como |NOME|, para chamar atenção na caixa de entrada.
- Intrigue, cativa.

Transformar dados em ação

Na edrone, você coleta dados pessoais como datas de nascimento, cidade, país e dados comportamentais: produtos visualizados, adicionados ao carrinho, valores de pedidos, entre outros. Para melhorar a entregabilidade e as métricas de engajamento dos destinatários, recomendamos personalizar mensagens e usar esses dados.

Personalizar

Adicionar o nome do destinatário no e-mail ou no assunto da mensagem e personalizar o conteúdo com base em recomendações de produtos criadas a partir do histórico de compras do cliente pode aumentar o engajamento e, conseqüentemente, melhorar a entregabilidade.

Incentivar assinantes a encaminhar e-mails

Como você provavelmente sabe, interações em mídias sociais são classificadas usando vários sistemas de pontuação. Vamos usar o Facebook como exemplo. Você pode ver uma postagem e simplesmente clicar em “curtir”, e o algoritmo do Facebook interpretará isso como um interesse no conteúdo. Se você comentar na postagem, o algoritmo considerará que você está um pouco mais interessado - está disposto a expressar seus pensamentos sobre o tema. Se você compartilhar, é um sinal ainda mais forte. Encaminhar e-mails é avaliado positivamente pelos filtros de spam. O que você pode fazer para aumentar as chances disso? Devo salientar que não é um assunto simples. Você pode criar suas ofertas de forma que os destinatários se beneficiem ao compartilhá-las, por exemplo, oferecendo descontos em grupo ou usando links afiliados. Lembre-se de que às vezes, apenas pedir ou persuadir é o suficiente! Digamos que você esteja criando uma newsletter promocional para o Dia dos Namorados. “Compartilhe esta mensagem com seus amigos para que eles não se esqueçam de comprar um presente para seus entes queridos!”

Seja criativo

Diferentes formas de agrupar clientes ajudam a enviar conteúdo relevante para cada grupo, aumentando seu engajamento. É essencial lembrar que cada um desses grupos terá necessidades diferentes. Usando o exemplo de uma loja de artigos esportivos, clientes que apoiam o São Paulo não gostariam de receber e-mails promovendo camisas do Corinthians. Isso poderia até resultar em cancelamento da assinatura da newsletter. Quanto mais diversificado o banco de dados, mais conteúdo específico é enviado.

Incentivar interação - CTAs envolventes

O botão de call-to-action é um elemento-chave de interação projetado para encorajar os usuários a realizar ações específicas. O texto deve ser curto, conciso, cativante, por exemplo, “Entrar”, “Verificar”, “Descobrir”. Também vale a pena escolher uma cor que contraste com o fundo, mas se encaixe no estilo geral do criativo. Além disso, coloque o botão no topo da mensagem para que seja visível acima da dobra do e-mail, sem a necessidade de rolar.

Garanta um design de e-mail atraente

Projete seu e-mail para ser claro, conciso e esteticamente atraente. Adicione gráficos e elementos visuais apropriados que enfatizem a mensagem. O uso de GIFs, como exibições de produtos animados, pode ser eficaz. Os contadores regressivos que mostram o tempo restante para promoções também têm impacto.

Não seja monótono, entregue valor

Enviar e-mails com muita frequência pode irritar os destinatários. Enviar muitos e-mails promocionais pode parecer uma boa estratégia para não ser esquecido e comunicar benefícios, mas vá devagar. Ver a sua empresa na caixa de entrada todos os dias pode gerar reclamações.

Sua campanha de reengajamento

Não é incomum que um certo percentual de assinantes não reaja aos seus e-mails por vários meses. Alguns usuários perdem interesse ou param de usar o endereço de e-mail para o qual você envia mensagens. Uma campanha de re-engajamento visa os assinantes passivos com o objetivo de reacender o interesse deles. No entanto, antes de direcionar uma campanha de re-engajamento para um assinante passivo, é necessário entender o que fez com que eles perdessem interesse.



OUTLET | FEMININO | MASCULINO | NOVIDADES | BÁSICOS

O melhor presente
é aquele que traz um sorriso ao rosto do nosso amigo secreto.

CONFIRA

Amigo Secreto
Seleção de FAVORITOS

COMPRA AGORA

Presentes
Até R\$150,00

COMPRA AGORA

Campanha criada para a marca **KAUÊ PLUS SIZE**. Foi preparada uma campanha de newsletter para toda a base, com o objetivo de aumentar o número de cliques na newsletter e o número de visitas ao site.

oi,Bem!

BEBÊ | INFANTIL | FEMININO | OI,DESCONTO

ÚLTIMO DIA

CYBER MONDAY

ÚLTIMA
CHANCE!

MODA FEMININA E PLUS ATÉ

70% OFF

+

FRETE GRÁTIS

NAS COMPRAS ACIMA DE R\$149

COMPRE AGORA!



Campanha criada para a marca **OI, BEM!**. Foi preparada uma campanha de newsletter com o objetivo de aumentar o número de vendas através de uma promoção no site.



Celulares

Smartwatch

Casa

Viagem e Lazer

Beleza e Saúde

Áudio

Ofertas

LANÇAMENTO

XIAOMI Smart Band 8

Estilo em cada atividade



COMPRE AGORA

Campanha criada para a marca **MI BRASIL**. Foi preparada uma campanha de newsletter com o objetivo de aumentar o número de vendas através de um lançamento de um novo produto.

Passo 7: use segmentação

A segmentação no marketing por e-mail desempenha um papel crucial na melhoria da entrega das mensagens. Através da segmentação, você pode personalizar o conteúdo do e-mail para grupos específicos de destinatários com base em suas preferências, comportamentos ou dados demográficos. Conteúdo mais personalizado e adaptado aumenta a probabilidade de que os destinatários percebam a mensagem como valiosa, impactando positivamente a taxa de abertura.

A segmentação também permite um melhor alinhamento do conteúdo com os interesses dos destinatários, reduzindo o risco de enviar e-mails indesejados. Através da segmentação, é possível evitar situações em que os e-mails sejam tratados como spam devido ao agrupamento inadequado de destinatários.

Use segmentos

Usando interesses:

Pense no que faz sentido para o seu negócio. Se for uma loja de artigos esportivos, a segmentação com base no time favorito e nos esportes praticados pode ser uma boa ideia.

Usando comportamentos anteriores:

Monitore a atividade do usuário no site, na loja online. Colete dados sobre produtos visualizados, adicionados ao carrinho, compras, etc., e depois crie segmentos com base nas preferências de produto e comportamentos de compra. Segmentar a lista de contatos com base em seus comportamentos de compras anteriores, interesses e preferências pode aumentar a precisão dos e-mails enviados, resultando em uma taxa de abertura maior.

Segmentação com base no ciclo de vida do cliente:

Divida seus assinantes em segmentos dependendo do estágio em que se encontram no ciclo de vida do cliente (por exemplo, novos assinantes, clientes fiéis, possíveis cancelamentos).

Personalize o conteúdo de acordo com as necessidades de cada grupo, fornecendo informações valiosas com base no estágio em que estão.

Segmentação usando RFM:

Use a segmentação RFM para obter os melhores resultados em seus esforços de marketing por e-mail. RFM significa Recência (quando foi feita a última compra), Frequência (com que frequência as compras são feitas) e Valor Monetário (o valor dessas compras). Envolve categorizar os clientes em 10 categorias. Isso permite identificar e valorizar clientes fiéis e também lutar por aqueles que, por algum motivo, pararam de visitar sua loja.

Envie para os engajados:

Enviar mensagens para clientes que regularmente abrem e-mails é crucial para a entregabilidade de e-mails. Clientes que regularmente abrem seus e-mails mostram maior engajamento. Ao enviar a eles informações adicionais, ofertas ou conteúdo adaptado às suas preferências, você aumenta as chances de manter a atenção deles. Se os destinatários abrem seus e-mails, é mais provável que cliquem nos links dentro deles. Ao fornecer conteúdo que corresponda aos seus interesses, você aumenta as chances de gerar cliques. Empresas de entregabilidade de e-mails monitoram as interações dos destinatários com um determinado remetente. Enviar conteúdo para destinatários ativos afeta positivamente sua reputação como remetente, contribuindo para uma melhor entregabilidade geral. Destinatários que abrem seus e-mails geralmente não os marcam como spam. Cuidar desse segmento ajuda a reduzir o risco de suas mensagens acabarem na pasta de spam. Além disso, ao enviar mensagens para destinatários ativos, você tem a oportunidade de uma personalização de conteúdo mais precisa. Você pode adaptar ofertas, informações ou recomendações às suas interações anteriores. Os leitores regulares são um segmento valioso que pode ser segmentado com base em comportamentos específicos. Isso permite fornecer um conteúdo ainda mais personalizado. Em resumo, enviar mensagens para clientes que abrem e-mails não apenas aumenta a eficácia das campanhas, mas também impacta positivamente a reputação do remetente e a entregabilidade de e-mails.

Aproveite o ciclo de engajamento do cliente no **marketing por e-mail**

No cenário atual de marketing por e-mail, há uma compreensão comum da importância do ciclo de engajamento do cliente com as mensagens entregues. Com base nas interações, esse ciclo é dividido em cinco seções-chave, cada uma exigindo uma abordagem individual:

Engajamento ativo (0-30 dias desde a última interação) - Os destinatários estão ativos, respondendo às mensagens e mostrando interesse. Este é o momento ideal para fornecer conteúdo sobre as últimas ofertas, promoções ou informações.

Engajamento recente (30-90 dias) - Destinatários que estavam ativos, mas suas interações diminuíram ligeiramente. É essencial manter o interesse deles fornecendo conteúdo adaptado às suas preferências anteriores.

Falta de engajamento (3-6 meses) - Um grupo que perdeu atividade. Nesse caso, implementar uma estratégia de reativação é valioso, oferecendo benefícios únicos, promoções ou incentivos para encorajar um retorno.

Necessidade de reengajamento (6-12 meses) - Destinatários nesta fase provavelmente começaram a perder interesse. É crucial fornecer conteúdo que atualize sua memória e lembre-os do valor do seu produto ou serviço.

Inativos (12+ meses) - Assinantes que não abriram e-mails por um período prolongado. Considerar estratégias de reativação é importante, mas ao mesmo tempo, deve-se ter cuidado para manter a lista removendo endereços inativos.

Para cada setor e domínio, a quantidade e o tipo de interações podem variar. diferentes soluções dentro do contexto do ciclo de engajamento é crucial.

Passo 8: cuide do conteúdo

A maneira como você formula o conteúdo do seu e-mail pode impactar significativamente a construção de um relacionamento com o cliente. Por quê?

Porque o que você diz no assunto do e-mail determina se ele será aberto e como você o constrói pode influenciar se será entregue ou não. E-mails bem elaborados, seguindo princípios amplamente aceitos, alcançam os destinatários enquanto driblam os filtros de spam e incentivam a interação do usuário, afetando positivamente a entregabilidade futura. Essa espiral ascendente melhora consideravelmente sua entregabilidade geral.

A evolução dos filtros de spam usados pelos Provedores de Serviços de Internet (ISPs) enfatiza a importância do conteúdo, já que spammers empregam várias táticas para evitar métodos baseados em reputação.

Apesar dos principais provedores de serviços de e-mail não detalharem explicitamente o formato ideal para um e-mail chegar à caixa de entrada, eles oferecem conselhos valiosos e princípios gerais para orientar a comunicação. Além disso, a indústria de marketing por e-mail fornece vários princípios-chave para remetentes que criam mensagens de e-mail em massa.

Nossos conselhos:

Mantenha uma alta proporção de texto para links

Manter uma proporção credível e relevante de texto para links é crucial para evitar filtros de spam e oferecer um valor real de conteúdo aos assinantes. Limitar os links, especialmente em e-mails promocionais, aumenta a credibilidade e se alinha com as preferências dos ISPs.

Mantenha uma alta proporção de texto para imagem

Os ISPs prestam atenção ao equilíbrio entre imagens e texto. As proporções recomendadas são tipicamente de 60%-40% ou 70%-30%, com o texto tendo o valor mais alto. Uma mensagem composta apenas por imagens aciona alertas de spam, destacando a importância de combinar imagens com texto real.

Uso consistente de modelos

Modelos consistentes ajudam os ISPs a identificá-lo como remetente, atuando como uma impressão digital que contribui para sua reputação como remetente. Embora a inovação seja essencial, mudanças frequentes nos modelos podem impactar negativamente a entregabilidade, enfatizando o valor da continuidade.

Evite palavras suspeitas

Certas palavras ou frases podem acionar filtros de spam, e é aconselhável evitá-las. Enquanto termos específicos associados diretamente a anúncios médicos ou de relacionamento geralmente são sinalizados, o uso de palavras como “grátis”, “compre agora” ou “tempo limitado” requer moderação para uma abordagem equilibrada.

Use palavras com sabedoria

Enquanto palavras como “grátis”, “compre agora” ou “ótima oferta” são aceitáveis, use-as com parcimônia. O uso excessivo desses termos afeta negativamente a percepção do e-mail, enfatizando a importância da moderação tanto para marketing eficaz quanto para filtragem de conteúdo.

Evite truques

Tentar esconder ou disfarçar conteúdo através de táticas como espaçamento de letras ou pontuação pode levar à detecção e classificação como spam. Transparência e comunicação direta são preferíveis a tentativas de manipulação.

Teste antes de enviar

Realizar testes A/B antes de lançar uma campanha em massa garante que o e-mail seja legível em vários dispositivos e evite pastas de spam. Testar a responsividade em smartphones, tablets e computadores ajuda a evitar problemas de exibição em diferentes plataformas, contribuindo para uma experiência positiva do usuário.

Teste em vários clientes de e-mail

Enviar e-mails de teste para diferentes contas é crucial para refinar estratégias de entregabilidade. Analisar reações em várias plataformas ajuda a ajustar o conteúdo e os elementos estruturais para minimizar o risco de classificação como spam. Uma configuração adequada, testada em várias contas, aumenta a confiança de que os destinatários recebam mensagens em sua caixa de entrada principal, aumentando a eficácia das campanhas de e-mail.

Personalize o conteúdo para o estágio da jornada do cliente

Adaptar o conteúdo ao estágio atual da jornada do cliente permite a criação de conteúdo relevante e ajustado com precisão, aumentando a probabilidade de engajamento. Abordar a conscientização da marca no início, fornecer conteúdo educacional na fase de interesse e oferecer ofertas personalizadas durante a fase de compra não apenas melhora a interação do destinatário, mas também minimiza o risco de ser marcado como indesejado.

Passo 9: envie regularmente

O envio de boletins informativos em excesso pode ter um impacto negativo na entregabilidade de e-mails que pode ser influenciado por vários fatores relacionados à frequência do envio de boletins informativos:

Aumento do risco de ser classificado como spam: Se você enviar muitas mensagens em um curto período, há o risco de que seus e-mails sejam considerados spam. Os serviços de e-mail utilizam filtros de spam que podem identificar atividades de envio excessivo como suspeitas.

Fadiga do destinatário: Bombardear regularmente os destinatários com mensagens pode levar à fadiga e perda de interesse. Os destinatários podem começar a ignorar seus e-mails ou até mesmo marcá-los como spam.

Aumento nas taxas de rejeição e cancelamento de inscrição: O envio excessivo pode levar a taxas mais altas de rejeição e cancelamento de inscrição. Isso, por sua vez, pode afetar negativamente sua reputação como remetente.

Redução no engajamento: Mensagens muito frequentes podem resultar em uma diminuição no engajamento do destinatário. Isso, por sua vez, pode afetar como os algoritmos de e-mail avaliam a qualidade de suas mensagens.

Para minimizar os efeitos negativos, considere implementar as seguintes práticas:

Segmentação da lista de assinantes: Ajuste a frequência de envio para diferentes grupos de destinatários com base em suas preferências e comportamentos.

Monitoramento de métricas de engajamento: Verifique regularmente métricas como taxas de abertura, taxas de cliques, taxas de rejeição e taxas de cancelamento de inscrição. Responda adequadamente aos sinais de diminuição do engajamento.

Testes A/B: Realize testes A/B para identificar a frequência ideal de envio para seu público.

Respeite as preferências dos assinantes: Dê aos assinantes a opção de escolher a frequência de recebimento de mensagens.

É importante observar que a frequência ideal de envio pode variar dependendo do setor, tipo de conteúdo e preferências do público-alvo. Monitorar regularmente os resultados e ajustar as estratégias é crucial para manter uma entregabilidade saudável de e-mails.

O envio irregular de boletins informativos também pode impactar a entregabilidade, embora de maneira diferente do envio excessivo. **Aqui estão algumas considerações para o envio irregular:**

- **Incerteza do destinatário:** O envio irregular pode deixar os destinatários incertos sobre quando esperar a próxima mensagem sua. Isso pode levar a um engajamento reduzido, já que os destinatários podem estar inseguros se vale a pena permanecer inscritos.
- **Risco de esquecimento:** Se você enviar mensagens de forma muito irregular, há o risco de os destinatários simplesmente esquecerem sua empresa ou conteúdo, o que pode afetar as taxas de abertura e o engajamento.
- **Flutuações nas taxas de abertura:** Os algoritmos dos provedores de e-mail podem reagir ao envio irregular, impactando as taxas de abertura. A regularidade pode ajudar a manter métricas de engajamento estáveis.
- **Dificuldade em construir relacionamentos:** A comunicação regular com os destinatários permite a construção de relacionamentos duradouros. O envio irregular pode complicar a manutenção desses relacionamentos, especialmente se os destinatários não perceberem um engajamento consistente da sua parte.

Para minimizar os efeitos negativos do envio irregular, considere as seguintes ações:

- **Estabeleça um plano de envio:** Embora a irregularidade possa ser compreensível às vezes, é valioso estabelecer algum tipo de plano de envio, mesmo que não seja um cronograma mensal. Por exemplo, se você enviar boletins informativos em resposta a eventos importantes, informe os destinatários sobre o plano de envio.
- **Notifique sobre mudanças:** Se você planeja alterações na frequência de envio, informe seus assinantes. Comunique claramente por que essas mudanças estão ocorrendo.
- **Monitore o engajamento:** Monitore de perto métricas como taxas de abertura, taxas de cliques e outros indicadores de engajamento para avaliar como o envio irregular afeta as reações dos destinatários. No caso de envio irregular, é crucial entender que os destinatários são diversos, e ajustar estratégias para as especificidades do seu público-alvo é essencial.

Passo 10: faça testes A/B

Os testes A/B não apenas impactam o conteúdo e a eficácia das campanhas de e-mail, mas também desempenham um papel crucial na melhoria da entregabilidade.

○ que testar:

Eficácia da linha de assunto

Os testes A/B permitem a comparação de diferentes variantes de linhas de assunto de e-mail, influenciando significativamente as decisões dos destinatários de abrir mensagens. Melhorar a linha de assunto pode aumentar a taxa de abertura, impactando como os filtros de spam percebem a mensagem.

Personalização do endereço do remetente

Experimentos com a personalização do endereço do remetente ajudam a identificar se os assinantes respondem melhor a mensagens de um indivíduo específico ou da própria empresa. Ajustar adequadamente esse elemento pode aumentar a confiança entre os destinatários e minimizar o risco de mensagens serem tratadas como spam.

Otimização do horário de envio ideal

Testar diferentes horários e dias para o envio de e-mails permite a identificação dos momentos em que os destinatários têm mais probabilidade de abrir e responder às mensagens. Entregar conteúdo no momento ideal aumenta a chance de uma recepção positiva.

Testes de conteúdo

Experimentos com vários elementos de conteúdo, como texto, gráficos ou layout, podem influenciar a avaliação da qualidade da mensagem pelos filtros de spam. Melhorar a qualidade do conteúdo pode reduzir o risco de mensagens serem classificadas como indesejadas.

Customização do comprimento do conteúdo

Os testes A/B ajudam a determinar o comprimento ideal do conteúdo que mantém a atenção dos destinatários. Conteúdo excessivamente longo pode ser interpretado como spam, sendo essencial encontrar um equilíbrio entre informações e clareza.

Teste de CTA (chamada para a ação)

A Chamada para Ação (CTA) desempenha um papel crucial na eficácia da campanha. Testes A/B permitem a identificação de formulações de CTA que geram mais interações. A redação precisa e o posicionamento estratégico do CTA impactam na avaliação dos filtros de spam sobre o conteúdo.

Esses são os princípios-chave anti-spam para orientá-lo, mas encorajamos experimentação e atualização das melhores práticas de conteúdo. As regulamentações do cenário de e-mails mudam e estar atualizado sobre como os filtros de spam avaliam e classificam mensagens é crucial.

Agora, você sabe que otimizar diferentes elementos de campanha ajuda a evitar problemas de entregabilidade e aumenta as chances de interação eficaz com o destinatário.

Passo 11: garanta facilidade para o descadaastro

O link para cancelamento muitas vezes é colocado no rodapé do e-mail, permitindo que os assinantes cancelem a assinatura a qualquer momento. Incluir o link para cancelamento no rodapé do e-mail pode ajudar na entregabilidade da mensagem de e-mail. Cada vez que você envia um e-mail para um destinatário, há vários detalhes pequenos que os filtros de spam e os ESPs (Provedores de Serviços de E-mail) verificam para avaliar a credibilidade da mensagem de e-mail. Para manter um relacionamento positivo com os destinatários e cumprir as regulamentações de privacidade, adicionar links de cancelamento em mensagens de e-mail se torna não apenas uma necessidade, mas também uma estratégia com benefícios para os remetentes. Entendemos que é doloroso ver pessoas se descadastrando de sua lista de contatos, mas é mais benéfico do que você pode imaginar. Às vezes, mesmo o conteúdo mais envolvente pode não ser adequado para alguns assinantes. Se isso acontecer e seus assinantes não encontrarem um link para cancelar a inscrição, eles podem simplesmente marcar suas mensagens como spam.

Como os links de cancelamento apoiam a entregabilidade?

Colocar esses links no rodapé da mensagem de e-mail é um detalhe para o qual os filtros de spam prestam atenção ao avaliar a credibilidade de mensagens de e-mail recebidas de endereços anteriormente não contatados. Para aqueles que conduzem campanhas de spam em massa ou assumem servidores de e-mail ou endereços de e-mail para enviar mensagens em massa, geralmente, nenhum tempo é gasto adicionando esses links às suas mensagens. Apenas ter esse link no conteúdo do e-mail é suficiente para provar que você é um remetente legítimo e não está tentando espalhar mensagens maliciosas. Além de ter protocolos de segurança apropriados para o domínio do remetente, como SPF, DKIM e DMARC, adicionar esses detalhes mínimos ao endereço de e-mail pode ser um fator-chave para decidir se a mensagem passará pelo filtro de spam. A maioria dos filtros visa impedir a entrega de mensagens maliciosas ou inúteis na caixa de entrada do destinatário. Simplesmente adicionar a opção de cancelar a inscrição de e-mails de um endereço específico é um sinal para os servidores de e-mail de que você já está aplicando um método para evitar contatos futuros, caso o destinatário deseje, facilitando a passagem pelos filtros de spam.

Conformidade com regulamentações e proteção de dados pessoais

Introduzir um link para cancelamento de campanha por e-mail não é apenas uma questão de boa prática, mas também de conformidade com regulamentações de proteção de dados, como o LGPD. A conformidade com o LGPD (Lei Geral de Proteção de Dados) requer aderência a certas regras quanto ao processamento de dados pessoais, incluindo dados coletados durante inscrições por e-mail. Essas regulamentações impõem a obrigação de permitir que os destinatários cancelem facilmente e efetivamente a assinatura da lista de e-mails. Isso atua como uma salvaguarda de privacidade, dando aos destinatários o controle sobre o conteúdo que recebem.

Redução das taxas de marcação como spam

A ausência de um link para cancelamento ou escondê-lo em um local inacessível pode levar à frustração do destinatário. Como resultado, alguns podem recorrer a marcar mensagens como spam em vez de perder tempo procurando a opção de cancelamento. Adicionar um link visível reduz o risco desse tipo de interação e mantém taxas saudáveis de entregabilidade. Ao introduzir uma opção fácil de cancelamento, você elimina a frustração para os destinatários que não desejam mais receber suas mensagens. Isso reduz indicadores de interação negativa, como ignorar mensagens ou marcá-las como indesejadas. Como resultado, você mantém um relacionamento positivo mesmo com aqueles que optaram por cancelar a inscrição.

Otimização da lista

Os links para cancelamento permitem manter uma lista de assinantes ótima e alinhada com os interesses. Ao remover regularmente os destinatários sem engajamento, você mantém o banco de dados atualizado e adaptado às reais necessidades. Este é um passo crucial na otimização da eficácia das campanhas de marketing.

Como colocar os links de cancelamento

Além dos próprios links de cancelamento, é igualmente importante colocar o link de cancelamento em um local visível com uma fonte suficientemente grande, especialmente na área de rodapé do e-mail. Evite colocá-lo em locais difíceis de encontrar, como letras pequenas ou seções ocultas. A conveniência do destinatário é fundamental para o cancelamento eficaz, portanto, garanta fácil acesso a essa opção. O link de cancelamento deve ser colocado relativamente no início do conteúdo do e-mail. Deixe-o visível sem a necessidade de rolagem. Os destinatários que, por várias razões, desejam cancelar a inscrição devem ter a oportunidade imediata de dar esse passo. Além disso, para e-mails do Gmail, aqueles que pesam muito serão truncados, incluindo o link de cancelamento.

Passo 12: acompanhe as mudanças nas tendências de entregabilidade

O ambiente de negócios é dinâmico. Onde a comunicação eletrônica desempenha um papel crucial, a entregabilidade de e-mails se torna um elemento imensamente importante das estratégias de marketing e comunicação. No entanto, para entender os desafios atuais relacionados à entregabilidade de e-mails, é necessário acompanhar as mudanças nessa área, com atenção especial para a evolução das políticas dos principais Provedores de Serviços de E-mail (ESP). À medida que as tecnologias evoluem e os usuários se tornam mais exigentes, a entregabilidade se torna uma tarefa cada vez mais complexa. Portanto, empresas que utilizam o marketing por e-mail devem monitorar continuamente as mudanças nessa área.

Com o avanço da inteligência artificial, os algoritmos de filtragem de spam passam por modificações contínuas. As empresas precisam ajustar suas estratégias para evitar que suas mensagens sejam classificadas como spam. Os principais provedores de serviços de e-mail, como Gmail, Outlook ou Yahoo, introduzem regularmente mudanças em suas políticas que impactam a entregabilidade de e-mails. Essas plataformas são peças-chave cujas decisões afetam milhões de empresas e profissionais de marketing. O Gmail introduz regularmente novos recursos, como categorias de caixa de entrada ou filtros de promoções. Se adaptar a essas mudanças é crucial para manter uma alta entregabilidade nessa plataforma.

O Outlook enfatiza a segurança. As configurações do DMARC (Autenticação de Mensagens Baseada em Domínio, Relatório e Conformidade) e outras proteções anti-spam se tornam mais rígidas, exigindo que os remetentes ajustem suas práticas. O Yahoo foca em combater phishing e golpes, implementando verificações de segurança mais rigorosas que podem afetar a entregabilidade.

A entregabilidade de e-mails é um processo dinâmico que requer uma adaptação constante às condições em mudança. Acompanhar as mudanças nos algoritmos de filtragem e políticas dos principais ESPs é crucial para manter a eficácia das campanhas de e-mail. Empresas que entendem e se adaptam a essas mudanças terão uma melhor chance de sucesso no mundo competitivo do marketing na internet.

RESUMO

No contexto do marketing por e-mail, a entregabilidade refere-se à capacidade das mensagens enviadas alcançarem as caixas de entrada dos assinantes, evitando filtros de spam. É um elemento crucial de campanhas de e-mail eficazes, pois mesmo a mensagem mais bem planejada não terá resultados se não for entregue ao destinatário.

Para gerenciar efetivamente a entregabilidade de seus e-mails, siga vários princípios-chave. Mantenha seu banco de dados impecável. Remova regularmente endereços de e-mail incorretos e evite armadilhas de spam, garantindo a higiene da lista. Implemente a autenticação de remetente configurando mecanismos SPF, DKIM e DMARC. Isso aumentará a credibilidade de seus envios e ajudará a evitar armadilhas anti-spam. Aqueça gradualmente sua infraestrutura, especialmente com campanhas significativas, para evitar que suas mensagens sejam tratadas como spam.

Analise os dados de seus envios, monitorando estatísticas e reações dos destinatários. Ajuste sua estratégia com base nos resultados obtidos. Foque nos clientes engajados segmentando sua lista e adaptando ofertas às suas necessidades. Envie conteúdo para destinatários ativos para manter o interesse deles. Garanta um design de e-mail esteticamente atraente. Crie e-mails atrativos e legíveis, prestando atenção em gráficos e layout, aumentando o apelo de suas mensagens. Planeje envios regulares, mantendo uma presença constante nas caixas de entrada dos destinatários. Construa seu banco de dados usando o modelo Double Opt-In, garantindo que os assinantes confirmem seu desejo de receber mensagens.

Realize testes A/B, experimentando com diferentes elementos de campanha, como cabeçalhos ou conteúdo para otimizar a eficácia. Seguindo esses dez princípios, você aumentará as chances de uma entregabilidade de e-mail bem-sucedida e manterá uma reputação positiva como remetente.