Como autenticar seu domínio de e-mail

Se o domínio de e-mail da sua campanha não estiver autenticado, há uma grande chance de que alguns dos seus e-mails de abandono de carrinho sejam erroneamente classificados como spam. Isso acontece porque os provedores de e-mail (como Gmail, Outlook, etc.) não conseguem verificar se o e-mail realmente veio de um remetente confiável.

Autenticar seu domínio é uma etapa crucial, pois isso aumenta significativamente as chances de seus e-mails chegarem à caixa de entrada dos seus clientes, em vez de serem bloqueados ou desviados para a pasta de spam. Isso, por sua vez, contribui para uma recuperação de vendas mais eficiente e um impacto positivo na receita do seu negócio.

A boa notícia é que esse problema pode ser facilmente resolvido com a adição de dois simples registros no seu domínio. A autenticação de e-mail é um processo técnico que garante aos servidores de e-mail que a mensagem realmente foi enviada por você, e não por um remetente falsificado.

Sabemos que esse processo pode parecer complexo se você não tem experiência com TI. Por isso, preparamos este guia para ajudar você e sua equipe de TI a concluir essa tarefa de forma rápida e simples.

O que está envolvido?

Envie este guia para seu departamento de TI e solicite que concluam a Tarefa 1 e a Tarefa 2.

Quanto trabalho é esse para a equipe de TI?

Essa tarefa deve levar menos de 10 minutos.

Isso é seguro?

Sim, a equipe de TI poderá confirmar que este é um método seguro para melhorar a capacidade de entrega de e-mail.

Eu preciso fazer algo mais?

Nós gostaríamos de ouvir de volta de você uma vez que a tarefa foi concluída para que saibamos que a autenticação não afetará o desempenho de qualquer campanha futura.

Melhor desempenho da campanha

A conclusão dessas duas tarefas terá um impacto positivo significativo na entregabilidade de seu e-mail que será refletida na análise de desempenho da sua campanha quase imediatamente mostrando:

- Taxas de Abertura Aumentadas
- CTR aumentado
- Maior receita recuperada

Se você tiver outras dúvidas, não hesite em entrar em contato com seu gerente de contas.

Tarefa 1 - Atualizando um registro SPF existente

Caso você já tenha um registro SPF, por favor siga os quartos passos abaixo:

1. Acesse o provedor de DNS
2. Ache o arquivo TXT do registro SPF
3. Adicione a linha de código abaixo no registro SPF.

```
Include=spf.etagdigital.com
```

Por exemplo, se o registro SPF se parece com isso:

```
v=spf1 a mx ip4: 192.168.1.100 include:example.com ~all
```

O novo registro SPF deve ficar assim:

```
v=spf1 a mx ip4: 192.168.1.100 Include=spf.etagdigital.com include:example.com ~all
```

4. Tarefa completa, obrigado.

Se você atualmente não possui um registro SPF, será necessário criar um.
Por favor, siga esta tarefa alternativa.

Tarefa Alternativa – Criando um novo registro SPF

1. Acesse o provedor de DNS
2. Crie um novo registro SPF com o seguinte código:

```
v=spf1 a mx include=spf.etagdigital.com.br ~all
```

3. Tarefa completa, obrigado.

Tarefa 2 – Criando uma Chave DKIM

Para enviarmos e-mails utilizando o remetente escolhido é necessário que nosso servidor tenha as devidas permissões.

Remetente Escolhido: [sender@email.com]

Autenticação DKIM

Autentique e verifique a propriedade. Use isso para um melhor posicionamento na caixa de entrada.

Para autenticar via DKIM você tem 2 opções TXT ou CNAME.

Autenticação via TXT

Registro TXT para o nome do host e valor para assinatura DKIM.

Instruções:

1. Faça login no seu DNS e acesse nespresso.com
2. Crie um NOVO registro TXT
3. Adicione o nome do host e o registro DNS público para registrar e salve
4. Informe a seu representante para efetuar a verificação DKIM

Record type	TXT
Hostname	slkey._domainkey.dominiodocliente.com.br
Value	"v=DKIM1; k=rsa; p=MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAt4zlcVtD3c4oUAdEJWu4jFkajz17ilHJZ2eoav5X2/KSV5UXZ+zrzE4l/gqYCnmkCpApXHwin0dZ/jA75FK8n+xCLLgaqCDBck7n8xyjo+Smz50ujGtNfy+rVUcRT00Emh8ZPCtewzQy2A/OlY2s0V4hLd0hG5wIW/Topw2YoQk2wBhDNTE0axFt5QEx1qRV" "ZqWIp9nZXrb8mpwQbulvrkySXxvVSs8VXpOZ4aEWvD7cSVVQQ9XA1a2KcObm69bbm75qmZh++iqyKM3Hxuz6/g+0OjN9JykccUFzBtuLjlUmsJ+cR5/cvxjjpJ02EUctGmX/6gF/GOdpwOHKF9ZIQwIDAQAB"

Autenticação via CNAME

Registro CNAME para o nome do host e valor para assinatura DKIM.

Instruções:

1. Faça login no seu DNS e acesse nespresso.com
2. Crie um NOVO registro CNAME
3. Adicione o nome do host e o ponto no novo registro CNAME
4. Informe a seu representante para efetuar a verificação DKIM

Record type	CNAME
Hostname	dkim._domainkey. dominiodocliente.com.br
Value	tracking.socketlabs.com

Informação Extra

O que é SPF?

A publicação de registros SPF no Sistema de Nomes de Domínio (DNS) é uma maneira de listar qual endereços de IP são seguros para enviar e-mails em nome de seus domínios.

Se o endereço IP que envia e-mail em nome do domínio de uma empresa não estiver listado no registro SPF, ele não será autenticado e provavelmente será rejeitado pelos filtros de spam.

O que é DKIM?

DomainKeys Identified Mail (DKIM) é um processo de verificação que permite que uma marca leve responsabilidade de enviar uma mensagem de forma que possa ser reconhecida e justificada pelo destinatário ESP.

Este protocolo faz parte de um programa para limitar o spam, o spoofing e o phishing em campanhas de email marketing. Dependendo da implementação, o DKIM também pode provar que um email não foi modificado em trânsito - garantindo ainda mais a autenticidade.

Se você tiver outras dúvidas, não hesite em entrar em contato com o gerente da sua conta.