



Ebook

Configurações e ferramentas essenciais para

Email Marketing



A entrega na caixa de entrada é um dos maiores desafios para empresas que realizam ações de email marketing. Uma campanha onde a mensagem cai no lixo eletrônico ou é bloqueada pelos filtros anti-spam pode afetar completamente o sucesso de sua estratégia.

Pensando nisso, criamos esse material com uma série de configurações essenciais para que sua mensagem seja autenticada e reconhecida como confiável para os provedores de seus destinatários. Além disso, selecionamos diversas ferramentas que podem ser utilizadas para acompanhar sua reputação, autenticidade e também para verificar se o conteúdo de sua mensagem pode fazer com que ela seja bloqueada pelos filtros anti-spam.





Sumário

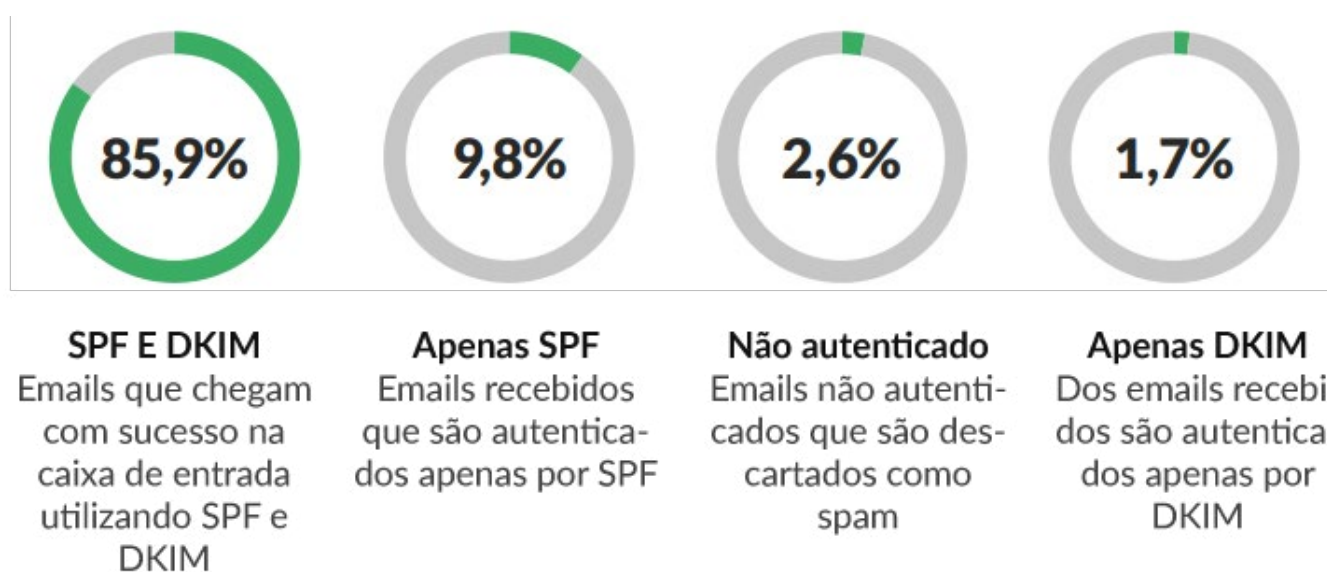
Configurações.....	4
SPF.....	5
DKIM.....	6
DMARC.....	7
CNAME.....	9
Ferramentas para analisar sua reputação..	10
Ferramentas para testes.....	15

Configurações

As configurações que listamos abaixo são essenciais para que seu email marketing seja reconhecido como válido e confiável. Essas configurações são realizadas no painel de hospedagem de seu domínio e servem para garantir ao provedor de seus contatos que é realmente você que está enviando a mensagem. Também é através delas que os servidores como Google, Microsoft e Yahoo compreendem que seu envio é seguro, diminuindo as chances de seu email ser bloqueado ou direcionado à caixa de spam.

O impacto positivo na adoção dessas configurações

As configurações de SPF, DKIM e DMARC estão, aos poucos, sendo adotados pelo mercado brasileiro. Segundo o relatório de benchmark de [Entregabilidade 2016 da Return Path](#), o Brasil está abaixo da média mundial na taxa de entrega na caixa de entrada. No mesmo ano, o [Google apresentou em seu blog](#) que quase 86% dos emails aceitos pelo provedor possuíam as configurações de SPF e DKIM autenticadas corretamente.



Informações apresentadas pelo Google em 2016



SPF

O **SPF** (Sender Policy Framework) é uma tecnologia que visa combater o envio não autorizado de mensagens. Ele diz quem pode enviar emails em nome do seu domínio, autenticando assim o remetente, ou seja, quando o servidor do seu contato receber seu email, ele irá verificar se a infraestrutura que realizou o envio está autorizada a utilizar o seu domínio. Se não estiver autenticado corretamente, a sua mensagem poderá ser rejeitada pelo provedor.

A configuração de SPF é uma entrada do tipo TXT na zona de DNS de seu domínio. Caso você utilize uma plataforma de envios de email marketing, a própria plataforma irá informar a include (lista de IPs) ou o IP que deve ser incluído em sua zona de DNS.

A Dinamize possui uma plataforma de consulta pública de suas configurações de SPF. Através da página meuspf.com você pode consultar quais são as includes e IPs autorizados a realizar envios com o seu domínio.



The screenshot shows the 'SPF PLATAFORMA DE CONSULTA' interface. At the top, it says 'Veja abaixo o resultado da busca do registro SPF para o domínio **dynamize.com**'. Below this is a search bar containing 'dynamize.com' and a green 'CONSULTAR' button. The results section shows 'Servidores DNS consultados: ns2.livebuzz.com.br, ns1.livebuzz.com.br.' and a green circular stamp that says 'APROVADO'. Below the results, there is a list of SPF records with dropdown menus for each. The first record is 'include:_spf.google.com', which is expanded to show a list of IP addresses: ip4:64.233.160.0/19, ip4:66.102.0.0/20, ip4:66.249.80.0/20, ip4:72.14.192.0/18, ip4:74.125.0.0/16, and ip4:108.177.8.0/21. Other records include 'include:snews.dynamize.com', 'include:sdspf.freshdesk.com', and '~all'.

Exemplo de consulta de SPF realizada pela página meuspf.com



DKIM

O **DKIM** (DomainKeys Identified Mail) - consiste em assinar as mensagens enviadas com uma chave pública, para garantir a autenticidade do remetente.

Ele executa funções parecidas com as do SPF, pois impede a falsificação do domínio, mas é mais complexo. Enquanto o SPF certifica quem está enviando, o DKIM verifica o cabeçalho da mensagem e garante que o conteúdo do email não tenha sido alterado de forma alguma durante o envio.

Ao ter um DKIM válido, o servidor destinatário irá comparar o conteúdo do seu texto (certificado pela entrada) com a entrada que foi configurada no seu domínio. Ao verificar que a entrada é a mesma, será entendido que a mensagem é autêntica e sem modificações, melhorando seus resultados de entregabilidade e, conseqüentemente, sua reputação.



DMARC

DMARC é a sigla em inglês para “Mensagem Baseada em Domínio de Autenticação, Relatório e Conformidade”, e é uma proposta de normatização para garantia de autenticidade de um email que tem sido muito bem aceita e largamente adotada, inclusive por grandes players como Google e Microsoft.

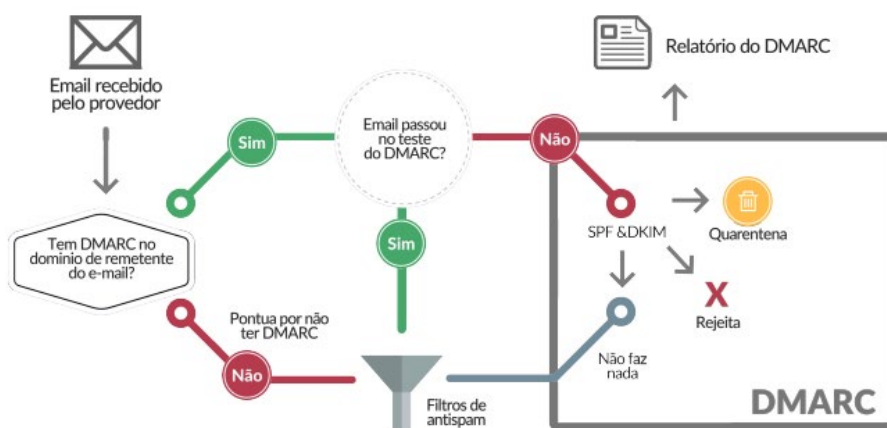
Em Outubro de 2015, o Google se comprometeu a adotar e implantar políticas mais duras de DMARC, inviabilizando, por exemplo, que ferramentas de email marketing usem como remetente, emails do domínio @gmail.com.

O DMARC baseia-se nas configurações de SPF e DKIM apresentadas acima. Ambas são mecanismos de proteção e segurança amplamente difundidos e em adicional o DMARC agrega uma função especial de relatórios, que permite monitorar o comportamento dos emails que estão sendo enviados utilizando o seu domínio.

Com a configuração correta do DMARC, é muito mais simples e eficaz determinar se uma mensagem é legitimamente enviada a partir de um suposto remetente; mas não apenas isso: o DMARC permite definir o que fazer se a mensagem realmente não for do remetente.

O DMARC aborda estas questões, ajudando os remetentes de email e receptores a trabalharem em conjunto para emails com melhor segurança, protegendo os usuários e as marcas contra abusos e emails falsos enviados indevidamente com o seu domínio.

Fluxo de funcionamento do DMARC



Como realizar a configuração de DMARC

Para realizar a configuração de DMARC é necessário possuir acesso à zona de DNS onde seu domínio estiver hospedado e criar uma entrada, conforme orientado abaixo:

Entrada: `_dmarc.meudominio.com`

Tipo: TXT

Conteúdo: o conteúdo deve ser criado de acordo com as preferências de sua marca.

Nome	TTL	Classe	Tipo	Registro
<code>_dmarc.meudominio.com</code>	14400	IN	TXT	<code>v=DMARC1; p=none; rua=mailto:dmarc@meudominio.com</code>

Tipos de entradas DMARC

Abaixo detalhamos um exemplo de cada tipo de entrada de DMARC. Escolha uma de sua preferência e inclua em seu painel de hospedagem para habilitar DMARC em seu domínio.

De acordo com a sua configuração, o provedor que receber um email de seu domínio sem a configuração de SPF e/ou DKIM, fará a ação definida por você. Além disso, todas as mensagens que passarem por essa verificação, serão incluídos no relatório diário enviado para o endereço cadastrado em sua configuração.

Tipos de ações	Nome da entrada	Tipo	Conteúdo
Provedor não realiza nenhuma ação	<code>_dmarc.meudominio.com</code>	TXT	<code>v=DMARC1; p=none; rua=mailto:dmarc@meudominio.com</code>
Provedor irá colocar em quarentena	<code>_dmarc.meudominio.com</code>	TXT	<code>v=DMARC1; p=quarantine; rua=mailto:dmarc@meudominio.com</code>
Provedor irá rejeitar a mensagem	<code>_dmarc.meudominio.com</code>	TXT	<code>v=DMARC1; p=reject; rua=mailto:dmarc@meudominio.com</code>

Nota: `meudominio.com` deve ser substituído pelo domínio do qual você está realizando a configuração.



CNAME

A configuração **CNAME** (Canonical Name) - é responsável pelos redirecionamentos necessários para o funcionamento da ferramenta, como os links da própria plataforma e os dados e estatísticas dos seus relatórios.

Com esses links de redirecionamento, quando houver imagens no seu email, links de visualização externa e descadastro, será muito mais difícil pontuar em ferramentas anti-spam ou cair em blacklists.

O processo de descadastros, contagem de visualizações e rastreamento de cliques é facilitado após a realização desta configuração, pois como já estará com um apontamento direto para ferramenta, será possível agrupar os dados e apresentá-los de uma forma mais simples e eficiente.



Ferramentas para analisar sua reputação

MxtoolBox

[Link de acesso](#)

O **MxtoolBox** é uma plataforma gratuita que oferece serviços de consulta e diagnóstico de domínios e IP's.

Através dele, é possível verificar se seu domínio foi listado em alguma blacklist, para que você possa realizar os procedimentos necessários para a solicitação de liberação.

The screenshot shows the MxtoolBox website interface. At the top, there is a navigation menu with options like 'MX Lookup', 'Blacklists', 'Diagnostics', 'Domain Health', 'Analyze Headers', 'Free Monitoring', 'DMARC', 'Investigator', 'DNS Lookup', and 'More'. Below the navigation, there is a search bar with a 'Blacklist Check' button and a 'Need help?' link. The main content area displays the results of a blacklist check for 'isbrae.com.br'. A green 'Monitor This' button is visible. A red banner indicates that the domain is on a blacklist, with a link to 'Click here for some suggestions'. Below this, a table shows the details of the blacklist entry.

	Blacklist	Reason	TTL	ResponseTime	
✖ LISTED	FABELSOURCES	██████████ was listed Detail	600	78	Ignore

Verificação no MxtoolBox



MultiRBL

[Link de acesso](#)

Assim como o MxtoolBox, o MultiRBL também é uma plataforma para monitoramento de blacklists de domínios e IPs.

Senderscore

[Link de acesso](#)

O Senderscore é utilizado para consultar a reputação dos IPs utilizados em envios. A pontuação dos IPs pode ser de 0 à 100 pontos. Através da pontuação de um IP, podemos saber como será a sua entrega. Quanto maior for a pontuação, melhor será a entrega.

Algumas das métricas avaliadas para determinar a pontuação de um IP são:

- **Taxa de reclamações:** são as denúncias de spam realizadas pelos contatos de seus envios.
- **Taxa de usuários desconhecidos:** envio para contatos com conta ou domínio inválidos.
- **Acessos de spamtraps:** contas inexistentes ou inativas utilizadas por diversos provedores de email, como Hotmail, para encontrar domínios que não têm controle sobre sua base. Bases compradas ou desatualizadas, podem caracterizar spammers.
- **Blacklists:** foram criadas para ajudar os provedores a evitarem a entrega de envios indesejados. Um endereço de IP pode acabar sendo listado em uma blacklist devido a alta taxa de denúncias de spam, contatos inválidos ou envio para spamtraps.



97

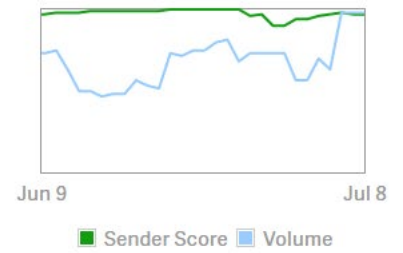
Hostname :: 97504882-idc.fo.dprofor.com.br

Moderate Volume Sender ?

Return Path Certified ?

Return Path Safe ?

[Whois Lookup](#)



Reputation Measures ?

Impact on this score ?

Blacklists ?

Low

Complaints ?

Low

Infrastructure ?

Low

ISP Bulk Rate ?

[Contact us for details](#)

Message Filtered ?

Low

Verificação de IP no SenderScore

Google Postmaster

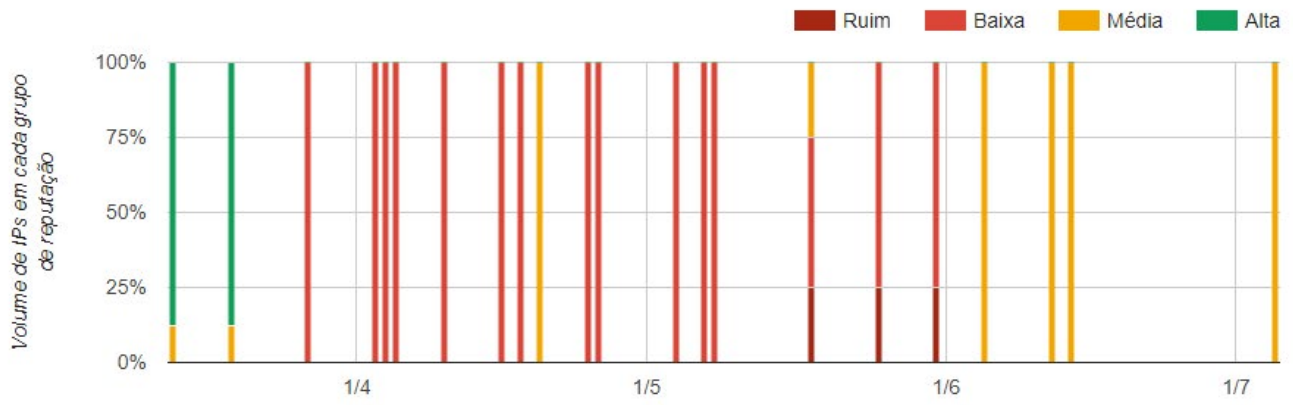
[Link de acesso](#)

Essa é uma plataforma que indica como está a reputação do seu domínio e IP junto ao provedor Gmail. Ela também mostra um relatório de taxa de spam, erros de entrega, como estava a autenticação do domínio no momento do envio, entre outros dados.

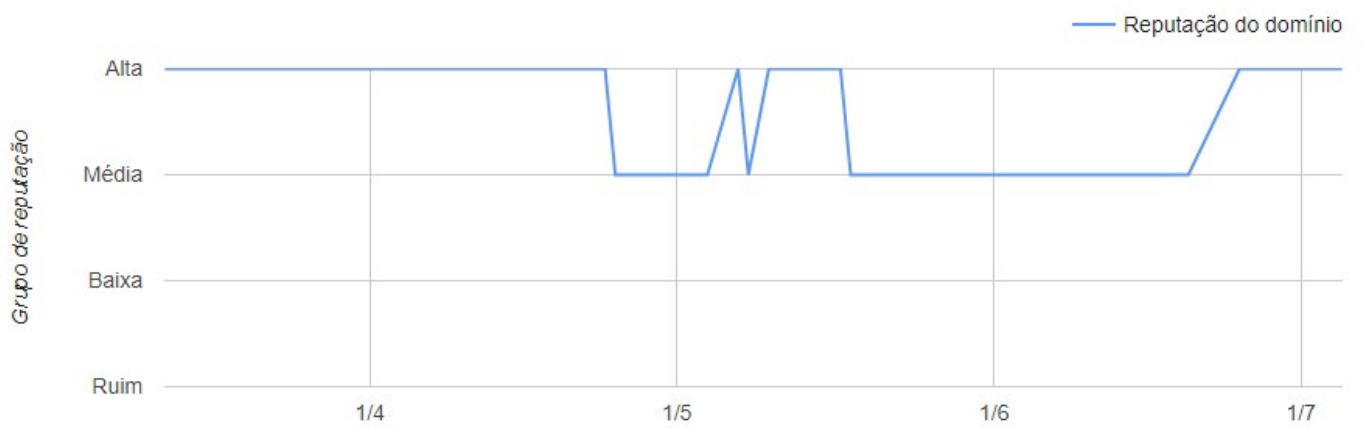
Para utilizá-la, basta ter uma conta do Google e realizar uma configuração na zona de DNS do seu domínio, criando uma entrada do tipo CNAME ou TXT, para autorizar a verificação da reputação do seu domínio.



Reputação de IP ?



Reputação do domínio ?



Verificação da reputação no Google Postmaster



Microsoft SNDS

[Link de acesso](#)

O Microsoft SNDS realiza uma verificação da reputação de seus IPs junto ao Outlook.

Para acessar o Microsoft SNDS, você precisará efetuar o login em uma conta da Microsoft e realizar um processo de autorização para que você possa ter acesso às informações sobre seus IPs.

Activity period [?]	RCPT commands [?]	DATA commands [?]	v Message recipients [?]	Filter result [?]	Complaint rate [?]	Trap message period [?]	Trap hits [?]
Total: 10 days	5,096	5,045	5,045	8 red days	0.2%		0
1/27/2009 12:00 PM - 1/27/2009 3:00 PM	950	949	949		< 0.1%		0
1/8/2009 10:00 AM - 1/8/2009 12:00 PM	935	930	930		0.1%		0
12/10/2008 9:00 AM - 12/10/2008 10:00 PM	859	852	852		0.1%		0
11/18/2008 2:00 PM - 11/18/2008 4:00 PM	789	785	785		0.5%		0
12/30/2008 11:00 AM - 12/31/2008 5:00 AM	570	557	557		< 0.1%		0
1/13/2009 11:00 AM - 1/13/2009 3:00 PM	305	304	304		0.7%		0
12/11/2008 10:00 AM - 12/11/2008 9:00 PM	191	190	190		< 0.1%		0
12/5/2008 3:00 PM - 12/5/2008 5:00 PM	188	187	187		< 0.1%		0
11/28/2008 11:00 AM - 11/28/2008 2:00 PM	171	170	170		< 0.1%		0
11/10/2008 9:00 AM - 11/10/2008 4:00 PM	138	121	121		< 0.1%		0
Total: 10 days	5,096	5,045	5,045	8 red days	0.2%		0

Verificação de reputação na Microsoft SNDS



Ferramentas para testes

Existem algumas ferramentas que disponibilizam testes tanto para o conteúdo da mensagem que pretende enviar quanto sobre as configurações do seu domínio, para verificar sua validade. Abaixo, listamos alguns serviços que podem auxiliar nestas verificações.

Litmus

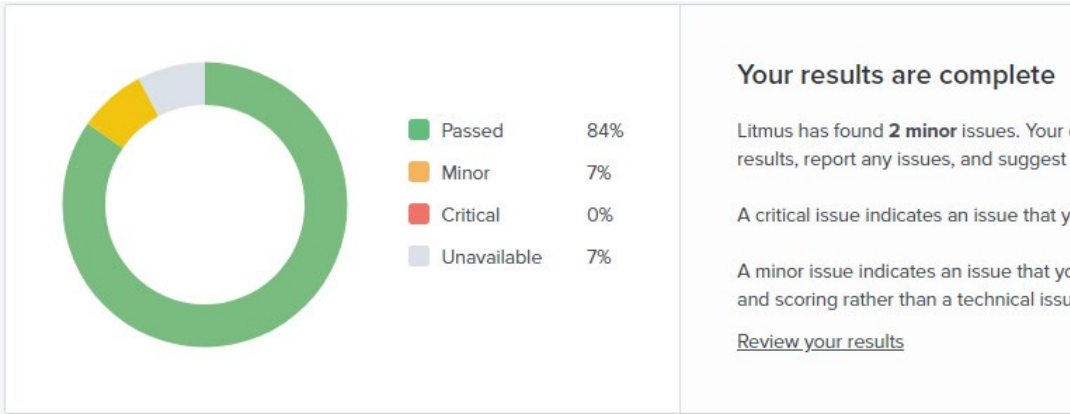
[Link de acesso](#)

É uma ferramenta utilizada para testar o conteúdo de seus envios e verificar se as configurações do domínio estão validadas. Além dessa análise, também é possível realizar testes da sua peça em diferentes provedores de recebimento, verificando o carregamento correto dela em todos eles.

Na simulação de entrega será indicado em qual local seu email chegou nos diferentes provedores de recebimento, como Hotmail. Os envios podem ser entregues na caixa de entrada, caixa de spam ou lixo eletrônico.

Realizando testes nessa ferramenta, você conseguirá analisar se há algum fator pontuado negativamente no conteúdo ou configurações do seu domínio, para que então você possa realizar alterações melhorando os aspectos prejudiciais antes de realizar o envio final, se certificando que sua campanha alcançará os melhores resultados de entrega e visualizações possíveis.





Your results are complete

Litmus has found **2 minor** issues. Your results, report any issues, and suggest

A critical issue indicates an issue that y

A minor issue indicates an issue that yo and scoring rather than a technical issu

[Review your results](#)

Authentication Filters

Check for the existence and status of your authentication records and other best practices.



Blacklist Filters

Check your IP address and Domains against important blacklists.



Placement Filters

Check the inbox placement of your email test.



Score Filters

Check your email test against multiple score based filters.



SpamAssassin

[Saiba mais sobre o SpamAssassin](#)

Recebemos sua mensagem de teste [TESTE] Já se inscreveu em nossos webinars de julho? ??? e passou no SpamAssassin com uma pontuação de 0,5 .

Pontuação Check	
Status	Texto descritivo
	Seu e-mail tem muitas imagens, mas relativamente pouco texto. Considere adicionar mais conteúdo de texto. Se o seu e-mail é composto de uma imagem singular, considere fatiar essa imagem e adicionar texto do sistema ao corpo, em vez de todo o texto como parte da imagem.
	A cor da sua fonte é muito semelhante à do fundo. Tente ajustar o contraste do texto para torná-lo visível. Ocultar ou ofuscar texto ou links em seu e-mail é uma tática comumente usada em mensagens de spam.

Teste no Litmus



MailTester

[Link de acesso](#)

O MailTester também é uma ferramenta que realiza testes e análises dos seus envios, verificando se há práticas que devem ser alteradas e validando as configurações do seu domínio no momento do envio.



Teste no MailTester

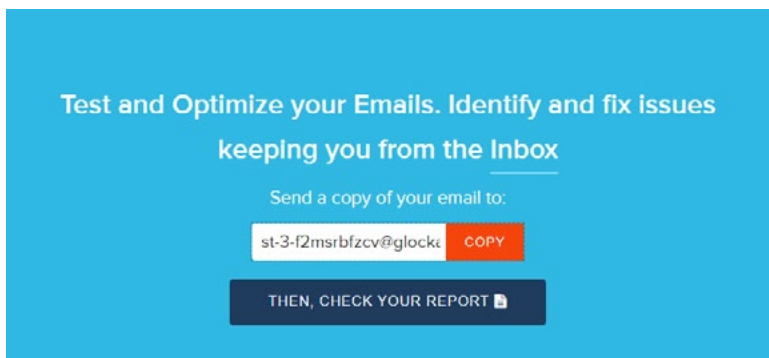
Ele dará uma pontuação final para sua mensagem, que pode variar de 0 a 10, de acordo com a análise que será feita do seu envio. O MailTester disponibiliza a realização de 3 testes gratuitos por dia.



GlockApps

[Link de acesso](#)

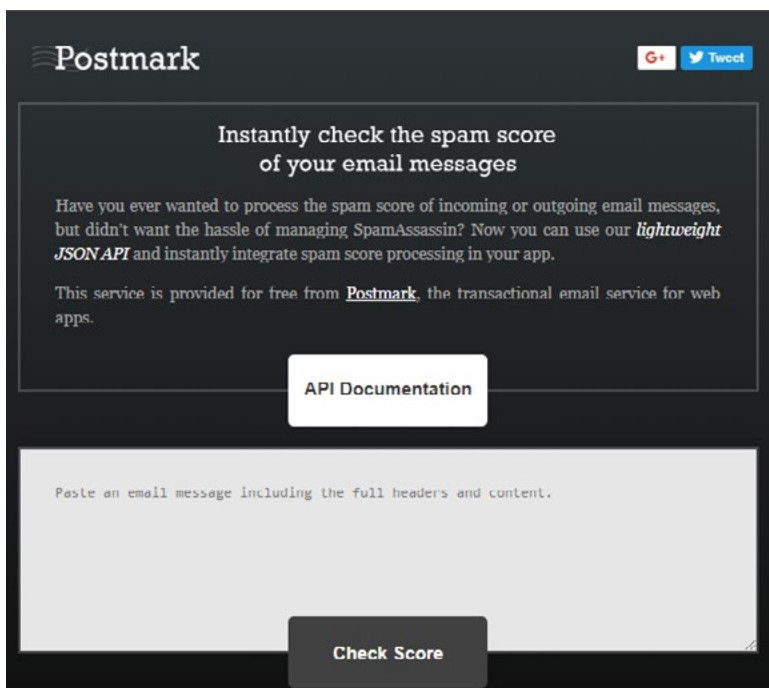
O GlockApps é outra ferramenta utilizada para avaliação de relatórios de entrega dos envios. Este serviço é disponibilizado de forma gratuita.



Postmark

[Link de acesso](#)

Pelo Postmark, você pode inserir código-fonte de sua peça de email para testá-lo e verificar a pontuação do seu HTML.



Todas as configurações de **SPF**, **DKIM**, **DMARC** e **CNAME** servem para os diferentes provedores identificarem seu envio como autenticado, aumentando assim as chances de seu envio chegar na caixa de entrada de seus destinatários.

Além disso, utilize-se de plataformas para acompanhamento constante da reputação de seus domínios e IPs e procure realizar testes constantes para entender o comportamento dos diferentes filtros anti-spam.