Améliorer la délivrabilité des emails

Autorisation obligatoire du domaine de l'email

Chaque journaliste et chaque influenceur reçoit quotidiennement des centaines d'emails. Certains d'entre eux sont légitimes et indispensables —les vôtres! Mais beaucoup ne sont que des emails indésirables ou des tentatives d'escroquerie, tout comme ceux que vous pouvez recevoir dans votre propre boîte de réception.

Pour améliorer la sécurité, des mesures ont été prises pour mieux identifier un email comme légitime. En particulier, une attention accrue est portée à la vérification que l'expéditeur, en l'occurrence Cision, soit autorisé à envoyer des emails au nom de votre organisation.

Cela nécessite toutefois des étapes supplémentaires pour garantir que les emails envoyés par Cision en votre nom seront correctement livrés.

Vous trouverez ci-dessous les explications sur ces différentes étapes:

☐ 1 **Cision vous fournit toutes les configurations techniques nécessaires: enregistrement SPF, DKIM et DMARC**

☐ 2 **Demander à vos équipes IT d'ajouter les entrées DNS pour le SPF, DKIM et DMARC afin d'être sûr que les emails envoyés par Cision en votre nom seront bien reçus**

Vous pouvez également le faire vous-même si vous avez accès à vos enregistrements DNS – à voir avec votre hébergeur

☐ 3 **Vérifier avec Cision que tout fonctionne (notre équipe de domain client est disponible pour vous aider)**

En fonction de la solution qui vous convient, ils peuvent vous fournir toute information manquante, notamment l'adresse(s) IP et les clés DKIM

4 **Toutes les étapes sont réalisées afin d'améliorer le taux de délivrabilité de vos messages**

Les bonnes pratiques pour améliorer la sécurité de vos emails

Si vous ne connaissez pas l'adresse IP ou le domaine à ajouter aux clés SPF et/ou DKIM générées pour votre nom de domaine, veuillez envoyer une demande à domainhelp@cision.com. Cette information doit ensuite être communiquée à votre service informatique ou à l'hébergeur de votre nom de domaine.

SPF (Sender Policy Framework)

Le protocole SPF permet au propriétaire d'un nom de domaine de spécifier quels serveurs sont autorisés à envoyer des emails à partir de ce domaine. Ainsi, cela empêche les spammeurs d'envoyer des messages non autorisés qui semblent provenir de votre domaine. Lorsqu'un serveur reçoit un email, il vérifie si l'adresse IP du serveur expéditeur figure dans la liste des domaines autorisés ou non autorisés selon l'enregistrement SPF de l'expéditeur.

SPF

Créer un nouvel enregistrement SPF ou mettre à jour l'existant sur votre domaine.

La politique SPF d'un domaine est définie à l'aide d'un enregistrement TXT. Pour que la vérification soit complétée correctement, chaque domaine ne peut avoir qu'un seul enregistrement SPF.

Si vous n'avez pas les adresses IP à ajouter à l'enregistrement SPF, veuillez nous contacter car cela dépend de la plateforme que vous utilisez.

DKIM (DomainKeys Identified Mail)

Le DKIM permet à un utilisateur d'authentifier des emails à l'aide d'une signature électronique. Le serveur détermine si la signature et la clé de l'enregistrement correspondent, ce qui garantit que le message est authentique et n'a pas été modifié lors de l'envoi. Les serveurs destinataires utilisent le DKIM pour vérifier que le propriétaire du domaine a effectivement envoyé le message.

DKIM

Ajoutez des clés DKIM à vos serveurs DNS* pour le domaine que vous utilisez afin de recevoir des réponses des journalistes.

Cela doit être au niveau du nom de domaine, les sous-domaines ne fonctionnent pas.

Si vous n'avez pas les clés DKIM, veuillez nous contacter car cela dépend de la plateforme.

*DNS: Domain Name System ("répertoire Internet") transforme les noms de domaine en adresses IP que les navigateurs utilisent pour charger les pages internet. Chaque appareil connecté à internet a sa propre adresse IP, qui est utilisée par d'autres appareils pour le localiser et pour rechercher des informations (par exemple, enregistrement SPF, clés DKIM) dans les domaines. Remarque : le propriétaire du domaine contrôle les données DNS.

Autorisation obligatoire du domaine de l'email

SPF

DKIM

DMARC

Email

CISION

Contactez-nous:
domainhelp@cision.com

Les bonnes pratiques pour améliorer la sécurité de vos emails

Si vous ne connaissez pas l'adresse IP ou le domaine à ajouter aux clés SPF et/ou DKIM générées pour votre nom de domaine, veuillez envoyer une demande à domainhelp@cision.com. Cette information doit ensuite être communiquée à votre service informatique ou à l'hébergeur de votre nom de domaine.

DMARC (Domain-based Message Authentication, Reporting, & Conformance)

Le DMARC est un protocole qui unifie SPF et DKIM. Les instructions contenues dans l'enregistrement DMARC d'un nom de domaine indiquent au serveur destinataire quoi faire d'un email qui échoue à la vérification SPF et/ou DKIM. DMARC veille à ce que votre domaine obtienne la délivrabilité qu'il mérite en fonction de vos pratiques d'envoi grâce à l'utilisation du domaine dans toutes les phases d'authentification de vos messages.

DMARC

Activer la politique DMARC policy et selon votre préférence, mettre en place « p=none » (ou « p=quarantine », ou « p=reject » selon les politiques de sécurité en vigueur dans votre organisation)

Vous pouvez l'activer une fois que les enregistrements DKIM ont été ajoutés et vérifiés par votre hébergeur.

Exigences relatives aux emails:

À compter de février 2024, Gmail et Yahoo! imposeront aux expéditeurs envoyant 5 000 messages ou plus par jour vers des comptes Gmail/Yahoo! de: authentifier les courriels sortants, éviter l'envoi de courriels indésirables ou non sollicités, et simplifier le processus de désinscription pour les destinataires.

Email

Utiliser un nom de domaine que vous possédez (@company.com) pour envoyer vos emails

N'utilisez pas gmail.com, hotmail.com ou yahoo.com (ou un domaine que vous ne possédez pas) comme adresse expéditrice.

Lorsque le DKIM est correctement configuré, que la politique DMARC a été activée et que vous envoyez des emails à partir de votre propre domaine, ce plafond ne devrait plus être un problème.

Autorisation obligatoire du domaine de l'email

SPF

DKIM

DMARC

Email

CISION

Contactez-nous:

domainhelp@cision.com