



DMARC MANAGER

PROTÉGEZ LA RÉPUTATION DE VOTRE MARQUE EN SÉCURISANT VOS DOMAINES CONTRE L'USURPATION D'IDENTITÉ PAR COURRIEL, L'HAMEÇONNAGE ET LE USURPATION D'IDENTITÉ ÉLECTRONIQUE GRÂCE À UNE GESTION INTUITIVE DE DMARC, DKIM ET SPF.

DomainKeys Identified Mail



DKIM

Signe numériquement vos courriels afin que les destinataires sachent que le message provient bien de vous et qu'il n'a pas été modifié.

Sender Policy Framework



SPF

Légitime votre domaine comme étant le seul autorisé à envoyer des courriels en votre nom.

Domain-based Message Authentication, Reporting and Conformance



DMARC

Aide à garder les boîtes de réception propres et détermine quoi faire des courriels qui échouent aux contrôles DKIM ou SPF.

La gestion de l'authentification des courriels est un casse-tête pour de nombreuses organisations. Mettre en place et maintenir des politiques DMARC, DKIM et SPF sécuritaires représente un défi important, surtout lorsqu'on gère plusieurs domaines. Sans des paramètres DMARC appropriés, les entreprises risquent d'endommager leur réputation d'expéditeur et s'exposent davantage aux attaques d'usurpation d'identité par courriel.

En parallèle, se conformer aux exigences strictes des fournisseurs de messagerie ajoute une couche de complexité. Le manque de visibilité sur la performance des campagnes et l'existence d'activités courriel « cachées » au sein des organisations constituent d'autres difficultés. Enfin, l'objectif d'atteindre les boîtes de réception visées (plutôt que les dossiers de courrier indésirable) est peu probable sans une sécurité courriel adéquate.

MAÎTRISEZ FACILEMENT DMARC, DKIM ET SPF ET PROTÉGEZ LA RÉPUTATION DE VOTRE MARQUE



Assurer la conformité – Configurez et maintenez facilement des politiques exemplaires pour DMARC, DKIM et SPF.



Gérer le DNS simplement – Ajoutez des entrées DNS et modifiez-les en quelques secondes, sans friction.



Prévenir l'usurpation – Obtenez une vue d'ensemble complète des sources qui envoient des courriels via vos domaines.



Assurez la livraison des courriels en respectant les normes d'authentification tout en protégeant la réputation de votre marque.



FONCTIONNALITÉS

Configurateur de domaines : Le service fournit une interface intuitive pour configurer et maintenir des politiques exemplaires DMARC, DKIM et SPF, ainsi que des paramètres TLS, pour plusieurs domaines. Avec le Gestionnaire DMARC, vous pouvez administrer les enregistrements SPF/DMARC et appliquer des changements DNS en quelques secondes.

Tableau de bord d'état : Le tableau de bord offre une vue d'ensemble complète avec diverses statistiques, notamment les domaines gérés, le nombre d'expéditeurs autorisés et non autorisés, le volume de courriels autorisés et non autorisés envoyés, ainsi que le nombre de courriels ayant réussi ou échoué aux contrôles DMARC.

Analyse des sources de courriel : Cette fonctionnalité fournit une vue d'ensemble des sources qui envoient des courriels via vos domaines. Elle détaille les volumes de courriel, les statuts d'authentification (DMARC réussi/échoué), la catégorisation des sources (autorisées ou non autorisées), la délivrabilité, la réputation de l'expéditeur et le niveau de menace.

Image de marque BIMI : Une fois votre domaine conforme à DMARC, vous pouvez utiliser la fonctionnalité BIMI pour afficher votre logo à côté des courriels dans les boîtes de réception compatibles, ce qui maximise l'impact, la reconnaissance de la marque et la confiance.

Chiffrement SMTP-TLS : Assurez-vous que les courriels sortants sont transmis de façon sécuritaire grâce au chiffrement SMTP-TLS. Recevez des rapports détaillés sur les courriels qui n'étaient pas chiffrés et qui n'ont pas pu être livrés, ajoutant une couche de sécurité à vos communications.

Rapports d'échec et alertes : Les rapports d'échec fournissent des données détaillées en temps réel sur les messages qui échouent aux vérifications DMARC. Cela vous aide à comprendre qui envoie des courriels au nom de vos domaines et pourquoi certains messages échouent. Configurez les alertes souhaitées et recevez un courriel à l'adresse indiquée lorsqu'un événement survient, ce qui permet une réponse plus rapide aux menaces.

