HORNETSECURITY

FICHE D'INFORMATIONS

DMARC MANAGER

PROTÉGEZ LA RÉPUTATION DE VOTRE MARQUE EN PROTÉGEANT VOS DOMAINES CONTRE L'USURPATION D'IDENTITÉ, LE PHISHING ET LE SPOOFING GRÂCE À UNE GESTION INTUITIVE DE DMARC, DKIM ET SPF.

Email identifié par DomainKeys	Cadre de la politique de l'expéditeur	Authentification, notification et conformité des messages par domaine
DKIM	**SPF**	**DMARC**
Signez vos emails de façon numérique afin que les destinataires sachent que l'email provient bien de vous et qu'il n'a pas été modifié.	Rend légitime votre domaine pour qu'il soit le seul autorisé à envoyer des emails en votre nom.	Veille à l'entretien de votre boîte de réception et détermine ce qu'il advient des emails qui ne respectent pas les normes DKIM ou SPF.

La gestion de l'authentification des emails représente un casse-tête pour de nombreuses entreprises. La mise en place et le maintien de politiques DMARC, DKIM et SPF sécurisées représentent un défi considérable, en particulier pour celles qui gèrent plusieurs domaines. Sans paramètres DMARC appropriés, les entreprises mettent en péril leur « réputation d'expéditeur » et se rendent vulnérables aux tentatives d'usurpation d'identité par email. Dans le même temps, le respect des exigences strictes des fournisseurs de services de messagerie ajoute une nouvelle couche de complexité. Le manque de visibilité sur les performances des campagnes d'emails et l'existence d'activités d'emails cachées au sein des entreprises constituent une autre difficulté désagréable à laquelle les entreprises doivent faire face. En outre, le souhait des entreprises d'atteindre les messageries de leurs clients plutôt que leurs dossiers de courrier indésirable a peu de chances de se concrétiser sans une sécurité adéquate des emails.

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

Ça concerne quoi ?

Communication par email

Comment DMARC Manager vous aide-t-il ?

GARANTIR LA CONFORMITE

Configurez et maintenez sans effort les meilleures pratiques DMARC, DKIM et SPF

GÉRER FACILEMENT LE DNS

Ajoutez en toute transparence des entrées DNS et modifiez-les en quelques secondes

PRÉVENIR L'USURPATION D'IDENTITÉ

Obtenez une vue d'ensemble complète des sources qui envoient des e-mails via vos domaines

Quelles sont les améliorations ?

Assurez la livraison des emails en vous conformant aux normes d'authentification et protégez la réputation de votre marque en même temps

HORNETSECURITY

FICHE D'INFORMATIONS

FONCTIONNALITÉS

Configurateur de domaine : ce service vous offre une interface intuitive pour configurer et maintenir les politiques de meilleures pratiques DMARC, DKIM et SPF ainsi que les paramètres TLS pour plusieurs domaines. Avec DMARC manager, vous pouvez administrer les enregistrements SPF/DMARC et mettre en œuvre des changements DNS en quelques secondes.

Tableau de bord du statut : le tableau de bord vous offre un aperçu complet de diverses statistiques, notamment les domaines gérés, le nombre d'expéditeurs autorisés et non autorisés, le volume d'emails autorisés et non autorisés envoyés, et le nombre d'emails qui ont réussi ou échoué au test DMARC.

Analyse des sources d'emails : cette fonctionnalité vous offre une vue d'ensemble des sources qui envoient des emails par l'intermédiaire de vos domaines. Elle détaille les volumes d'emails, les statuts d'authentification (DMARC pass/fail), la catégorisation des sources (autorisées ou non), la délivrabilité, la réputation de l'expéditeur et le niveau de menace.

Image de marque par email BIMI : une fois que votre domaine est conforme à la norme DMARC, vous pouvez utiliser la fonctionnalité BIMI qui vous permet d'afficher votre logo à côté des emails dans les boîtes de réception prises en charge, ce qui maximise l'impact des emails, la reconnaissance de la marque et la confiance.

Chiffrement SMTP-TLS : assurez-vous que les emails sortants sont transmis en toute sécurité grâce au chiffrement SMTP-TLS. Recevez des rapports détaillés sur les emails qui n'ont pas été chiffrés et qui n'ont pas été transmis, ce qui constitue une autre couche de sécurité pour vos communications par email.

Rapports d'échecs et alertes : les rapports d'échecs fournissent des données détaillées en temps réel sur les emails qui échouent aux contrôles DMARC. Cela vous aide à comprendre qui envoie des emails au nom de vos domaines et pourquoi certains emails ne sont pas transmis. Configurez les alertes de votre choix et recevez un email à l'adresse spécifiée lorsqu'un événement se produit, ce qui vous permet de réagir plus rapidement aux menaces.