HORNETSECURITY

DMARC MANAGER

LA SOLUTION À L'USURPATION D'ADRESSE ÉLECTRONIQUE

La confiance est le fondement même des communications électroniques professionnelles, cependant les cybercriminels exploitent cette confiance en usurpant l'identité de domaines ou de personnes de confiance pour perpétrer des escroqueries, ce qui conduit souvent à des attaques de type « Business Email Compromise » (BEC).

L'IMPACT DE L'USURPATION D'ADRESSE ÉLECTRONIQUE :

» **Perte financière** due à des emails frauduleux (par exemple, de fausses factures).
» **Atteinte à la réputation** due à l'usurpation d'identité, entraînant une perte de confiance de la part des clients et des partenaires.
» **Risque accru d'attaques par phishing,** exposant les données sensibles de l'entreprise.

DMARC : VOTRE DÉFENSE CONTRE L'USURPATION D'ADRESSE ÉLECTRONIQUE

DMARC (Domain-based Message Authentication, Reporting & Conformance) est un puissant protocole d'authentification des e-mails qui aide les entreprises à prévenir l'usurpation d'adresse électronique. Il fonctionne avec **SPF** et **DKIM** pour garantir que seuls les e-mails autorisés sont envoyés à partir de votre domaine, protégeant ainsi votre marque et vos canaux de communication.

COMMENT ÇA FONCTIONNE :

SPF vérifie l'enregistrement SPF du serveur d'envoi pour s'assurer que l'email a été envoyé à partir d'une adresse IP autorisée. Si l'adresse IP est répertoriée dans l'enregistrement SPF, la vérification est concluante, sinon elle échoue.	**DKIM** vérifie si l'email est chiffré avec la clé privée du domaine d'envoi, puis la valide par rapport à la clé publique correspondante. Si la correspondance est positive, le contrôle est réussi, sinon il échoue.	**DMARC** vérifie que le « de » de l'email est correspond au même domaine de messagerie que SPF et DKIM ont validé lors de leurs propres vérifications.	Enfin, **la balise de politique** (« p ») dans l'enregistrement DMARC du domaine d'envoi indique au serveur de réception comment traiter l'email en fonction des résultats de la vérification.

HORNETSECURITY

La mise en place et la maintenance des politiques DMARC, DKIM et SPF peuvent s'avérer de véritables casse-têtes, en particulier si vous gérez ces politiques pour des entreprises importantes et complexes, en gérant de nombreux domaines, de multiples configurations et des exigences potentiellement différentes pour chaque domaine.

MAIS IL EXISTE UNE SOLUTION : **ÉVITER LE CASSE-TÊTE LIÉ À LA CONFIGURATION DE DMARC GRÂCE À DMARC MANAGER**

AVEC DMARC MANAGER, VOUS POUVEZ :

- Avoir une visibilité sur les personnes qui envoient des emails sous un domaine et redonner le contrôle au propriétaire du domaine, ce qui renforce et sécurise la réputation de la marque.
- Mettre en place et maintenir facilement des politiques de meilleures pratiques DMARC, DKIM et SPF pour plusieurs domaines.
- Obtenir des informations sur l'état de la livraison et de l'authentification des emails, ce qui permet d'identifier les campagnes légitimes et les tentatives potentielles d'usurpation d'identité.
- Améliorer les stratégies de marketing par email en s'assurant que les emails en masse sont livrés en respectant les normes d'authentification exigées par les principaux fournisseurs de services de messagerie tels que Yahoo et Gmail.
- Renforcez votre conformité aux réglementations sectorielles/mondiales telles que PCI DSS, NIST, GDPR, HIPPA, etc.

EN SAVOIR PLUS