

Guide : Lire les en-têtes Received des emails

Qu'est-ce qu'un en-tête Received ?

Chaque fois qu'un email passe par un serveur SMTP, une ligne Received est ajoutée en haut du message. Ces lignes montrent le chemin parcouru par l'email, du serveur d'origine jusqu'à la boîte du destinataire.

À quoi sert-il ?

L'en-tête Received permet de :

- Suivre les retards de livraison
- Identifier le MTA source
- Vérifier si l'email a bien été authentifié
- Détecter un spam ou une usurpation d'identité

Comment l'interpréter ?

Les en-têtes Received sont lus de bas en haut (le plus ancien est en bas).

Exemple :

Received: from mail.example.com (mail.example.com [192.0.2.1]) by mx.google.com with ESMTPS id abc123;

Tue, 30 Apr 2024 14:55:03 +0000 (UTC)

- mail.example.com : serveur émetteur
- mx.google.com : serveur récepteur (Gmail ici)
- Heure exacte de transmission entre les deux

Bonnes pratiques :

- Comparez les horodatages pour mesurer les délais
- Vérifiez que l'IP et le hostname sont cohérents
- Surveillez les anomalies (sauts d'heures, relais inconnus...)