Cybersecurity Insights

Google & Yahoo s’arment contre le spam et le phishing, êtes-vous prêts ?

Arnaud **LEBRUN**
Guillaume **HUREL**

Partner Almond
Consultant Cyber Tech & Transformation

UN DURCISSEMENT DES RÈGLES ANNONCÉ PAR GOOGLE ET YAHOO

Le 3 octobre 2023, les deux importants fournisseurs de messagerie, Google et Yahoo, ont annoncé durcir les règles de remise des emails vers leurs services.

Ces nouvelles mesures **visent à empêcher les spams et les messages malveillants** d'atteindre les boîtes de réception des utilisateurs de Google et Yahoo.

Toutes les organisations envoyant des emails à des utilisateurs utilisant les services de messagerie de Google ou Yahoo sont concernées. Les expéditeurs **de plus de 5000 emails** par jour ont des **exigences plus strictes.**

Ces mesures s'appliquent progressivement depuis le **2 février 2024.**

En cas de **non-conformité,** Google et Yahoo menacent **de ne plus remettre les emails** dans les boîtes des destinataires.

COMMENT SE CONFORMER À CES NOUVELLES MESURES ?

Les exigences pour tous les expéditeurs

Se protéger contre l'usurpation d'identité

→ Définir au moins une méthode **d'authentification pour vos emails** (SPF ou DKIM) :

- **SPF** permet de déterminer quelles adresses IP ont le droit d'envoyer des emails pour votre domaine.
- **DKIM** permet d'authentifier les emails de votre domaine grâce à une signature cryptographique.

→ Définir une **politique** DMARC **en cas d'échec de l'authentification** de vos emails :

- **DMARC** permet de définir une politique de traitement des emails en cas d'échec des contrôles effectués par SPF et DKIM.

→ Disposer d'un **enregistrement Reverse DNS** (rDNS) pour votre domaine :

- **L'enregistrement rDNS** permet de confirmer que votre domaine est associé à l'adresse IP qui envoie les emails.

Lutter contre le spam

→ Maintenir un taux de spam <0,3 % :

- Chaque fois que quelqu'un marque un de vos emails comme indésirable, votre taux de spam augmente. Pour ne pas dépasser le seuil de tolérance, vous devrez **surveiller les indicateurs de spam par des outils dédiés** (comme Postmaster Tool de Google).

→ Respecter la norme Internet RFC 5322 :

- Les spams contiennent parfois des en-têtes en double pour être plus efficaces. **La norme RFC 5322** qui définit le format approprié des emails, y compris leur corps, leurs en-têtes et leurs pièces jointes interdit cette pratique.

COMMENT SE CONFORMER À CES NOUVELLES MESURES ?

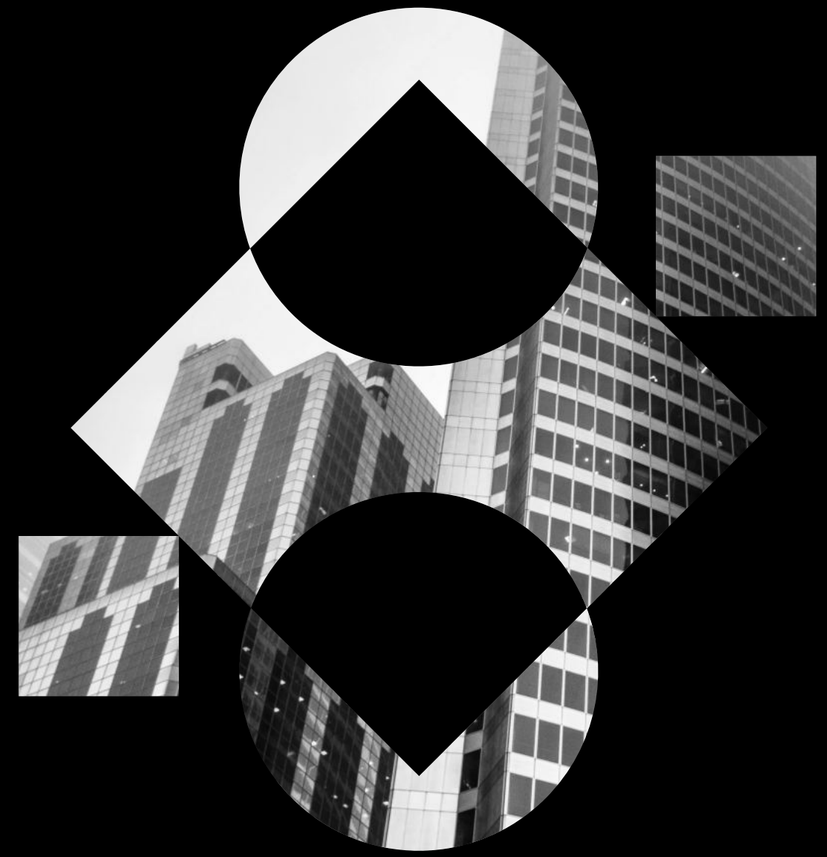
Les exigences pour les expéditeurs de plus de 5000 emails par jour

En plus des exigences précédentes, ces règles supplémentaires s'appliquent :

Se protéger contre l'usurpation d'identité

→ Définir les **deux méthodes d'authentification SPF et DKIM.**

→ Définir une **politique DMARC restrictive qui n'autorise que le domaine authentifié lors des vérifications SPF et DKIM.**



Lutter contre le spam

→ **Faciliter le désabonnement** aux communications commerciales :

- Placer un lien de **désabonnement en 1 clic** clairement visible dans le corps du message. Le désabonnement doit être **effectif sous deux jours.**

LES BÉNÉFICES ATTENDUS DE LA MISE EN CONFORMITÉ

En mettant en œuvre ces nouvelles règles de remise, Google et Yahoo rappellent **les bonnes pratiques de sécurité** de la messagerie accélérant ainsi les chantiers de sécurisation parfois en attente de sponsoring.

Cette conformité apportant des avantages tangibles tant pour les expéditeurs de campagnes marketing que pour les destinataires :

POUR LES EXPÉDITEURS

- Protection accrue de la marque en réduisant le risque d'usurpation d'identité des domaines de messagerie.
- Garantie de délivrabilité des emails.
- Meilleure visibilité des emails.
- Renforcement de la réputation de la marque.

POUR LES DESTINATAIRES

- Amélioration de la sécurité de la messagerie en luttant contre le phishing.
- Meilleure expérience utilisateur grâce à la réduction des spams.
- Renforcement de la confiance dans les messages reçus.

Avec le paramétrage d'une politique DMARC, vous pourrez utiliser la **norme BIMI** (Brand Indicators for Message Identification) afin que vos communications se distinguent parmi les messages reçus par vos clients.