

e-Mailing, spam : les bonnes pratiques



Gestan peut expédier des mails à des groupes de vos contacts. Au delà de 100 mails identiques envoyés à des destinataires différents, on peut commencer à parler de “mailing de masse”.

Pour envoyer un mail, il est nécessaire d'utiliser un service d'envoi de mail mis à votre disposition le plus souvent soit par le fournisseur de votre connexion internet, soit par le fournisseur de votre nom de domaine : il s'agit du service SMTP, ou serveur SMTP.

Il est important de respecter un certain nombre de règles, en matière d'e-mailing, afin d'éviter que vos destinataires ne se plaignent. Si vous suscitez trop de plaintes de vos destinataires, votre fournisseur SMTP peut vous couper l'accès au service.

Aussi recommandons-nous vivement de respecter les bonnes pratiques suivantes :

1. **“Confirmed Opt-In”** : vous ne pouvez envoyer un message à un destinataire privé que si votre destinataire a exprimé son consentement préalable (du moins en France, et dans de nombreux autres pays). Il vous faut donc un processus d'inscription qui prévoit de recueillir cet accord explicite (en général, un formulaire d'inscription suivi d'une confirmation explicite du destinataire).
2. **Maintenance de votre liste d'adresses** : supprimez toute adresse erronée de vos listes. Plus votre taux d'erreur est élevé, plus votre réputation se dégrade.
3. **“One-Click-Unsubscribe”** : Fournissez dans chaque message un lien par lequel le destinataire pourra se désinscrire, si possible en un seul clic.
4. **Format** : Si vous envoyez des e-mails en HTML, ajoutez une partie formatée en texte seulement afin d'assurer que vos messages soient lisibles chez tous vos destinataires (Gestan le fait automatiquement si votre codage HTML est correct).
5. **Provenance du message** : Précisez l'adresse de l'inscription du destinataire. Exemple : 'Vous recevez ce message parce que vous vous êtes inscrit à www.votredomaine.fr <<http://www.votredomaine.fr>>. Au cas où vous ne souhaiteriez plus les recevoir, veuillez cliquer ici (lien).'
6. **Poids des messages** : surveillez que vous n'envoyez pas des messages trop lourds. Pour un mailing de masse, un message de 300 Ko est une limite à ne pas dépasser. 100 ko est une valeur raisonnable. Si votre message comporte des images, préférez l'inclusion dans vos messages sous forme d'une adresse. Idem pour les pièces jointes.
7. **Inscription CNIL et collecte de données personnelles** : en France, la détention de tout fichier nominatif est soumise à déclaration à la CNIL. Il est interdit de procéder à la collecte de données nominatives sans l'accord de la personne concernée : à ce titre, le tracking des e-mails n'est théoriquement pas autorisé (Gestan ne le fait pas).

Avant toute expédition sur un nombre conséquent d'adresses (>100), nous vous recommandons de vous assurer auprès du service SMTP que vous allez utiliser que tout va bien se passer. En effet, de nombreux serveurs SMTP sont bridés en nombre de mails expédiables dans un délai donné.

Pourquoi vos emails arrivent-ils en spam ? 7 raisons possibles !

Source : codeur.com

1. Vous utilisez un domaine gratuit pour vos campagnes emailing

Gmail, yahoo, outlook, et autres hotmail, ne sont pas recommandés pour vos campagnes emailing. En effet, les Fournisseurs d'Accès Internet (FAI) rejettent les emails groupés provenant de ces domaines gratuits.

Ils préfèrent des noms de domaines enregistrés par un expéditeur individuel, qu'ils peuvent retrouver et dont ils peuvent évaluer la réputation.

Que faire ? Servez-vous de votre nom de domaine pour créer une adresse de messagerie dédiée à vos emailings. Celle-ci devrait ressembler à : `serviceclient@monentreprise.com`.

Ainsi, vous pouvez construire votre propre réputation d'expéditeur auprès des FAI. Sans compter que cette pratique donne une image plus professionnelle à vos newsletters.

2. Vous n'avez pas authentifié vos emails

L'une des principales raisons du spam est l'absence d'une authentification correcte. C'est comme quand vous refusez un appel parce que vous ne reconnaissez pas le numéro appelant.

Il existe des technologies pour authentifier vos emails et augmenter votre taux de délivrabilité. Cette pratique rend votre domaine digne de confiance aux yeux des filtres anti-spam. Les principales technologies d'identification d'emails sont :

- DKIM (Domain Key Identified Mail) : fournit une clé de cryptage et une signature numérique pour vérifier vos emails.
- SPF (Sender Policy Framework) : vérifie si l'adresse IP de l'expéditeur est approuvée.
- DMARC : vous devez déjà utiliser DKIM et SPF.

Si vous utilisez un nom de domaine personnalisé, vous pouvez mettre en place ces méthodes d'authentification en ajoutant des enregistrements TXT dans la gestion DNS de votre domaine.

3. Vous utilisez des mots associés aux spams

Pour protéger leurs utilisateurs des escroqueries, les FAI disposent d'une liste de mots déclencheurs de spam. En voici quelques-uns :

- Chèque
- Gratuit ou sans frais
- Offre exceptionnelle
- Garantie
- Augmenter les ventes
- Commander maintenant
- Sans risque

- Promotion spéciale
- Gagnant
- Argent

Des textes tout en majuscules, les points d'exclamation et l'abus d'émojis, ainsi que les fautes de grammaire, constituent également des raisons pour finir dans la boîte spam.

Contactez votre fournisseur pour connaître les mots qui déclenchent des signaux d'alerte et faites-en une liste des termes à éviter dans la ligne d'objet.

D'une manière générale, évitez les objets qui font des promesses mirobolantes ou proposent des offres exceptionnelles. Restez mesuré et factuel dans vos propos.

4. Vos emails ne sont pas HTML compatibles

Lorsque vous envoyez des emails à des amis ou à votre famille, le contenu est essentiellement textuel.

En tant qu'entreprise, vous devez inclure des visuels, des animations, un ou plusieurs boutons d'appel à l'action et d'autres éléments graphiques pour favoriser l'engagement. Pour cela, vous avez besoin de rédiger vos emails en HTML.

Cependant, vous devez suivre les bonnes pratiques pour éviter que le design devienne un prétexte pour se retrouver en spam :

- Utilisez une largeur maximale de 600 à 800 pixels pour vos emails.
- Veillez à ce que le code HTML soit le plus clair et le plus simple possible. Évitez les langages Javascript et Flash qui ne sont plus pris en charge par beaucoup de FAI.
- Maintenez un faible ratio image/texte.
- Optimisez et allégez vos images.
- Optimisez votre email pour les mobiles avec de petites images et des polices facilement lisibles.

5. Vos emails contiennent trop de pièces jointes

Les pièces jointes sont souvent utilisées pour diffuser des virus. Ainsi, elles déclenchent une alarme auprès des filtres anti-spam, en particulier les fichiers « .exe ».

Vos campagnes emailing ne doivent pas contenir de fichiers joints. Si vous devez en inclure, rendez disponible le document sur votre site Internet ou via un service de stockage cloud comme Dropbox ou Google Drive.

6. Vos emails ne comportent ni coordonnées ni lien de désabonnement

Les adresses physiques et les boutons de désabonnement participent à l'amélioration de la délivrabilité de vos emails. Par ailleurs, ils sont essentiels dans la gestion de votre image de marque.

En bas de page, pensez à bien indiquer les coordonnées de votre siège social. Pareil pour le lien de désabonnement. Celui-ci doit être visible en haut ou en bas de votre message. Si vous entravez la désinscription, les abonnés vous déclareront alors comme spam pour ne plus recevoir vos messages.

7. Vous envoyez trop d'emails en une seule fois

Si vous envoyez habituellement des emails à 10 000 abonnés et que vous passez soudainement à

200 000, vous risquez de déclencher les filtres anti-spam des FAI. Ce pic est considéré comme un comportement inattendu, voire comme une attaque malveillante.

Alors, si vous avez prévu d'augmenter la cadence, faites-le progressivement pour chauffer votre adresse IP.

i Autres articles “Technique”

- [Accès à distance](#)
- [Arrondis](#)
- [Développements spécifiques](#)
- [e-Mailing, spam : les bonnes pratiques](#)
- [Envoyer des mails avec Gestan](#)
- [Etats et Requêtes](#)
- [Etendre les fonctionnalités de Gestan](#)
- [Externalisation du courrier](#)
- [Gestan sur MAC](#)
- [Itinerix *](#)
- [Mettre en place un certificat SSL](#)
- [Migration de la version 15 vers la version A1](#)
- [Mise en réseau de Gestan](#)
- [ODBC sur HFSQL](#)
- [Paieement en ligne \(Paypal\)](#)
- [Paramétrer la recherche](#)
- [Présentation générale de Gestan](#)
- [Répertoires et fichiers](#)
- [Sauvegarde des données Gestan](#)
- [Serveur SMTP Google](#)
- [Serveur SMTP Office 365](#)
- [Serveur Spare](#)
- [Temps de réponse](#)
- [Tester la communication](#)
- [Tester votre connexion Internet](#)
- [Transférer Gestan d'ordinateur](#)
- [Tuto détaillé SuperPDP](#)
- [Téléphonie SIP-TAPI *](#)
- [Utiliser Linux](#)

From:
<https://manuel.gestan.fr/> - **Le manuel de Gestan**

Permanent link:
<https://manuel.gestan.fr/fr/wiki/tech/emailing>

Last update: **2026/06/22 19:37**