Envoyer des mails avec Gestan *

La proportion de mails non sollicités (spam) étant devenue très importante (de 55 à 95% du trafic selon les moments et les mesures), les entreprises gérant la transmission des mails ont considérablement durci les contraintes qui s'appliquent à l'envoi de mails. Aussi, si un expéditeur s'écarte trop des “bonnes pratiques”, les mails envoyés ne seront pas délivrés à leur destinataire. Dans le pire des cas, l'adresse IP du serveur expéditeur sera blacklistée, et les mails suivants, même légitimes, ne seront plus délivrés.

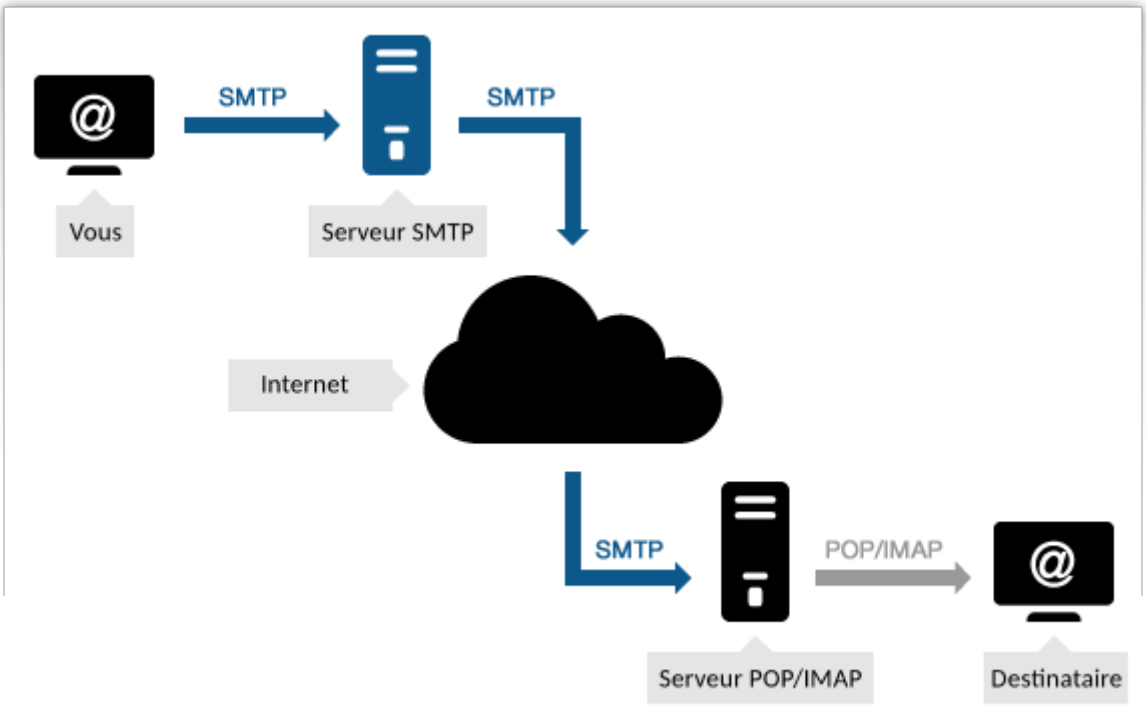
Il est donc important de connaître ces “bonnes pratiques” pour augmenter la délivrabilité de vos mails.

Les bases de l'envoi de mail

Pour envoyer un mail, votre ordinateur va utiliser le *service SMTP* (Simple Mail Transfer Protocol), pour envoyer votre mail sur le *Serveur SMTP* que vous aurez spécifié. Puis ce *serveur SMTP* va envoyer votre mail sur le *serveur POP/IMAP* de votre destinataire, sur lequel ce dernier va se connecter pour lire votre message. Pour simplifier, un serveur SMTP est le “tuyau de sortie” pour vos courriels.

Par exemple, si vous (moi@monentreprise.com) avez envoyé un mail à contact@gestan.fr, votre mail transitera via le protocole SMTP jusqu'à parvenir au serveur de messagerie du domaine monentreprise.com, pour être transmis au serveur de messagerie du domaine gestan.fr. votre destinataire, quand il va se connecter à sa messagerie, va se connecter au serveur de mail de son domaine, et va récupérer ses messages via le protocole IMAP (ou POP3).

L'ensemble de la transmission peut se représenter comme suit :



Au cours de la transmission, les serveurs effectuent des contrôles pour vérifier que votre mail n'est pas un courriel non-sollicité (spam). Votre message va obtenir un “spam score” : si ce score est trop élevé, votre message sera soit classé dans la boite spam de votre destinataire, soit carrément supprimé. On appelle *“délivrabilité”* le potentiel de votre mail à ne pas être classé en spam : il faut que votre délivrabilité soit maximale (donc qu'il obtienne le spam score le plus bas possible).

Comment vous assurer que vos mails n'arrivent pas en spam ?

S'il était possible, dans les débuts de l'utilisation des mails (depuis les années 60 jusqu'aux années 2000 environ), d'envoyer des mails sans contraintes, ce n'est plus du tout le cas aujourd'hui, tous les fournisseurs de service SMTP ayant durci les conditions d'envoi de mail.

Si vous enfreignez trop les règles d'envoi de mail, non seulement vos mails n'arriveront pas, mais l'adresse IP de votre serveur SMTP pourra être blacklistée, et les mails suivants, même légitimes, seront classés en spam. L'expertise en délivrabilité est devenue quasiment un métier à part entière.

Voici les points à vérifier pour vous assurer d'une bonne délivrabilité de vos mails.

Utiliser un nom de domaine professionnel

Utiliser une adresse mail générique (par exemple plomberie83@gmail.com) n'est pas une solution professionnelle.

Utilisez une vraie adresse professionnelle, comme par exemple contact@plomberie83.fr, et votre propre serveur SMTP (plus d'information sur le site de Mailjet).

📌 Un nom de domaine professionnel coûte entre 10 et 15 euros par an. Il s'ouvre en 10 minutes. Si vous souhaitez un nom de domaine professionnel, n'hésitez pas à en faire la demande auprès de dev@gestan.fr.

Utiliser votre propre serveur SMTP, ou un SMTP professionnel

Quand vous envoyez des mails, vous précisez le SMTP que vous utilisez.

Par exemple, vous pourriez préciser que les mails que vous expédiez depuis l'adresse mail contact@plomberie83.fr doivent utiliser le SMTP de GMail. Ce n'est pas une bonne idée, les mails transitant pas les serveurs de Google étant scannés et utilisés à des fins publicitaires.

Préférez :

- soit le serveur SMTP rattaché à votre nom de domaine. Si vous avez acheté un domaine comme maboite.com, votre fournisseur de nom de domaine met à votre disposition un serveur SMTP
- soit un serveur SMTP professionnel, il y en a pléthore

Authentifier vos mails

Pour authentifier vos mails, il faut paramétrer :

- votre enregistrement SPF
- votre enregistrement DKIM
- votre enregistrement DMARC

Ce sont des éléments de votre paramétrage DNS, qui s'effectue depuis l'interface de gestion de votre nom de domaine, dépendant de votre fournisseur de nom de domaine.

Eviter les mots liés au spam

Eviter le plus possible les mots qui sont souvent en relation avec des spams, comme : “Gratuit”, “sans frais”, “Offre exceptionnelle”, “Garantie”, “Augmenter les ventes”, “Commander maintenant”, “Sans risque”, “Promotion spéciale”, “Gagnant”, “Argent”.

Évitez aussi les textes entièrement en majuscules, trop de points d□exclamation, l□abus d□émojis, ainsi que les fautes de grammaire ou d'orthographe.

Codage HTML

Si vous envoyez des mails au format HTML (par opposition au format texte simple), suivez ces recommandations le plus possible :

- Utilisez une largeur maximale de 600 à 800 pixels
- Veillez à ce que le code HTML soit le plus clair et le plus simple possible. Évitez Javascript et Flash.
- Evitez de mettre trop d'images par rapport au texte
- Optimisez et allégez vos images.

Pièces jointes

Envoyez le minimum de pièces jointes.

Si vous avez des pièces jointes en nombre important, ou de grande taille, faites une archive zip et rendez les disponibles soit en les transmettant par un service respectant la confidentialité (par exemple swisstransfer, gratuit), soit via un service de stockage comme un emplacement FTP sur votre site Internet (évitez les services comme Dropbox ou Google Drive, la confidentialité n'étant pas garantie).

Précaution pour les emailings de masse

Au delà de 100 mails identiques envoyés à des destinataires différents, on peut commencer à parler de □mailing de masse□. Que vous effectuiez un mailing de masse par les fonctions d'envoi de mail de Gestan, ou par tout autre moyen, veillez à respecter ces dispositions :

- intégrez obligatoirement vos coordonnées, et un bouton de désabonnement, qui doit être visible en haut ou en bas de votre message. Si vous entravez la désinscription, certain de vos destinataires pourront vous déclarer comme spammeur, et ainsi dégrader votre réputation Internet.
- évitez d'envoyer trop d'emails à la fois : si vous envoyez habituellement des emails à 1000 abonnés et que vous passez d'un coup à 100.000, vous allez déclencher les filtres anti-spam des FAI. Si vous avez un envoi important à faire, avertissez votre hébergeur de domaine, ou mieux, passez par un service spécialisé comme Brevo, Mailjet ou autre.
- nettoyez régulièrement votre liste d'envoi : au dessus d'un certain taux d'adresses erronées, votre envoi pourra être considéré comme un spam.
- attention au taux de signalement comme spam. Le taux de plainte pour spam doit rester sous les 0,10 %.

***Réglementation France** : en France, un envoi régulier de messages n'est licite que si le destinataire a exprimé son consentement préalable à recevoir des emails. Il vous faut donc une inscription et une confirmation explicite du destinataire par la suite. La détention de tout fichier nominatif est soumis 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).*

Le blacklistage

Si un certain nombre de critères sont réunis (contenu des messages, volume, rythme d'envoi, etc), les serveurs par lesquels transitent les mails envoyés peuvent blacklister l'adresse IP de l'expéditeur, et bloquer toute transmission d'un mail provenant de la machine correspondante. Votre adresse IP peut être blacklisté à juste titre, parce que vous envoyez du spam, mais elle peut aussi être blacklistée par erreur, ou parce qu'un tiers a usurpé votre nom de domaine, ou a pris le contrôle de votre machine.

Comment faire pour savoir si votre IP est blacklistée

Vous pouvez utiliser par exemple le site multiRBL, qui va interroger les principaux serveurs de mail.

Si votre adresse IP est blacklistée, il ne vous reste plus qu'à entrer en contact avec les administrateurs de la liste, pour savoir pourquoi vous y figurez, et ce qu'il faut faire pour en sortir.

Note: **Pourquoi vous ne devriez pas utiliser une adresse personnelle pour vos communications professionnelles**

Une adresse mail provenant d'un domaine générique comme wanadoo.fr, orange.fr, free.fr, gmail.com, etc. (par exemple gestan@orange.fr ou gestan@gmail.com) n'est pas censée être une adresse professionnelle : une adresse mail **professionnelle** est suffixée par le domaine de l'entreprise, (par exemple contact@gestan.fr ou recrutement@gestan.fr).

Ainsi, l'adresse professionnelle de Bernard Arnault n'est certainement pas b.arnault@gmail.com, mais plutôt quelque chose comme b.arnault@lvmh.fr.

Or le support constate que beaucoup d'entreprises utilisent des adresses mail personnelles, notamment des adresses en gmail, pour leurs communications professionnelles.

En utilisant une adresse professionnelle à la place, vous bénéficiez de trois avantages majeurs :

- **vous améliorez la délivrabilité de vos courriels**, notamment par la possibilité de renseigner vos enregistrements DKIM et SPF.
- **une adresse professionnelle participe à construire votre identité de marque** : aucune entreprise "respectable" ne communique avec un domaine générique. Utilisant le domaine de votre entreprise, vous renforcez votre image de professionnalisme.
- **vous protégez vos données commerciales et celles de vos clients** : quand vous utilisez une adresse générique, les mails transitent par des serveurs dont la confidentialité n'est pas garantie, spécialement les services proposés par des entreprises étrangères comme Google avec gmail, relevant du Patriot Act et du Cloud Act. Vos données commerciales, mais aussi celles de vos clients sont ainsi susceptibles d'êtres exploitées ou revendues par ces entreprises tierces, sans que vous n'en soyez averti.

Pour aller plus loin

Formation

- SMTP : relais, serveur, on vous explique tout en 5 minutes ! (Mailjet)
- La délivrabilité.
- Eviter de passer en liste noire
- Arobase, site généraliste sur l'email

Technique

- Pourquoi vos emails arrivent-ils en spam ? 7 raisons possibles ! (Codeur)
- Utilisation du SMTP de Google (GMAIL)

SPF, DKIM, DMARC

- Tout savoir sur l'enregistrement SPF
- Utilité du SPF.
- l'enregistrement DKIM
- DMARC, DKIM et SPF

Outils

- Un site pour tester votre serveur SMTP
- Interface DIG
- 9 outils de test de délivrabilité.

Actu

- L'impact des mises à jour de sécurité de Gmail et Yahoo en 2024 sur votre emailing (Mailjet)

Tester votre délivrabilité

Tester votre délivrabilité

Vous pouvez tester la délivrabilité de vos mails auprès de services tels que :

- https://www.mail-tester.com
- http://www.isnotspam.com
- https://mxtoolbox.com/deliverability
- https://kickbox.com
- https://www.sendforensics.com/email-deliverability-test
- MultiRBL.valli

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
Paiement 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
Téléphonie SIP-TAPI *
Utiliser Linux