

Note pour Brainsonic : notre système de messagerie (Exchange/MS365) a un comportement proche des systèmes de nos clients. C'est donc un bon point de départ pour des tests de bonne configuration

Listons ici les bonnes pratiques qui permettent de s'assurer (ou du moins de réduire le risque) que les destinataires, leurs employés, leurs clients et partenaires, recevront bien les emails d'un nouveau service, site.

Configurer un envoi depuis Sendinblue

1. Se connecter à la [plateforme Sendinblue](#) à l'aide du compte `liveteam@brainsonic.com`
2. Aller dans le menu Expéditeurs et IP
3. Cliquer sur Ajouter un nouvel expéditeur
4. Définir un nom d'expéditeur (nom qui s'affichera dans le champ De dans le client email du destinataire)
5. Définir une adresse d'envoi de type `no-reply.[nom du client]@eventmailing.brainsonic.com`
6. Ajouter une IP et sélectionner `153.92.227.92 eventmailing.brainsonic.com`
7. Valider le formulaire
8. Dans les paramètres de votre Campagne choisissez l'expéditeur que vous venez de créer.

Configurer avant de tester

Ne pas envoyer d'email avant d'avoir effectué toute la configuration car la réputation du nouveau service pourrait être impactée négativement

Entrées DNS

Ajouter les entrées DNS sur le domaine d'expédition. Elles sont probablement fournies par le service d'envoi - Dans les exemples l'envoi se ferait avec l'adresse

`nepasrepondre@mail.mondomaine.com`

- - DMARC (en général un `_dmarc.mail.mondomaine.com IN TXT "..."`)
 - SPF (en général un `mail.mondomaine.com IN TXT "v=spf1..."`)
 - Une clé spécifique au service d'envoi (en général un `mail.mondomaine.com IN TXT "code=..."`)
 - DKIM (en général un `mail._domainkey.mail.mondomaine.com IN TXT "code=..."`)

Contenu du message

Veillez à ce que les liens inclus dans le courriel soit tous avec le protocole `https://`

Campagnes d'invitation

Si vous envoyez une sollicitation commerciale (i.e., campagne d'invitation) c'est que vous risquer d'envoyer beaucoup d'email sur les mêmes systèmes de messagerie (par opposition aux emails transactionnels qui arrivent au fil de l'utilisation).

Dans ce cas il faut respecter les règles classiques du mass-emailing :

- ○ Assurez-vous d'avoir obtenu le consentement explicite des récipiendaires à recevoir cette sollicitation
- Assurez-vous que la liste de récipiendaires est à jour et qu'elle ne comporte pas (trop) d'alias inexistantes
- Ajouter un lien unsubscribe au pied de page
- Mentionner le nom et l'adresse (postale) de l'organisation qui exploitera les données collectées

Adapter les règles anti-usurpation

S'applique uniquement aux envois dont l'expéditeur fait partie du(des) même domaines que l'organisation destinatrice.

Une règle Anti-usurpation d'identité a pu être mise en place. Il sera donc nécessaire d'ajouter une exception.

Exemple : un courriel est considéré comme indésirable si son expéditeur est hors de l'organisation ET qu'il utilise un domaine appartenant à l'organisation.

Il faudra alors ajouter une règle du type : "Sauf si l'adresse IP de l'expéditeur est".

Exemple de règle anti-spoofing pour Brainsonic sur Exchange Online

The screenshot shows the Exchange Admin Center interface. On the left is a navigation pane with 'mail flow' selected. The main area displays a list of rules, with 'Spoofing' highlighted. The configuration for this rule is shown on the right, including an 'Except if...' section with two red arrows pointing to IP address ranges: '153.92.227.92' and '77.32.172.135'. The rule body contains the text 'création projet'.

Dans le cas de Brainsonic, nous avons ajouté le domaine `eventmailing.brainsonic.com` afin qu'ils ne soient pas considérés comme potentielle usurpation d'identité.