Nos recommandations pour assurer une bonne délivrabilité de vos communications par mail

Mon mail n'est pas un spam !

Pour être lu, le message doit être transmis. Le messager doit donc être de qualité pour être autorisé à délivrer son message.

En 2023, une majorité du trafic mail mondial est du spam (*email envoyé en masse et non sollicité par le destinataire*) Cette statistique souligne la nécessité de se conformer aux bonnes pratiques d'envoi et d'éviter les comportements susceptibles de déclencher les filtres anti-spam.

Canal de communication simple et efficace par excellence, l'email tient une place considérable dans les moyens de communications numériques, en complément des sites web, des réseaux sociaux et autres supports. Il est ainsi très utilisé par les marques, les entreprises et les particuliers pour s'adresser à leurs abonnés, leurs clients et leurs contacts.
Outil incontournable, le mail est aussi une porte d'entrée facile pour les tentatives d'extorsion, escroquerie et autres tentatives de fraude.
Les fournisseurs de messagerie ont durci d'année en année leurs filtres anti-spam.

L'envoi de masse de courriels se trouve donc au croisement de 2 enjeux majeurs :
- la délivrabilité
- la lutte contre les spams

La délivrabilité, qui concerne la capacité des courriels à atteindre efficacement les boîtes de réception des destinataires, dépend de multiples facteurs, tels que la qualité de la liste de contacts, le respect des bonnes pratiques d'envoi, et la configuration appropriée des paramètres techniques. *cf liste en document joint*

En parallèle, la lutte contre les spams est une préoccupation essentielle, car les filtres anti-spam des fournisseurs de messagerie se sont durcis en 2024 et filtrent sévèrement les courriels non sollicités ou suspects, menaçant ainsi la visibilité et l'impact des campagnes de marketing par courriel.
Ainsi, maîtriser ces deux aspects devient impératif pour optimiser l'efficacité et la légitimité des envois de courriels en masse.

Sans évoquer ici les spams venant de pseudo comptes officiels (Police, Post, ou d'autres faux expéditeurs) pour vous soutirer des informations ou de l'argent, les mailing de vos newsletter ont pu connaitre ces derniers temps des difficultés d'acheminement, de délivrabilité.

L'Office information et communication vous recommande ainsi sous forme de check-list pratique et utile ses recommandations sur les bonnes pratiques d'envoi en nombre de mails.

Check-list - 10 bonnes pratiques

Chaque adresse mail d'expéditeur ou du moins son domaine d'adresse, @eerv.ch par exemple, est analysé par les serveurs de réception d'e-mail (Gmail, bluewin, infomaniak,…) et les clients de messagerie (Outlook, Exchange, etc.)

Un score est alors attribué avec son taux de spam. Plus ses adresses en @eerv.ch sont classées en spam, plus le domaine est mal noté et donc ses mails MAL DELIVRÉS.
Un taux de spam supérieur à 0,1% peut nous valoir d'être relégué directement en spam par un fournisseur de messagerie pour nos prochaines campagnes.

Voici 10 recommandations pour améliorer la délivrabilité des e-mails en général et dans l'écosystème EERV en particulier :

1. ☐ **Utiliser une liste de contacts propre et bien entretenue :** Assurez-vous que votre liste de contacts est composée d'adresses e-mail valides et actives. Supprimez régulièrement les adresses invalides et les abonnés inactifs pour maintenir la qualité de votre liste.
   Mettez à jour votre liste régulièrement- Respecter bien les demandes de désabonnement

2. ☐ **Personnaliser les e-mails :** L'intitulé de l'expéditeur et le mail associé doivent être explicites et ne pas inciter le destinataire à vous déclasser en spam.
   43% des destinataires signalent l'email comme spam sur la base de l'adresse de l'expéditeur.
   Eviter en EERV les mails no-reply et indiquer bien le nom de votre Entité Paroisse de xxx – EERV et un mail valide nom.prenom@eerv.ch ou paroisseXX@eerv.ch ou paroisse@bluewin.ch
   Les e-mails personnalisés avec la mention des *nom et prénom* des abonnés ont tendance à avoir un meilleur taux d'ouverture et d'engagement.

3. ☐ **Éviter les « spam words » et « spam phrases » en objet**
   Il convient de rédiger un objet de mail clair, précis, rassurant et sans fausses promesses.
   Les filtres antispam surveillent une liste de mots afin de limiter les messages promotionnels et frauduleux dans les boîtes mails des particuliers. ils peuvent déclencher les filtres et nuire à la délivrabilité.
   Ainsi : Pas de mots empruntés au secteur e-commerce qui serait lus par les filtres anti-spam comme des mails indésirables car non sollicités (gratuit/promotion, caractère monétaire 50CHF€$, de 100%, meilleur prix, pas cher, inscription gratuite, …)

4. ☐ **Rédigez des mailing/Newsletter avec un ratio texte image de 60% de texte.**
   Concrètement, votre lettre d'information ne doit pas être une liste de flyers.

5. ☐ **Optimiser le contenu pour les mobiles :** La plupart des gens consultent leurs e-mails sur des appareils mobiles, alors assurez-vous que vos e-mails sont optimisés pour les petits écrans. Utilisez un design réactif et des images légères pour des temps de chargement rapides.

6. **Inclure une option de désabonnement claire :** Assurez-vous que chaque e-mail contient un lien de désabonnement facile à trouver et à utiliser.
   Respectez les demandes de désabonnement rapidement pour éviter que les abonnés ne signalent vos e-mails comme spam.

7. **Ajouter en fin de mail l'adresse physique** contribue à l'authenticité du message et donc de l'expéditeur. Sa délivrabilité sera meilleure.

8. **Ne pas sur-solliciter vos contacts**
   Un envoi régulier avec cadencement raisonnable est préférable à des envois trop fréquents qui pourraient pousser des destinataires à vous classer comme spam. Surtout si ces mails ne sont pas désirés ou ne faisant pas l'objet initialement d'un consentement. Un envoi excessif peut entraîner des désabonnements et des plaintes de spam.

9. **Surveiller les taux de rebond :** Surveillez de près les taux de rebond de vos e-mails. Les rebonds peuvent être durs (adresses e-mail invalides) ou doux (boîtes de réception pleines). Identifiez et supprimez les adresses e-mail invalides pour maintenir une bonne réputation d'expéditeur.
   Cet indicateur se trouve pour Mailchimp dans le rapport de campagne d'emailing.

10. **Authentifier son domaine de messagerie**
    Ces protocoles d'authentification aident les fournisseurs de messagerie à vérifier l'authenticité des e-mails envoyés depuis votre domaine et contribuent à renforcer la confiance dans vos e-mails.

Focus sur l'authentification du Domaine (DKIM, DMAR etc.)

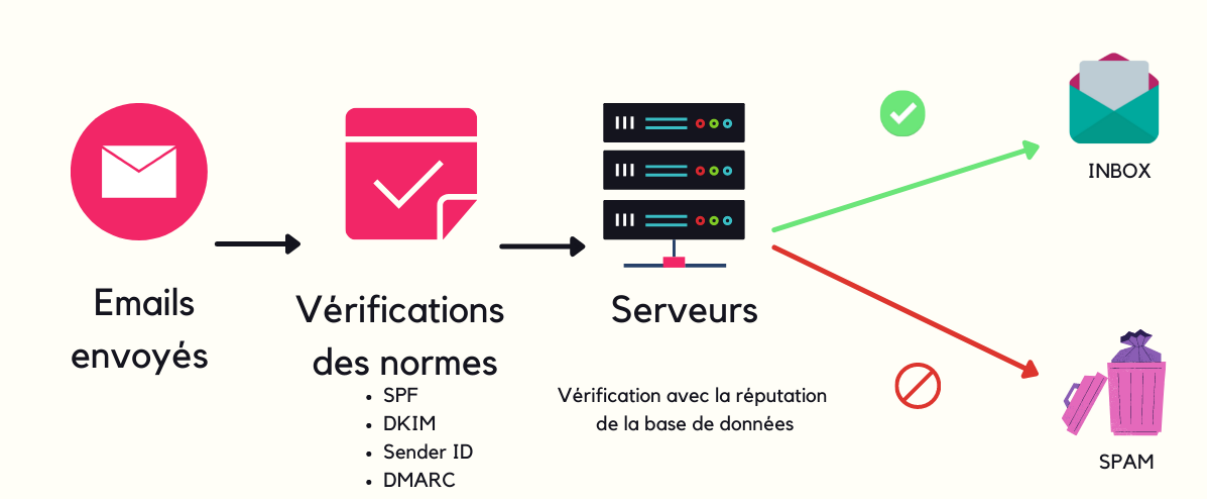
Un point important à ajouter est de vérifier régulièrement les paramètres de configuration de votre outil d'emailing. Mailchimp, Brevo et autres vous informent en amont normalement.

Ces protocoles d'authentification aident les fournisseurs de messagerie à vérifier l'authenticité des e-mails envoyés depuis votre domaine et contribuent à renforcer la confiance dans vos e-mails.
Une configuration correcte de SPF, DKIM et DMARC peut améliorer la délivrabilité des e-mails en réduisant les chances que vos e-mails soient marqués comme spam ou frauduleux.

Pour l'EERV, cela a été fait en janvier 2024 par l'OIC pour tous ceux qui utilisent un MailChimp avec une adresse mon.nom@eerv.ch. Il faut juste aller dans Compte > Profil > Domaine et cliquer sur « *Lancer l'authentification* »

Liens utiles :
Mailchimp
Brevo
Infomaniak

schéma



Rappel - Envois en nombre par mail

L'envoi d'un message à un nombre important de personnes n'est pas une chose anodine. Choisir le bon outil pour la tâche à effectuer.

Dans la période où le recours à la communication digitale apparaît comme primordial, il est important de rappeler que l'usage du courriel, comme tout autre moyen de communication, est soumis à quelques règles et usages, tant sur le plan rédactionnel que technique.

L'utilisation du mail reste un moyen de s'adresser personnellement, que ce soit via internet (Webmail) ou par une application dédiée (Outlook, etc.):
- à une ou plusieurs personnes (un petit groupe)
- mais en aucun cas comme un outil de communication de masse.

Ce genre d'utilisation risque en effet de mettre en péril le système de messagerie (@eerv.ch) en identifiant les usagers de ce domaine comme spameurs.
Alors non seulement, votre adresse sera écartée et votre message ne sera pas délivré mais le risque que l'entier du domaine soit placé sur ce que l'on appelle des « listes noires », est bien réel, créant ainsi de nombreux problèmes pour l'ensemble des utilisateurs.

Si vous souhaitez faire un envoi de masse, il est donc indispensable d'utiliser un outil internet adéquat tel que Mailchimp (https://mailchimp.com/) par exemple ou Brevo ou via un autre plateforme tierce
Mailchimp est le programme utilisé à ce jour par l'OIC-EERV.

Nous vous encourageons donc vivement à choisir le bon outil en fonction du public auquel vous vous adressez.

N'hésitez pas à faire appel à l'OIC ou au support-web@eerv.ch pour obtenir les éléments graphiques identifiant votre lieu d'Eglise dans votre envoi ou pour toute question sur ce sujet.

Les obligations légales dans l'utilisation des mails

Lorsque vous envoyez des e-mails à des utilisateurs dans le cadre d'une campagne de marketing par e-mail, vous êtes soumis à certaines obligations légales, en particulier en ce qui concerne le respect de la vie privée et la protection des données.

En Suisse, les obligations légales pour le marketing par e-mail sont régies principalement par la Loi fédérale sur la protection des données (LPD) et par la Loi contre la concurrence déloyale (LCD).
Voici quelques-unes des principales obligations légales pour un mailing :

Consentement : Vous devez obtenir le consentement préalable des destinataires avant de leur envoyer des e-mails à des fins de marketing. Le consentement doit être libre, spécifique et éclairé. Il est recommandé d'utiliser un opt-in confirmé pour obtenir un consentement explicite.
Il doit également être facile pour les destinataires de retirer leur consentement à tout moment.

Identification de l'expéditeur : Vous devez clairement identifier qui est l'expéditeur de l'e-mail et fournir des informations de contact valides, y compris une adresse postale physique.

Droit de retrait : Vous devez inclure un mécanisme de désabonnement clair et facile à utiliser dans chaque e-mail marketing. Les destinataires doivent pouvoir se désabonner facilement de vos listes d'envoi, et vous devez respecter leurs demandes de désabonnement dans un délai raisonnable.

Protection des données personnelles : Vous devez protéger les données personnelles des destinataires conformément aux lois sur la protection des données en vigueur. Cela signifie que vous devez mettre en place des mesures de sécurité appropriées pour éviter tout accès non autorisé, perte, altération ou divulgation des données personnelles des destinataires.

Respect des lois anti-spam : Vous devez respecter les lois anti-spam applicables dans votre pays et dans les pays où vos destinataires se trouvent. Cela comprend des dispositions telles que l'interdiction de l'envoi d'e-mails non sollicités et l'obligation de respecter les préférences de communication des destinataires.

La défiance des internautes face aux dangers connus et méconnus des mails entrants

Le mail est une porte d'entrée facile pour les tentatives d'extorsion, escroquerie et autres tentatives de fraude.
Outre le classique spam et les virus/malwares, il existe plusieurs autres dangers associés aux courriels pour les destinataires :

- **Pharming** : Le pharming est une technique utilisée par les cybercriminels pour rediriger les utilisateurs vers de faux sites web, souvent conçus pour ressembler à des sites légitimes, afin de voler des informations sensibles telles que des identifiants de connexion, des numéros de carte de crédit, etc. Les courriels peuvent être utilisés comme moyen d'attirer les utilisateurs vers ces faux sites.

- **Hameçonnage (spear phishing)** : Contrairement au phishing classique qui cible un large public, le spear phishing est une forme ciblée de phishing dans laquelle les cybercriminels personnalisent leurs attaques en utilisant des informations spécifiques sur la victime, telles que son nom, son entreprise, son poste, etc. Cela rend ces attaques plus difficiles à détecter et plus susceptibles de réussir.

- *Ingénierie sociale* *dite de l'attaque au président* (source NCSC): Les courriels peuvent également être utilisés dans des attaques d'ingénierie sociale, où les cybercriminels manipulent les destinataires pour obtenir des informations sensibles ou les inciter à prendre des mesures indésirables. Cela peut inclure des techniques telles que l'usurpation d'identité, la manipulation émotionnelle ou la création de scénarios crédibles pour inciter les destinataires à agir de manière impulsif.

- **Fuite d'informations confidentielles** : L'envoi accidentel ou non autorisé d'informations confidentielles par courriel peut compromettre la sécurité et la confidentialité des données.

Liste des Cybermenaces sur le site de l'Office fédéral de la cybersécurité OFCS
https://www.ncsc.admin.ch/ncsc/fr/home.html