Secuenza

Guide de délivrabilité : SPF, DKIM et DMARC

Que vos e-mails arrivent dans la boîte de réception dépend de deux choses : que les fournisseurs puissent vérifier que c'est bien vous, et que votre boîte mail ait une bonne réputation. Ce guide explique les trois enregistrements qui le prouvent, comment les configurer chez les fournisseurs les plus courants et quelles habitudes protègent votre réputation.

Pourquoi c'est important

Gmail, Yahoo et Outlook.com demandent à ceux qui envoient souvent d'avoir **SPF, DKIM et DMARC** sur leur domaine, de permettre de se désinscrire de chaque e-mail en un clic et que presque personne ne le signale comme spam. Sans ces enregistrements, vos e-mails finissent généralement en spam, ou n'arrivent même pas.

Secuenza envoie depuis votre propre boîte mail : c'est donc votre fournisseur de messagerie qui signe (ou non) chaque e-mail. Ce que vous devez faire, c'est publier dans le DNS de votre domaine les données qui le confirment.

Avant de commencer : où est votre DNS

Le DNS de votre domaine se gère là où vous l'avez acheté ou là où vous l'avez fait pointer (le bureau d'enregistrement, votre hébergeur, Cloudflare…), ce qui n'est pas toujours là où se trouve votre messagerie. Connectez-vous à ce panneau et cherchez la zone DNS : c'est là que vous ajoutez les enregistrements de ce guide.

Un changement de DNS met de quelques minutes à quelques heures à être visible. Revenez ensuite dans **Vérifications** dans Secuenza.

SPF : qui peut envoyer pour votre domaine

Le SPF est un enregistrement **TXT** à la racine du domaine qui commence par `v=spf1`, indique quels serveurs peuvent envoyer en son nom et se termine par `~all` (les autres sont suspects) ou `-all` (les autres sont rejetés).

Fournisseur	Ce que votre SPF doit inclure
Microsoft 365	`include:spf.protection.outlook.com`
Google Workspace	`include:_spf.google.com`
IONOS	`include:_spf-eu.ionos.com`
OVHcloud	`include:mx.ovh.com`
Hostinger	`include:_spf.mail.hostinger.com`
Aruba	`include:_spf.aruba.it`
Zoho Mail (UE)	`include:zoho.eu`

Par exemple, avec Microsoft 365 : `v=spf1 include:spf.protection.outlook.com ~all`.

Trois règles à connaître :

- **Il ne peut y avoir qu'un seul SPF.** Si vous en avez déjà un (pour votre site, votre logiciel de facturation), n'en ajoutez pas un autre : regroupez les `include` dans le même enregistrement. Avec deux, aucun ne fonctionne.
- **10 requêtes au maximum.** Chaque `include` compte, ainsi que ceux qu'il contient. Au-delà, les serveurs le considèrent comme cassé.
- **Jamais** `+all` : n'importe qui pourrait envoyer en votre nom.

Si votre boîte mail est une adresse Gmail ou Outlook.com (et non de votre domaine), vous n'avez rien à configurer : le SPF et la signature sont ceux du fournisseur. Ces boîtes ont en revanche des limites basses, que Secuenza respecte.

DKIM : la signature de vos e-mails

Avec DKIM, votre fournisseur signe chaque e-mail avec une clé privée et vous publiez la clé publique dans le DNS, sous un nom comme `selecteur._domainkey.votredomaine.fr`. Le destinataire sait ainsi que l'e-mail n'a pas été modifié en chemin et qu'il vient bien de votre domaine.

- **Microsoft 365 :** dans le portail Microsoft Defender, dans les paramètres d'authentification des e-mails (DKIM), choisissez votre domaine. Il vous donne deux enregistrements **CNAME** (`selector1` et `selector2`) : ajoutez-les à votre DNS et revenez dans le portail pour activer la signature.

- **Google Workspace :** dans la console d'administration, sous Gmail → Authentifier les e-mails, générez un enregistrement de **2048 bits**, ajoutez-le en **TXT** sur `google._domainkey` et cliquez sur « Commencer l'authentification ».
- **IONOS, OVHcloud, Hostinger, Aruba, Zoho et la plupart des hébergeurs :** cherchez « DKIM » dans le panneau de la messagerie. Beaucoup l'activent tout seuls si le DNS est aussi chez eux ; sinon, ils vous donnent l'enregistrement à copier.

Secuenza cherche la signature sous les noms habituels de chaque fournisseur. Si la vôtre porte un autre nom, le **test d'envoi réel** (Pro) la trouve. Utilisez des clés de **2048 bits** : celles de 1024 sont déjà considérées comme faibles.

DMARC : que faire de ce qui échoue

DMARC est un enregistrement **TXT** sur `_dmarc.votredomaine.fr` qui indique aux fournisseurs quoi faire d'un e-mail qui prétend venir de votre domaine mais ne passe ni SPF ni DKIM, et où vous envoyer les rapports. Pour qu'il compte, le domaine de l'expéditeur doit correspondre à celui du SPF ou de la signature DKIM (l'« alignement »).

Commencez par observer :

```
v=DMARC1; p=none; rua=mailto:dmarc@votredomaine.fr
```

1. **Deux à quatre semaines en `p=none`** : rien ne change, mais vous recevez des rapports sur qui envoie pour votre domaine. Vérifiez que tout ce qui est légitime part signé (votre boîte mail, votre site, vos factures).
2. **Passez à `p=quarantine`** : ce qui échoue ira en spam.
3. **Puis à `p=reject`** : ce qui échoue est rejeté. C'est ce qui protège le mieux votre domaine contre ceux qui voudraient se faire passer pour vous.

Les rapports arrivent en XML. Des services gratuits les résument ; il suffit d'y jeter un œil de temps en temps.

Le vérifier avec Secuenza

Dans la fiche de chaque boîte mail, **Vérifications** contrôle SPF, DKIM et DMARC, ainsi que la réception du courrier (MX), le nom inverse du serveur, MTA-STS, BIMI et le chiffrement. Chaque vérification apparaît en vert, orange ou rouge, avec ce qu'il faut configurer et où. Si vous avez déjà un SPF, Secuenza vous propose l'enregistrement complet avec ce qui manque.

Avec **Pro**, en plus :

- **Test d'envoi réel :** Secuenza envoie un vrai e-mail depuis votre boîte mail et vous dit ce que voit le serveur qui le reçoit : signature, SPF, alignement DMARC, chiffrement et vérification anti-spam.
- **Listes noires :** il vérifie si votre serveur ou votre domaine figurent sur les listes qu'utilisent les filtres.

Et la section **Sécurité** réunit ce que le frein a arrêté, vos chiffres sur 30 jours face à leurs limites et l'état de chaque boîte mail : Sécurité de l'envoi l'explique.

La réputation : ce que regardent les filtres

Une fois les enregistrements en place, c'est votre comportement qui compte :

- **Commencez doucement.** Une boîte mail ou un domaine neufs qui envoient soudain des centaines d'e-mails ressemblent à du spam. La montée en charge progressive de Secuenza augmente la limite jour après jour.
- **Respectez les limites.** Pour chaque fournisseur, Secuenza utilise une limite quotidienne et horaire prudente, en dessous de son maximum, et répartit les envois sur vos horaires.
- **Facilitez la désinscription.** Chaque e-mail contient le lien de désinscription et l'en-tête qui permet à Gmail et Outlook d'afficher leur bouton « Se désabonner ». Les désinscriptions s'appliquent tout de suite.
- **Des listes propres.** N'achetez jamais de listes. Les e-mails non distribués et les contacts inactifs sont mis de côté, et le frein de sécurité met une campagne en pause s'il y a trop d'e-mails non distribués ou de désinscriptions, et arrête les envois vers un fournisseur où personne n'ouvre vos e-mails.
- **Peu de plaintes.** Si plus de 2 ou 3 personnes sur mille signalent vos e-mails comme spam, les filtres vous pénalisent. N'écrivez qu'à ceux qui attendent vos e-mails.
- **Des e-mails qui ressemblent à ceux d'une personne.** Un texte clair, peu de liens, pas de raccourcisseurs d'URL, des images entourées de texte. Importez les images depuis l'éditeur : celles de Drive ou de Dropbox, ou collées dans l'e-mail, finissent souvent en spam. La vérification anti-spam vous signale ce qui pèse souvent.
- **Obtenez des réponses.** Une réponse est le meilleur signe que votre e-mail est le bienvenu. Écrivez pour qu'on vous réponde.

Si vos e-mails vont en spam

1. Ouvrez **Vérifications** : les trois enregistrements sont-ils au vert ?
2. Avec Pro, faites le **test d'envoi réel** et regardez ce qui échoue sur le serveur qui reçoit.
3. Revoyez la **vérification anti-spam** des e-mails de la campagne.

4. Regardez dans **Sécurité** si le frein a arrêté un fournisseur, et dans **Résultats**, les désinscriptions et les e-mails non distribués : s'ils augmentent, arrêtez et nettoyez la liste.
5. Baissez la limite quelques jours, puis remontez-la doucement.