Fiche mémo · Leçon 12 · 31 min

Faire arriver vos courriels, domaine, SPF, DKIM, DMARC et désinscription en un clic

Un courriel de prospection arrive s'il est authentifié et s'il ne fait pas fuir ceux qui le reçoivent. Publiez SPF, DKIM et DMARC sur votre domaine, gardez les plaintes sous 0,1 %, envoyez quelques dizaines de messages par jour depuis votre boîte et réservez un sous-domaine authentifié à tout outil de séquence.

Objectifs

- Vérifier les enregistrements SPF, DKIM et DMARC de votre domaine et corriger ce qui manque
- Lire dans l'en-tête d'un message reçu les résultats des trois contrôles et leur alignement
- Préparer un sous-domaine d'envoi et suivre chaque semaine le taux de plainte et les rebonds

À retenir

- Trois contrôles décident de l'arrivée : SPF autorise le serveur, DKIM signe le message, DMARC vérifie que le domaine visible est aligné et dit quoi faire en cas d'échec.
- Un domaine n'a qu'un seul enregistrement SPF ; un outil d'envoi y ajoute son include, un service abandonné en sort.
- DMARC commence à p=none avec une adresse de rapports, et passe à quarantine quand les rapports ne montrent que vos services.
- Quelques dizaines de messages par jour depuis votre boîte ; un outil de séquence envoie depuis un sous-domaine authentifié et préchauffé.
- Le taux de plainte se garde sous 0,1 % ; à faible volume, une seule plainte peut suffire à passer au rouge.

La demande à recopier

Demande à recopier **Faire relire la liste de vos enregistrements DNS**

```
Rôle : tu relis la configuration d'envoi de courriels d'une PME.
Contexte : nous envoyons depuis [Google Workspace ou Microsoft 365] et depuis [outil de
séquence, ou aucun]. Voici les enregistrements TXT et CNAME de notre domaine, copiés depuis
l'interface de notre registraire, sans aucun identifiant de connexion : [collez la liste].
Tâche : dis ce qui manque ou pose problème pour SPF, DKIM et DMARC : enregistrement absent,
deux SPF au lieu d'un, service d'envoi non inclus, include d'un service abandonné, DMARC sans
adresse de rapports.
Format : un tableau (contrôle ; constat ; correction proposée ; documentation à consulter).
Pour toute valeur à publier, renvoie à la documentation de l'éditeur au lieu de l'inventer. Si
la liste ne permet pas de conclure, dis-le.
```

Note : Ne collez jamais un mot de passe de registraire, ni la clé privée DKIM : seule la partie publique va dans le DNS.

Le code à recopier

Les enregistrements d'un domaine qui envoie depuis Google Workspace TEXT

```
; Domaine d'exemple : remplacez exemple.fr par votre domaine.
; SPF : un seul enregistrement TXT à la racine du domaine.
exemple.fr.                 TXT  "v=spf1 include:_spf.google.com ~all"
; Microsoft 365 à la place de Google : "v=spf1 include:spf.protection.outlook.com -all"
; Un outil d'envoi en plus : son include s'ajoute DANS le même enregistrement.

; DKIM : la valeur est générée par la console de la messagerie, à recopier telle quelle.
google._domainkey.exemple.fr. TXT  "v=DKIM1; k=rsa; p=[clé publique copiée de la console]"

; DMARC, premier palier : observer sans bloquer, recevoir les rapports.
_dmarc.exemple.fr.          TXT  "v=DMARC1; p=none; rua=mailto:dmarc@exemple.fr"
; Second palier, après plusieurs semaines de rapports propres :
; "v=DMARC1; p=quarantine; pct=100; rua=mailto:dmarc@exemple.fr"
```

Relevé du 19/11/2026 sur les documentations de Google Workspace et de Microsoft. Une modification du DNS peut demander quelques heures avant d'être visible partout.

Les erreurs fréquentes

L'erreur, et pourquoi elle coûte	La correction
Créer un second enregistrement SPF pour chaque nouvel outil d'envoi. Un domaine ne peut avoir qu'un enregistrement SPF. Avec deux, le contrôle échoue en erreur, y compris pour les messages de la messagerie habituelle.	Ajoutez l'include du nouvel outil dans l'enregistrement existant, retirez celui des services abandonnés, puis vérifiez par un message de test.
Publier DMARC directement à p=reject, « pour être protégé ». Un service oublié qui envoie au nom du domaine (logiciel de devis, formulaire du site, outil de facturation) voit ses messages refusés sans que personne ne comprenne pourquoi.	Commencez à p=none avec une adresse de rapports, identifiez chaque source, corrigez, puis passez à quarantine, et à reject seulement ensuite.

Les trois contrôles d'un message, et ce qui les juge

SPF
Le serveur qui envoie est-il autorisé par le domaine ? Une liste publiée dans le DNS.

DKIM
Le message est-il signé par le domaine, et intact depuis l'envoi ? Une clé publique dans le DNS.

DMARC
Le domaine de l'adresse From est-il aligné sur SPF ou DKIM ? Et que faire sinon : rien, indésirables ou refus.

Réputation
Plaintes, rebonds, désinscriptions honorées, régularité des volumes : ce que les filtres apprennent de vos envois.

De haut en bas : ce que le serveur du destinataire vérifie, dans l'ordre. DMARC ne passe que si SPF ou DKIM passe pour le domaine visible.