

# Protéger sa messagerie : SPF, DKIM, DMARC

Empêcher les fraudeurs d'envoyer des emails en votre nom — et améliorer votre délivrabilité au passage.

10 min de lecture · Niveau Avancé · [cyberionis.fr/ressources/securite-email](https://cyberionis.fr/ressources/securite-email)

Sans configuration adaptée, n'importe qui peut envoyer un email qui semble provenir de votre domaine — vers vos clients, vos fournisseurs, votre banque. Trois mécanismes standards, SPF, DKIM et DMARC, permettent de verrouiller l'usage de votre nom de domaine.

## 1. Les trois piliers

- SPF : liste publique des serveurs autorisés à envoyer des emails pour votre domaine
- DKIM : signature cryptographique qui prouve que le message n'a pas été altéré et vient bien de chez vous
- DMARC : la politique qui dit aux destinataires quoi faire d'un email qui échoue aux contrôles (ne rien faire, mettre en spam, rejeter) et vous envoie des rapports

## 2. Mise en place progressive

Ces réglages se font dans la zone DNS de votre domaine. La démarche prudente : publier SPF, activer DKIM chez votre fournisseur de messagerie, puis déployer DMARC en mode observation ( $p=\text{none}$ ) pour analyser les rapports pendant quelques semaines, avant de durcir vers  $p=\text{quarantine}$  puis  $p=\text{reject}$ .

Attention aux oublis classiques : les outils qui envoient en votre nom (CRM, newsletters, facturation) doivent figurer dans le SPF et signer en DKIM, sinon leurs emails finiront en spam.

## 3. Au-delà des protocoles

- Double authentification sur toutes les boîtes : une messagerie compromise contourne tous ces mécanismes
- Chiffrement TLS activé chez votre fournisseur
- Filtrage anti-spam/anti-phishing en amont des boîtes
- Sensibiliser les équipes : la technique ne bloque pas tout

## 4. Pourquoi c'est devenu incontournable

Longtemps « bonne pratique d'expert », cette configuration est devenue une exigence de fait : Google et Yahoo rejettent ou classent en spam les emails des domaines expéditeurs sans SPF/DKIM alignés, et exigent DMARC pour les envois en volume. Un domaine mal configuré, ce sont vos devis qui arrivent en spam chez vos prospects — et vos clients qui reçoivent de faux emails « de votre part » sans que rien ne les bloque.

## CAS CONCRET

Symptôme classique en PME : « nos emails arrivent en spam chez certains clients depuis quelques semaines ». Diagnostic récurrent : le nouvel outil de facturation envoie les factures « de la part de » l'entreprise, mais n'a jamais été ajouté au SPF ni signé en DKIM. Deux enregistrements DNS plus tard, la délivrabilité revient — et le domaine est verrouillé au passage.

---

## L'essentiel à retenir

- 01 Publier un enregistrement SPF couvrant tous vos outils d'envoi
- 02 Activer DKIM chez votre fournisseur de messagerie et vos outils d'emailing
- 03 Déployer DMARC en mode observation, puis durcir progressivement
- 04 Vérifier la configuration avec un outil de test (ex. mxtoolbox)
- 05 Protéger chaque boîte par la double authentification
- 06 Re-vérifier à chaque nouvel outil qui envoie en votre nom

## Questions fréquentes

### Est-ce compliqué à mettre en place pour une petite entreprise ?

Techniquement, ce sont trois enregistrements DNS — une heure de travail pour qui connaît. La difficulté réelle est l'inventaire : recenser TOUS les services qui envoient des emails en votre nom (messagerie, CRM, facturation, newsletter, site web) pour ne rien casser. C'est une prestation courte et standard pour un prestataire ; le retour sur investissement (délivrabilité + anti-usurpation) est immédiat.

### Peut-on passer DMARC en p=reject directement ?

Déconseillé : sans période d'observation (p=none) avec analyse des rapports, vous risquez de faire rejeter vos propres emails légitimes envoyés par un outil oublié. La trajectoire prudente — none quelques semaines, puis quarantine, puis reject — évite l'auto-sabotage tout en atteignant la protection maximale.

### Nos emails partent parfois en spam malgré SPF/DKIM/DMARC corrects. Pourquoi ?

L'authentification est nécessaire mais pas suffisante : la réputation joue aussi — contenu (mots déclencheurs, pièces jointes), volume soudain, taux de plainte des destinataires, réputation de l'adresse IP d'envoi partagée. Vérifiez d'abord l'authentification avec un outil de test ; si elle est propre, le problème est côté réputation ou contenu.

### À quoi servent les rapports DMARC et qui doit les lire ?

Les serveurs destinataires vous envoient des rapports listant qui a envoyé des emails revendiquant votre domaine, et si ces envois ont passé les contrôles. Bruts, ils sont illisibles (XML) : utilisez un service d'agrégation qui les transforme en tableau de bord. C'est ce qui révèle à la fois vos outils oubliés et les campagnes d'usurpation en cours.

## Pour aller plus loin

MXToolbox — tester SPF, DKIM et DMARC — [mxtoolbox.com/SuperTool.aspx](https://mxtoolbox.com/SuperTool.aspx)

Cybermalveillance.gouv.fr — sécuriser sa messagerie — [www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/messagerie](https://www.cybermalveillance.gouv.fr/tous-nos-contenus/bonnes-pratiques/messagerie)

### Un projet cloud ou d'infrastructure ?

Choix, migration, sécurisation, supervision : Cyberionis conçoit des infrastructures sobres et qui durent.  
contact@cyberionis.fr · 06 64 90 07 74 · cyberionis.fr