



CHECKLIST

Sécuriser vos e-mails : SPF, DKIM & DMARC

10 vérifications pour bloquer l'usurpation de votre domaine et le phishing

Sedona Radar — audit de sécurité externe automatisé

Sedona AI Lecture ~10 min Édition 2026 sedona-ai.com

Votre nom de domaine est une signature : sans protection, n'importe qui peut envoyer des e-mails « de la part de » votre entreprise et piéger vos clients, vos fournisseurs ou vos propres salariés. Trois enregistrements DNS ferment cette porte — SPF, DKIM et DMARC — et conditionnent désormais la délivrabilité de vos envois chez Gmail et Yahoo. Cette checklist vous guide dans le bon ordre de déploiement, avec les pièges qui cassent des envois légitimes, pour passer d'un domaine ouvert à un domaine verrouillé sans coupure.

À retenir

- SPF, DKIM et DMARC ne se remplacent pas : ils se complètent. Seul DMARC protège l'adresse « De : » réellement affichée à vos destinataires.
- Ordre imposé : SPF → DKIM → DMARC en p=none (observation) → durcissement progressif vers quarantaine puis reject.
- Depuis février 2024, Gmail et Yahoo exigent SPF + DKIM + DMARC alignés pour tout expéditeur de masse (>5 000 messages/jour).
- Le piège n°1 : passer en p=reject sans avoir lu les rapports agrégés → vous bloquez vos propres factures, newsletters et notifications.
- Le piège n°2 : dépasser 10 résolutions DNS dans votre SPF (fréquent avec plusieurs SaaS) → l'enregistrement devient invalide.
- Un audit de surface (ou un scan Sedona Radar) vérifie ces trois enregistrements depuis l'extérieur, comme le fait un attaquant.

01 Pourquoi c'est vital (et urgent)

L'e-mail reste le premier vecteur d'attaque. L'usurpation de domaine alimente l'hameçonnage et la fraude au virement (BEC, « arnaque au président ») : un e-mail qui semble venir de votre PDG ou de votre comptable, alors que rien dans votre domaine ne l'a authentifié. Sans DMARC en mode strict, votre marque peut être imitée à l'identique.

1re menace

L'hameçonnage reste la première cybermenace en France en 2025, avec plus de 500 000 victimes accompagnées ; le piratage de compte devient la menace n°1 des professionnels (+45 %).

Cybermalveillance.gouv.fr, Rapport d'activité et état de la menace 2025

55,5 Md\$

Pertes mondiales déclarées liées à la fraude au virement par compromission d'e-mail (BEC), cumulées sur 305 033 incidents (2013–2023).

FBI IC3, Business Email Compromise: The \$55 Billion Scam (11/09/2024)

42 %

Seuls 42 % des domaines dotés d'un enregistrement DMARC sont réellement en mode d'application (quarantine/reject) ; 78 % ont un enregistrement mais la majorité laisse la porte entrouverte.

Valimail, 2026 State of DMARC Report

Ce n'est plus optionnel pour vos envois

Depuis février 2024, Gmail et Yahoo imposent à tout expéditeur de masse (plus de 5 000 messages par jour vers leurs boîtes) une authentification SPF + DKIM avec alignement DMARC, un taux de spam maintenu sous 0,30 %, et un désabonnement en un clic. Sans cela, vos e-mails sont rejetés ou classés indésirables.

02 Les 3 protocoles en 2 minutes

Protocole	Ce qu'il fait	Où il vit (DNS)
SPF (RFC 7208)	Liste les serveurs autorisés à envoyer pour votre domaine (enveloppe « MAIL FROM »).	Enregistrement TXT à l'apex du domaine
DKIM (RFC 6376)	Signe cryptographiquement chaque message ; le destinataire vérifie l'intégrité et l'origine.	TXT sur <sélecteur>._domainkey.votredomaine
DMARC (RFC 7489)	Aligne l'adresse « De : » visible sur SPF/DKIM, dicte quoi faire en cas d'échec, et renvoie des rapports.	TXT sur _dmarc.votredomaine

Le point clé souvent ignoré

SPF et DKIM valident des identifiants « techniques » invisibles de l'utilisateur. Seul DMARC vérifie que le domaine réellement affiché dans « De : » est bien le vôtre. C'est donc DMARC qui protège votre marque aux yeux de vos destinataires.

03 SPF — autoriser les bons émetteurs

- ☐ Un seul enregistrement SPF (TXT) existe pour le domaine — jamais deux, sinon SPF est invalide.
- ☐ Tous les services légitimes qui envoient en votre nom y figurent : messagerie (Microsoft 365 / Google Workspace), CRM, ERP, outil de facturation, plateforme d'e-mailing.
- ☐ L'enregistrement se termine par -all (rejet strict) une fois la liste stabilisée — ~all (softfail) est toléré en phase de transition.

- ☐ Le nombre total de résolutions DNS reste inférieur ou égal à 10 (compter chaque include:). Au-delà, SPF renvoie une erreur et n'est plus évalué.
- ☐ Les domaines qui n'envoient jamais d'e-mail (domaines parkés) publient un SPF « vide » : v=spf1 -all.

04 DKIM — signer chaque message

- ☐ La signature DKIM est activée sur votre plateforme d'envoi principale (Microsoft 365, Google Workspace...) et sur chaque outil tiers qui envoie en votre nom.
- ☐ La clé publique est publiée en DNS (TXT) sur le bon sélecteur ; la clé fait au minimum 1024 bits (2048 recommandé).
- ☐ Un e-mail de test reçu affiche « DKIM=pass » dans l'en-tête, avec un domaine de signature (d=) aligné sur votre domaine.
- ☐ Les sélecteurs et clés sont documentés et font l'objet d'une rotation périodique.
- ☐ Chaque nouveau service d'envoi passe par une activation DKIM avant sa mise en production.

05 DMARC — durcir sans rien casser

1 Publier p=none avec des rapports

Créez _dmarc.votredomaine avec p=none et une adresse rua= pour recevoir les rapports agrégés (RUA). Aucun impact sur la délivrabilité : vous observez seulement.

2 Cartographier vos émetteurs

Pendant 2 à 4 semaines, lisez les rapports RUA pour identifier TOUS les services qui envoient légitimement en votre nom et corriger leur SPF/DKIM.

3 Monter en quarantaine

Passez en p=quarantine (éventuellement avec pct= pour un déploiement progressif) : les messages non authentifiés partent en indésirables plutôt qu'en boîte de réception.

4 Verrouiller en reject

Une fois zéro faux positif constaté, passez en p=reject : toute usurpation de votre domaine est purement et simplement bloquée.

- ☐ Un enregistrement DMARC existe sur _dmarc et sur les sous-domaines émetteurs.
- ☐ Une adresse rua= collecte les rapports agrégés (idéalement via un outil de lecture DMARC).
- ☐ La politique cible est p=reject — l'objectif final, pas p=none laissé en place indéfiniment.

06 Les pièges qui coûtent cher

Ne passez jamais en reject « à l'aveugle »

Le durcissement DMARC sans lecture préalable des rapports est la première cause d'incident : factures, notifications, newsletters et e-mails transactionnels légitimes se retrouvent bloqués.

Toujours observer (p=none) avant de durcir.

Surveillez la limite des 10 lookups SPF

Chaque include: de SaaS consomme des résolutions DNS. Au-delà de 10, SPF devient invalide (permerror) et n'authentifie plus personne. Consolidez, ou utilisez une technique d'aplatissement (flattening) suivie régulièrement.

Autres écueils fréquents : un SPF trop permissif (+all), une clé DKIM trop courte ou jamais renouvelée, et l'oubli des sous-domaines (un attaquant usurpera factures.votredomaine si _dmarc n'y est pas déclaré).

07 Aller plus loin

- MTA-STS (RFC 8461) : force le chiffrement TLS entre serveurs de messagerie, contre l'interception.
- TLS-RPT (RFC 8460) : reçoit des rapports sur les échecs de connexion chiffrée.
- BIML : affiche votre logo de marque dans la boîte de réception — nécessite un DMARC en mode d'application (quarantine/reject) et souvent un certificat de marque (VMC).
- Respectez les exigences Google/Yahoo de bout en bout : PTR (reverse DNS) valide, en-têtes de désabonnement en un clic, format des messages conforme.

Vérifiez comme un attaquant

Un attaquant lit vos enregistrements DNS en quelques secondes pour savoir si votre domaine est usurpable. Faites-le avant lui : un scan de surface révèle immédiatement un SPF laxiste, un DKIM absent ou un DMARC resté en p=none.

§ Sources

1. Cybermalveillance.gouv.fr — Rapport d'activité et état de la menace 2025 — <https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/rapport-activite-2025>
2. FBI IC3 — Business Email Compromise: The \$55 Billion Scam (PSA, 2024) — <https://www.ic3.gov/PSA/2024/PSA240911>
3. Valimail — 2026 State of DMARC Report — <https://www.valimail.com/newsroom/valimail-2026-dmarc-report/>
4. Google — Email sender guidelines (exigences expéditeurs) — <https://support.google.com/mail/answer/81126>
5. RFC 7208 — Sender Policy Framework (SPF) — <https://www.rfc-editor.org/rfc/rfc7208>

6. RFC 6376 — DomainKeys Identified Mail (DKIM) — <https://www.rfc-editor.org/rfc/rfc6376>
7. RFC 7489 — Domain-based Message Authentication (DMARC) — <https://www.rfc-editor.org/rfc/rfc7489>
8. ANSSI — Recommandations pour la mise en œuvre d'un service DNS (ANSSI-PA-105) — <https://cyber.gouv.fr/publications>

Votre domaine est-il usurpable ?

Sedona Radar analyse ce que votre domaine expose sur Internet, dont ses enregistrements DNS de messagerie (SPF, DKIM, DMARC), comme le ferait un attaquant. Lancez un scan gratuit (environ 45 minutes, médiane mesurée) : vous verrez la note de votre DNS ; le détail SPF, DKIM et DMARC est inclus dès le plan Starter.

Lancer mon scan gratuit

sedona-ai.com/scan-gratuit