Stratégie, Sécurité

Emails professionnels SPF, DKIM, DMARC : pourquoi vos mails arrivent en spam

Un email professionnel peut être légitime et pourtant finir en spam si le domaine n'est pas correctement authentifié. SPF, DKIM et DMARC aident les serveurs de réception à vérifier qui a le droit d'envoyer au nom de votre domaine. Repères pratiques pour PME, formulaires WordPress, WooCommerce, newsletters et outils tiers.

Publié le 20 mai 2026

Ce qu'il faut retenir de ce dossier

Un email professionnel peut arriver en spam pour plusieurs raisons : domaine mal authentifié, serveur non autorisé, signature DKIM absente, politique DMARC inexistante, mauvaise réputation d'adresse IP, contenu trop promotionnel, pièce jointe suspecte ou formulaire WordPress configuré avec une adresse d'expéditeur incohérente.

SPF, DKIM et DMARC ne garantissent pas à eux seuls l'arrivée en boîte de réception. Ils constituent toutefois le socle minimal d'authentification. Google indique depuis 2024 que les expéditeurs qui envoient vers des comptes Gmail doivent respecter des exigences d'authentification, et recommande de configurer SPF, DKIM et DMARC pour les domaines d'envoi.

Pour une PME, le point clé n'est pas d'ajouter une ligne DNS au hasard. Il faut d'abord cartographier tous les outils qui envoient au nom du domaine : messagerie professionnelle, site WordPress, formulaires, WooCommerce, newsletter, CRM, facturation, outil de support ou plateforme marketing. Un seul outil oublié peut suffire à provoquer des échecs d'authentification.

DMARC doit aussi être déployé avec méthode. On commence généralement par observer avec une politique p=none, puis on corrige les flux légitimes avant de passer éventuellement à quarantine ou reject. Une politique trop stricte appliquée trop tôt peut bloquer de vrais emails.

Vos emails arrivent en spam, ou votre domaine peut être usurpé

Le symptôme est souvent simple : un client dit ne pas avoir reçu le devis, une notification WooCommerce tombe dans les indésirables, un formulaire WordPress n'aboutit plus, une campagne emailing est bloquée, ou un correspondant reçoit un message suspect qui semble venir de votre entreprise.

Ces problèmes ne viennent pas toujours du contenu de l'email. Les serveurs de réception vérifient aussi si le domaine est cohérent avec le serveur qui envoie le message. Autrement dit, ils cherchent à savoir si l'email a bien le droit de se présenter comme venant de @votre-entreprise.fr.

Le risque n'est pas seulement commercial

Un défaut d'authentification peut dégrader la délivrabilité de vos vrais emails, mais aussi faciliter l'usurpation de votre domaine dans des tentatives de phishing ou de fraude. Cybermalveillance.gouv.fr rappelle que l'hameçonnage consiste à tromper la victime en se faisant passer pour un tiers de confiance afin de voler des informations personnelles, professionnelles ou bancaires.

Trois signaux d'alerte

- Des clients disent ne pas recevoir vos devis, factures ou confirmations.
- Les emails du site WordPress ou de WooCommerce arrivent en spam.
- Vous découvrez qu'un outil tiers envoie depuis votre domaine sans avoir été configuré dans le DNS.

Cartographier tous les expéditeurs avant de corriger le DNS

La plupart des erreurs viennent d'une vision trop simple : “notre messagerie fonctionne, donc notre domaine est configuré”. En réalité, une entreprise utilise souvent plusieurs canaux d'envoi qui ne passent pas tous par le même serveur.

Avant de modifier SPF, DKIM ou DMARC, il faut donc lister tous les expéditeurs légitimes.

Flux d'envoi	Exemples	Erreur fréquente	Conséquence possible
Collaborateurs	Microsoft 365, Google Workspace, serveur mail de l'hébergeur	Le domaine est configuré uniquement pour la messagerie principale	Les emails salariés passent, mais pas ceux du site ou des outils tiers.
Site web	WordPress, formulaires, WooCommerce, espace client	Le site envoie via le serveur web sans SMTP authentifié	Formulaires, commandes ou notifications peuvent arriver en spam.
Outils tiers	Newsletter, CRM, facturation, support, marketing automation	L'outil n'est pas autorisé dans SPF ou ne signe pas en DKIM	Les emails sortants de l'outil échouent aux contrôles d'authentification.
Sous-domaines	news.exemple.fr, mail.exemple.fr, support.exemple.fr	Le sous-domaine n'a pas sa propre configuration d'envoi	Les campagnes ou emails transactionnels sont mal identifiés.

Visuel de contenu à créer : image-emails-professionnels-cartographie-expediteurs.webp

Schéma recommandé : un domaine d'entreprise au centre, relié à trois familles d'expéditeurs, messagerie, site web, outils tiers, puis aux trois contrôles SPF / DKIM / DMARC.

SPF, DKIM, DMARC : trois rôles différents

SPF, DKIM et DMARC sont complémentaires. Ils ne mesurent pas la qualité commerciale d'un email : ils aident les serveurs de réception à vérifier l'identité technique de l'expéditeur.

?SPF : la liste des serveurs autorisés

SPF publie dans le DNS la liste des serveurs autorisés à envoyer pour le domaine. Google rappelle que l'enregistrement SPF doit inclure tous les expéditeurs d'emails du domaine.

?DKIM : la signature du message

DKIM ajoute une signature cryptographique vérifiable par le serveur de réception. L'IETF définit DKIM dans la RFC 6376.

?DMARC : la règle de décision

DMARC s'appuie sur SPF et DKIM, vérifie l'alignement avec le domaine visible dans l'en-tête “De”, puis indique quoi faire en cas d'échec.

Analogie :

SPF indique quels livreurs ont le droit de livrer au nom de l'entreprise. DKIM ajoute un sceau sur le courrier. DMARC dit au gardien ce qu'il doit faire si le livreur ou le sceau ne correspond pas à l'identité annoncée.

SPF : attention à la liste incomplète

SPF est souvent la première brique configurée, mais aussi l'une des plus mal comprises. Si un outil tiers n'est pas inclus dans l'enregistrement SPF, ses emails sont plus susceptibles d'être marqués comme spam. Google le précise explicitement dans ses consignes SPF.

DKIM : chaque outil important doit signer

DKIM doit être activé pour le domaine qui envoie les emails. Pour Google, la signature DKIM est utilisée par les serveurs de réception pour vérifier que le message a bien été envoyé par le propriétaire du domaine. En pratique, chaque service important, messagerie, newsletter, CRM, outil transactionnel, peut nécessiter sa propre clé DKIM.

DMARC : observer avant de bloquer

DMARC permet de publier une politique : none pour observer, quarantine pour demander le placement en spam, reject pour demander le rejet. Pour un domaine déjà utilisé par plusieurs outils, le déploiement doit être progressif afin de ne pas bloquer des flux légitimes.

Point de prudence

Un domaine peut “passer SPF” ou “passer DKIM” sans réussir DMARC si le domaine authentifié n'est pas aligné avec le domaine visible dans l'adresse “De”. C'est pour cette raison que DMARC doit être testé avec des emails réels.

L'usurpation de domaine : quand quelqu'un écrit en votre nom

La délivrabilité n'est qu'une partie du sujet. L'autre enjeu est la protection de l'identité de votre entreprise. Sans politique d'authentification suffisamment maîtrisée, un attaquant peut tenter d'envoyer des messages qui semblent provenir de votre domaine ou d'un nom proche.

Ces messages peuvent servir à imiter une demande de paiement, relancer une facture frauduleuse, envoyer un lien de phishing, demander un changement de RIB ou piéger un collaborateur. Le destinataire voit une adresse ou un nom d'expéditeur familier, mais l'email ne vient pas réellement de l'entreprise.

Pourquoi DMARC compte pour la réputation

DMARC aide le propriétaire du domaine à surveiller les usages de son domaine et à indiquer aux serveurs de réception quoi faire lorsque des messages échouent aux contrôles. Google recommande aussi les rapports DMARC pour identifier les expéditeurs susceptibles d'usurper l'identité d'un domaine.

WordPress, WooCommerce, CRM, newsletters : les cas où tout se complique

Un domaine peut être correctement configuré pour la messagerie des collaborateurs, mais mal configuré pour les emails envoyés par le site web ou un outil tiers. C'est l'un des cas les plus fréquents.

?Formulaires WordPress

Un formulaire ne devrait pas envoyer “depuis” l'adresse du visiteur. Il vaut mieux envoyer depuis une adresse du domaine, par exemple site@votre-domaine.fr, et placer l'adresse du visiteur en Reply-To.

?WooCommerce

Confirmations de commande, réinitialisations de mot de passe et notifications administrateur doivent être fiables. Un SMTP authentifié ou un service transactionnel est souvent préférable à l'envoi brut par le serveur web.

?Newsletters

Les plateformes d'emailing doivent être autorisées et signer les emails. Pour les campagnes, un sous-domaine dédié peut faciliter le pilotage de la réputation.

?CRM, facturation, support

Ces outils sont souvent oubliés lors de la configuration DNS. Pourtant, ils envoient des messages critiques : devis, factures, tickets, relances, confirmations.

Repère pratique

Un bon audit ne commence pas par copier une ligne SPF trouvée dans une documentation. Il commence par un inventaire : “qui envoie quoi, avec quelle adresse, depuis quel service, vers quels destinataires ?”.

Les erreurs DNS qui font échouer l'authentification

Les erreurs d'authentification email sont souvent invisibles pour le dirigeant. Le site semble fonctionner, l'outil indique que le message a été envoyé, mais le serveur de réception refuse, met en spam ou dégrade la réputation du domaine.

Erreur fréquente	Conséquence concrète	Correction à prévoir
Plusieurs enregistrements SPF sur le même domaine	SPF peut échouer complètement, car un domaine ne doit pas publier plusieurs politiques SPF concurrentes.	Fusionner les autorisations dans un seul enregistrement SPF cohérent.
Outil tiers absent du SPF	Les emails de newsletter, CRM ou facturation sont plus susceptibles d'être marqués comme spam.	Ajouter l'outil légitime dans SPF, selon sa documentation officielle.

DKIM non activé pour un service important	Le message n'est pas signé par le domaine, ce qui réduit la confiance technique.	Activer DKIM dans chaque service d'envoi et publier la clé DNS fournie.
DMARC en p=none jamais analysé	Le domaine observe les échecs, mais personne ne corrige les sources non conformes.	Lire les rapports DMARC, corriger les flux légitimes, puis renforcer progressivement la politique.
SPF trop permissif	Le domaine autorise trop largement l'envoi, ce qui affaiblit la protection.	Limiter les expéditeurs aux services réellement utilisés.
Redirections email non maîtrisées	SPF peut échouer lors du transfert, selon le chemin emprunté par le message.	S'appuyer davantage sur DKIM et vérifier les pratiques du service de transfert.
Sous-domaines oubliés	Une campagne envoyée depuis news.domaine.fr peut échouer même si domaine.fr est correctement configuré.	Configurer SPF, DKIM et DMARC pour les sous-domaines d'envoi.
Serveur web utilisé comme expéditeur sans SMTP	Les emails WordPress peuvent être mal authentifiés ou associés à une IP partagée de mauvaise réputation.	Utiliser un SMTP authentifié ou un service transactionnel adapté.

Visuel de contenu à créer : image-emails-professionnels-erreurs-dns.webp

Infographie recommandée : tableau visuel “Erreur DNS -> Effet sur l'email -> Action correctrice”, avec pictogrammes SPF, DKIM et DMARC.

Vérifier votre configuration en quelques minutes

Certains outils gratuits permettent de faire un premier diagnostic. Ils ne remplacent pas une analyse complète, mais ils aident à identifier rapidement les erreurs les plus visibles.

?MXToolbox

Permet de consulter les enregistrements MX, SPF, DKIM, DMARC et certaines listes de blocage. Utile pour un premier contrôle DNS.

?mail-tester.com

Permet d'envoyer un message réel vers une adresse de test et d'obtenir un rapport sur l'authentification, le contenu et certaines alertes.

?Google Postmaster Tools

Utile pour les domaines qui envoient des volumes significatifs vers Gmail. Google y affiche notamment des informations de réputation et de taux de spam.

?Rapports DMARC

Les rapports agrégés DMARC permettent d'identifier les sources qui envoient au nom du domaine et celles qui échouent aux contrôles.

Attention aux diagnostics partiels

Un test réussi depuis un outil ne signifie pas que tous les flux sont corrects. Il faut tester la messagerie, le site WordPress, WooCommerce, les newsletters, le CRM et les outils de facturation séparément.

Les questions à poser avant de modifier votre DNS

Question | Si la réponse est non
Savez-vous quels outils envoient des emails au nom du domaine ? | Vous ne pouvez pas sécuriser correctement la délivrabilité ni détecter les expéditeurs oubliés.
SPF contient-il tous les expéditeurs légitimes ? | Certains emails peuvent échouer ou être marqués comme spam.
DKIM est-il activé pour chaque outil important ? | Les messages ne sont pas correctement signés, ce qui réduit la confiance technique.
DMARC est-il publié et suivi ? | L'usurpation du domaine reste mal contrôlée et vous manquez de visibilité sur les sources d'envoi.
Le site WordPress utilise-t-il un SMTP authentifié ? | Les emails de formulaires ou notifications peuvent dépendre d'un serveur web peu fiable pour l'envoi.
WooCommerce est-il testé régulièrement ? | Des confirmations de commande, réinitialisations ou notifications administrateur peuvent être perdues.
Les outils marketing utilisent-ils un domaine ou sous-domaine dédié ? | La réputation des campagnes peut interférer avec la messagerie principale de l'entreprise.
Un responsable lit-il les rapports DMARC ? | Vous observez peut-être des anomalies sans jamais les corriger.

Ce que les lecteurs demandent souvent

SPF suffit-il pour éviter le spam ?

DMARC peut-il bloquer de vrais emails ?

Faut-il passer directement à p=reject ?

Pourquoi mes emails arrivent chez certains clients mais pas chez d'autres ?

WordPress doit-il envoyer les emails depuis le serveur web ?

Faut-il utiliser un sous-domaine pour les newsletters ?

Un email authentifié arrive-t-il toujours en boîte de réception ?

Conclusion

Les problèmes d'emails professionnels ne se résolvent pas en ajoutant mécaniquement SPF, DKIM ou DMARC. La priorité est de comprendre qui envoie réellement au nom du domaine : collaborateurs, site web, WooCommerce, newsletters, CRM, facturation, support et outils tiers.

Une fois cette cartographie réalisée, SPF, DKIM et DMARC deviennent des outils très puissants pour restaurer la confiance technique, limiter les emails en spam, mieux surveiller les usages du domaine et réduire les risques d'usurpation.

Pour une PME, le bon objectif est progressif : authentifier les flux légitimes, corriger les erreurs DNS, tester les emails réels, lire les rapports DMARC, puis renforcer la politique lorsque le domaine est maîtrisé.

Sources

- Google, Consignes pour les expéditeurs de messages : exigences Gmail depuis 2024, SPF/DKIM/DMARC, taux de spam, TLS, Postmaster Tools, désabonnement en un clic pour les gros expéditeurs.
- Google Workspace, Configurer SPF : principe de l'enregistrement SPF et inclusion des expéditeurs autorisés.
- RFC 7208, Sender Policy Framework (SPF) : spécification technique du mécanisme SPF.
- RFC 6376, DomainKeys Identified Mail (DKIM) Signatures : spécification technique DKIM.
- RFC 7489, Domain-based Message Authentication, Reporting, and Conformance (DMARC) : politique DMARC, alignement et rapports.
- Cybermalveillance.gouv.fr, Que faire en cas de phishing ou hameçonnage ? : définition, risques et bons réflexes face à l'usurpation et aux emails frauduleux.