

Empêchez l'usurpation de vos courriels

Cinq enregistrements DNS déterminent si quelqu'un peut envoyer un courriel convaincant en votre nom. Leur rôle, leur forme et les erreurs les plus fréquentes.

01

SPF

Quels serveurs peuvent envoyer en votre nom?

Gratuit

02

DKIM

Le message est-il signé et intact?

Gratuit

03

DMARC

Que se passe-t-il si ces vérifications échouent?

Gratuit

04

MTA-STS

Vos courriels entrants sont-ils chiffrés en transit?

Gratuit + HTTPS

05

BIMI

Les boîtes de réception peuvent-elles afficher votre logo?

≈ 750-1 500 \$ US/an

LES ENREGISTREMENTS

01 SPF

TXT à
example.com

```
v=spf1 include:spf.protection.outlook.com include:servers.mcsv.net -all
```

- Un seul enregistrement SPF par domaine. Deux enregistrements les invalident tous les deux.
- Dix recherches DNS au maximum, et chaque include: compte. Terminez par -all ou ~all, jamais +all.

02 DKIM

TXT ou CNAME à
selector._domainkey.
example.com

```
si._domainkey.example.com TXT "v=DKIM1; k=rsa; p=MIIBIjANBgkqhkiG9w0BAQEFAAOOC..."
```

- Activez-le pour chaque service qui envoie en votre nom : CRM, infolettre, facturation, gestion des demandes, pas seulement votre messagerie.
- Utilisez des clés de 2048 bits et publiez l'enregistrement exactement tel que le fournisseur le donne.

03 DMARC

TXT à
_dmarc.example.com

```
v=DMARC1; p=none; rua=mailto:dmarc@example.com ← départ : surveiller
v=DMARC1; p=reject; rua=mailto:dmarc@example.com ← objectif : bloquer
```

- p=none ne fait qu'observer. L'alignement compte : le domaine qui réussit SPF ou DKIM doit correspondre au domaine de l'expéditeur (From).
- Google et Yahoo (févr. 2024) ainsi que Microsoft Outlook.com (mai 2025) exigent DMARC des expéditeurs de plus de 5 000 messages par jour.

04 MTA-STS

TXT à
_mta-sts.example.com
politique à
https://mta-sts.
example.com/.well-
known/mta-sts.txt

```
_mta-sts.example.com TXT "v=STSV1; id=20261013"
mta-sts.txt: version: STSV1 · mode: enforce · max_age: 604800
mx: *.mail.protection.outlook.com
_smtptls.example.com TXT "v=TLSRPTv1; rua=mailto:tlsrpt@example.com"
```

- Commencez en mode: testing et lisez les rapports TLS avant d'appliquer la politique.
- Changez l'id à chaque modification de la politique, et gardez les lignes mx à jour avec vos enregistrements MX.

05 BIMI

TXT à
default._bimi.
example.com

```
v=BIMI1; l=https://example.com/logo.svg; a=https://example.com/vmc.pem
```

- Exige DMARC à p=quarantine ou p=reject, et un logo au format SVG Tiny PS.
- Gmail et Apple Mail exigent un certificat de marque : un VMC (marque déposée, ajoute le crochet bleu de Gmail) ou, pour Gmail, un CMC (logo utilisé depuis 12 mois ou plus).

DÉPLOYER DMARC SANS BLOQUER VOS COURRIELS

1

Listez vos expéditeurs

Messagerie, CRM, infolettre, facturation, formulaires Web, numériseurs

2

SPF + DKIM

Publiez SPF, activez DKIM pour chaque expéditeur

3

Surveillez

DMARC à **p=none**, lisez les rapports quelques semaines

4

Corrigez

Jusqu'à ce que le courriel légitime passe l'alignement

5

Appliquez

Quarantaine, puis rejet. Progressez avec **pct=25** au besoin

p=none

Surveillance seulement. Le courriel usurpé arrive quand même.

p=quarantine

Le courriel en échec va aux indésirables.

p=reject

Le courriel en échec est refusé. L'objectif.

Domaines qui n'envoient pas de courriel

SPF	<code>v=spf1 -all</code>
DMARC	<code>v=DMARC1; p=reject</code>
MX	<code>0 .</code> (MX nul, n'accepte aucun courriel)

Où activer DKIM (menus en anglais)

Microsoft 365	Defender portal > Email & collaboration > Policies & rules > Threat policies > Email authentication settings > DKIM
Google Workspace	Admin console > Apps > Google Workspace > Gmail > Authenticate email

Vérifiez vos enregistrements

SPF	<code>dig +short TXT example.com</code>
DMARC	<code>dig +short TXT _dmarc.example.com</code>
DKIM	<code>dig +short TXT s1._domainkey.example.com</code>
MTA-STS	<code>dig +short TXT _mta-sts.example.com</code>
BIMI	<code>dig +short TXT default._bimi.example.com</code>
Windows	<code>nslookup -type=TXT _dmarc.example.com</code>

VOTRE LISTE DE VÉRIFICATION

- ☐ Un seul enregistrement SPF, sous 10 recherches
- ☐ DKIM activé pour chaque service qui envoie en votre nom
- ☐ Rapports DMARC envoyés à une boîte que quelqu'un lit
- ☐ DMARC à **p=reject**, ou un plan daté pour y arriver
- ☐ Sous-domaines couverts (**sp=reject** une fois à **reject**)
- ☐ MTA-STS en mode enforce, avec rapports TLS
- ☐ Domaines inactifs verrouillés
- ☐ Un responsable quand un nouveau service d'envoi est ajouté

LES ENREGISTREMENTS BLOQUENT L'USURPATION, PAS TOUTES LES FRAUDES

- Confirmez tout changement de coordonnées bancaires en appelant un numéro que vous avez déjà, jamais celui du courriel.
- Voyez l'urgence et la confidentialité comme des signaux d'alerte, surtout de la part de la direction ou de fournisseurs.
- Vérifiez l'adresse réelle de l'expéditeur, pas le nom affiché. Les domaines semblables réussissent toutes les vérifications ci-dessus.
- Signalez les messages suspects aux TI au lieu de simplement les supprimer.

OUTIL UTILISÉ **Surveillance DMARC continue.** Les rapports sont difficiles à lire à la main. Nous utilisons **Mailsec** (mailsec.ca), une plateforme canadienne de DMARC et de sécurité des domaines, pour suivre les rapports et repérer les nouveaux expéditeurs.

Divulgateur : Mailsec est un client de Privateer Cybersecurity et peut nous verser une commission de recommandation.

Vous voulez qu'on le configure pour vous, ou un deuxième regard sur vos enregistrements?

Une aide d'expérience, en français ou en anglais. Réponse en 1 à 2 jours ouvrables.



privateer.ca · info@privateer.ca