



Guide complet

Configuration efficace des courriers indésirables dans Mozilla Thunderbird

et compréhension des mécanismes de réception du spam

(Valable sous Windows, macOS et Linux – comptes IMAP et POP)



Objectifs de la configuration

- Les courriers indésirables ne doivent pas apparaître dans la boîte de réception
 - Ils doivent être déplacés automatiquement vers le dossier **Indésirables**
 - Ils doivent être supprimés automatiquement après un délai défini
 - Il doit rester possible de récupérer un message légitime classé par erreur
 - En configuration **IMAP**, les actions doivent être synchronisées avec le serveur
 - Comprendre **pourquoi une adresse peut recevoir du spam sans avoir été utilisée activement**
-

1 Comprendre l'origine des courriers indésirables

Il est fréquent de recevoir des courriers indésirables même avec une adresse qui n'a été utilisée que très peu, voire jamais, sur des sites Internet. Cela s'explique par plusieurs mécanismes automatisés.

1.1 Collecte d'adresses par des robots automatisés

Les spammeurs utilisent des **robots logiciels** (scripts automatisés) capables de :

- Générer des millions d'adresses possibles à partir d'un nom de domaine (ex. *prenom.nom@domaine.com*, *initiale.nom@domaine.com*, etc.)
- Tester ces adresses par envoi massif de messages
- Déterminer quelles adresses existent réellement

Une adresse est considérée comme **valide** si :

- le message n'est pas rejeté par le serveur
 - ou si une interaction humaine est détectée (ouverture, clic, réponse)
-

1.2 Confirmation d'activité d'une adresse

Une adresse devient plus attractive pour les spammeurs lorsqu'elle est identifiée comme **active**, par exemple lorsque :

- des messages légitimes sont délivrés correctement
- des liens sont cliqués (y compris « se désinscrire » sur des mails frauduleux)
- l'adresse figure dans des bases de données issues de recoupements

Il ne s'agit pas nécessairement d'une fuite du service utilisé, mais souvent d'un **effet de corrélation**.

1.3 Bases de données utilisées par les spammeurs

Les robots et plateformes de spam s'appuient sur :

- des bases d'adresses générées automatiquement
- des listes issues d'anciennes fuites de données
- des bases enrichies par tests successifs (rebonds, délivrabilité, activité)
- des classifications probabilistes
(*par exemple : "adresse associée à un service financier"*)

Ces bases sont ensuite revendues ou partagées entre réseaux de spam.

1.4 Rôle des signalements et filtres globaux

À l'inverse, les fournisseurs de messagerie (et Thunderbird) utilisent :

- les signalements d'utilisateurs
- l'analyse des en-têtes techniques
- le contenu des messages
- des bases de signatures de spam mutualisées

Ce fonctionnement collectif permet, avec le temps, de **réduire fortement le volume de spam reçu**.

2 Activation du filtrage indésirable global dans Thunderbird

Procédure :

1. Ouvrir le **menu** ☰
2. Cliquer sur **Paramètres**
3. Sélectionner **Confidentialité et sécurité**
4. Aller à la section **Indésirables**

Vérifier que les options suivantes sont activées :

- ☒ *Activer les contrôles adaptatifs de courrier indésirable*
- ☒ *Quand un message est marqué comme indésirable*
→ **Le déplacer vers le dossier Indésirables**
- ☒ *Faire confiance aux en-têtes de spam du serveur*

Cette configuration permet une analyse combinée locale et serveur.

3 Vérification du dossier de destination des messages indésirables

Dans **Confidentialité et sécurité** :


- Vérifier que le dossier utilisé est :
 - **Indésirables du compte**
- Éviter l'utilisation des **Dossiers locaux**, en particulier pour les comptes IMAP

Cela garantit la synchronisation correcte avec le serveur de messagerie.

4 Déplacement automatique garanti des messages indésirables

Si les messages sont marqués comme indésirables mais restent visibles dans la boîte de réception, il est recommandé de créer un filtre dédié.

Création d'un filtre :


1. Ouvrir le **menu** 
2. Cliquer sur **Outils** → **Filtres de messages**
3. Sélectionner le compte concerné
4. Cliquer sur **Nouveau...**

Paramètres du filtre :

- Nom : Déplacement automatique des indésirables
 - Condition :
 - *État* → *est* → **Indésirable**
 - Action :
 - *Déplacer le message vers* → **Indésirables**
 - Option :
 - ☒ *Appliquer lors de la réception*
-

5 Suppression automatique des indésirables après un délai

Procédure :

1. Ouvrir le **menu** 
2. Cliquer sur **Paramètres**
3. Aller dans **Paramètres du compte**
4. Sélectionner le compte concerné
5. Cliquer sur **Paramètres serveur**
6. Se rendre à la section **Nettoyage automatique**

Configuration recommandée :

- ☒ *Vider le dossier Indésirables après* → **14 jours**
(ou 30 jours pour une adresse critique)
 - (optionnel) ☒ *Vider la corbeille en quittant*
-

6 Bonnes pratiques de sécurité

Recommandé :

- Ne pas ouvrir les messages indésirables
- Ne pas cliquer sur les liens de désinscription douteux
- Marquer les faux positifs comme **Non indésirable**
- Consulter le dossier Indésirables uniquement en cas de message attendu manquant

À éviter :

- Répondre aux spams
 - Cliquer sur des liens inconnus
 - Utiliser une adresse principale sur des services non fiables
-

7 Synchronisation IMAP et suppression côté serveur

Question :

Les messages indésirables sont-ils également supprimés du serveur en configuration IMAP ?

Réponse :

Oui, dans la quasi-totalité des cas.

En configuration **IMAP** :

- Le déplacement vers **Indésirables**
- Puis la suppression automatique après le délai défini

sont **synchronisés avec le serveur**, ce qui implique :

- suppression dans le webmail
- suppression sur les autres appareils
- absence de conservation côté serveur

Exceptions possibles (rares) :

- Paramètres de filtrage de courrier indésirable propres au fournisseur
 - dossiers système verrouillés
 - serveurs très restrictifs
-



Conclusion

Cette configuration, associée à une bonne compréhension du fonctionnement des robots de spam et des filtres, permet :

- une boîte de réception propre et lisible
- une protection efficace et durable
- une suppression automatisée sécurisée
- une synchronisation complète en environnement IMAP

Elle constitue une **configuration fiable, professionnelle et pérenne**.

Je vous prie d'agréer,
l'expression de mes salutations distinguées.

J. Magnin Ceo