

## faq pour professionnels

### 1. Généralités

Pourquoi MailInBlack est plus efficace que les systèmes antispam ordinaires ?  
Comment fonctionne MailInBlack ?

### 2. Questions de fond

Est-ce que tous les correspondants vont s'authentifier ?  
Comment récupérer une newsletter, une confirmation de commande par internet ou encore le message d'un correspondant parti en vacances avant de s'authentifier ?  
MailInBlack est-il compatible avec tous les systèmes de messagerie, architectures et matériels ?  
MailInBlack protège-t-il contre les virus ?  
MailInBlack protège-t-il contre les spams avec usurpation d'adresses ?  
MailInBlack traite-t-il les messages sortants ?  
Combien de temps les emails stoppés sont-ils gardés en mémoire ?  
Que trouve-t-on dans l'*Espace membre* ?  
MailInBlack est-il compatible avec les listes de distribution ?  
MailInBlack est-il compatible avec les alias ?  
Est-ce que MailInBlack retarde la réception des emails ?  
Comment tester MailInBlack ?

### 3. Questions pratiques

Comment accéder à l'*Espace abonné* ?  
Peut-on pré-autoriser des correspondants réguliers ?  
Comment récupérer immédiatement un email stoppé par MailInBlack ?  
Peut-on personnaliser la demande d'authentification ?  
Comment visualiser la demande d'authentification envoyée aux expéditeurs inconnus ?  
Dans quelle langue est envoyée la demande d'authentification ?  
Doit-on supprimer les spams stoppés par MailInBlack ?  
Peut-on interdire à une personne qui s'est authentifiée d'envoyer de nouveaux messages ?  
Comment bannir les adresses email des spammeurs ?

## 1. Généralités

### Pourquoi MailInBlack est meilleur que les systèmes antispam ordinaires ?

Pour les raisons suivantes :

- première solution à garantir 100% d'élimination des spams
- aucun message d'expéditeur humain stoppé par erreur
- aucun travail requis de la part de l'utilisateur/l'administrateur après l'installation

Basés sur des règles de filtrage du contenu du message génériques, les systèmes antispam ordinaires présentent les limites majeures suivantes :

- ils ne peuvent garantir l'élimination de 100% des spams, car les spammeurs contournent en permanence les règles de filtrage mises en place (exemple : le spam par image)
- ils bloquent par erreur des messages valides incertains ou équivoques pour les règles de filtrage (faux-positifs). Le système vous demande ainsi de vérifier régulièrement dans une « boîte à spams » que des bons messages n'ont pas été bloqués à tort. Ceci induit une perte de temps équivalente à recevoir des spams, et revient à trier ses messages
- ils requièrent un travail permanent pour faire évoluer les règles de filtrage (travail d'identification des spams, création de règles par mots clefs sur le contenu ou l'objet du message, adresses email à autoriser ou bannir...). Ceci induit encore une perte de temps conséquente sur le long terme.

La mission de MailInBlack est de faire gagner du temps à l'utilisateur protégé et à l'administrateur de la messagerie. Par conséquent, contrairement aux solutions de filtrage ordinaire, MailInBlack n'impose aucune action de paramétrage de filtre, de tri, de déclaration des spams, de contrôle, de suppression... Toutes synonymes de temps perdu. Une fois MailInBlack mis en place, l'utilisateur et l'administrateur bénéficient d'une économie maximale de temps.

Pour révéler les carences d'une solution concurrente de filtrage ordinaire, il suffit de demander au vendeur un engagement écrit sur :

- le pourcentage de spams arrêtés
- le pourcentage de faux positifs
- le nombre d'heures d'administration hebdomadaires

### Comment fonctionne MailInBlack ?

Lorsqu'un email est adressé à un utilisateur protégé, il arrive sur le serveur MailInBlack.

MailInBlack analyse tout d'abord si l'email est vérolé. Dans ce cas, le virus est détruit et le message stoppé. MailInBlack contrôle ensuite si l'expéditeur est autorisé à envoyer un message à cet utilisateur :

- S'il est dans son carnet d'adresses autorisées, l'email est transmis au serveur de messagerie
- S'il a été banni, l'email est stoppé
- S'il écrit pour la première fois, MailInBlack lui demande de s'authentifier en lui renvoyant un email

Si la procédure de vérification est correctement effectuée par l'expéditeur, le mail est transmis au serveur de messagerie. Dans le cas contraire, le message est placé dans une liste d'attente. Cette liste est accessible à tout moment sur le serveur MailInBlack. Par ailleurs, chaque utilisateur reçoit régulièrement et personnellement un récapitulatif interactif des e-mails stoppés (Digest). La réception de ce Digest interactif est paramétrable par utilisateur : 1 à 3 fois par jour à heures souhaitées, 1 fois par semaine à jour et heure souhaités ou désactivé.

## 2. Questions de fond

### Est-ce que tous les correspondants vont s'authentifier ?

Le spam étant maintenant un fléau, tous les expéditeurs qui écrivent pour la toute première fois à un utilisateur vont bien s'authentifier. Si, de plus, vous avez pris la peine de personnaliser la demande d'authentification avec un logo, ils le feront d'autant plus naturellement. Il est par ailleurs possible de pré-autoriser les contacts habituels de l'entreprise. Ainsi seuls vos nouveaux correspondants recevront une demande d'authentification après l'envoi de leur tout premier message.

### Comment récupérer une newsletter, une confirmation de commande par internet ou encore le message d'un correspondant parti en vacances avant de s'authentifier ?

Une à trois fois par jour (paramétrable individuellement) le système envoie par email à chaque utilisateur un rapport récapitulatif des messages stoppés. Si un utilisateur attend un message particulier de type newsletter, il pourra, par un simple clic, soit récupérer ponctuellement le message de cet expéditeur, soit le récupérer et autoriser en même temps l'adresse expéditrice à lui envoyer de futurs messages. Dans l'urgence, un utilisateur peut aussi se rendre dans son *Espace membre* sécurisé et visualiser, en temps réel, les messages stoppés. Ceux-ci sont gardés jusqu'à 45 jours (durée paramétrable par l'administrateur) avec MIB-Pro et 30 jours avec MIB-Asp, avant d'être automatiquement détruits.

### MailInBlack est-il compatible avec tous les systèmes de messagerie, architectures et matériels ?

Oui. MailInBlack étant une passerelle smtp et recevant tout le flux de messagerie de l'entreprise, le système est compatible avec n'importe quel serveur de messagerie et n'importe quelle architecture ou matériel (portables, pda, Blackberry, etc) placé en aval.

### **MailInBlack protège-t-il contre les virus ?**

Oui, contre tous les virus connus contenus dans les emails (mise à jour toutes les heures). MailInBlack a signé un accord de partenariat avec la société BitDefender qui protège plus de 120 millions d'utilisateurs dans plus de 100 pays. Cet anti-virus de messagerie entrante (classé meilleur antivirus par *l'Ordinateur Individuel* en Mai 2005) est fourni gracieusement.

### **MailInBlack protège-t-il contre les spams avec usurpation d'adresses ?**

Oui. Les spams diffusés avec des adresses usurpées résultent d'un spyware. Ce spyware est « transporté » dans l'email créé afin de contaminer l'ordinateur du destinataire, et d'ainsi propager le spam sans fin (le modèle économique des spammeurs étant d'atteindre le maximum de gens afin que certains achètent leurs produits). Dans ce cas, l'anti-virus de MailInBlack stoppe le spyware, sans se préoccuper si l'expéditeur est autorisé ou non.

Dans le cas exceptionnel où un email avec adresse usurpée est envoyé sans virus, les chances que ce message parvienne à son destinataire sont infimes : puisque MailInBlack est basé sur une authentification par binôme, il faudrait que les spammeurs parviennent à savoir qui est autorisé chez qui. Comme dit plus haut, le modèle économique des spammeurs est d'atteindre le maximum de personnes sans dépenser d'argent. Ils ne peuvent se permettre de passer du temps pour rechercher les binômes d'authentification. En outre, ils n'ont aucun intérêt à spammer une seule adresse.

### **MailInBlack traite-t-il les messages sortants ?**

Non. Le travail de la passerelle MailInBlack est de bloquer les spams entrants.

### **Combien de temps les emails stoppés sont-ils gardés en mémoire ?**

Les emails stoppés sont conservés sur le serveur MailInBlack jusqu'à 45 jours paramétrable avec MIB-Pro et 30 jours avec MIB-Asp. Ensuite, ils s'auto-détruisent. Personne ne doit perdre son temps pour les supprimer.

### **Que trouve-t-on dans l'Espace membre ?**

Chaque utilisateur protégé a accès à un *Espace membre* sécurisé par un mot de passe. Il y trouvera, en fonction des souhaits de l'entreprise : expéditeurs autorisés ; expéditeurs bannis (qui ont pris la peine de s'authentifier mais dont il ne souhaite pas recevoir de futurs messages) ; quarantaine des emails stoppés...

### **MailInBlack est-il compatible avec les listes de distribution ?**

Oui. Il suffit de pré-autoriser l'adresse email de la liste de distribution.

### **MailInBlack est-il compatible avec les alias ?**

Oui. MailInBlack accepte jusqu'à 6 alias par utilisateur, pour le coût d'une seule licence.

### **Est-ce que MailInBlack retarde la réception des emails ?**

Non. Après réception des messages par la passerelle MailInBlack, il faut quelques dizaines de secondes pour les traiter (anti-virus et anti-spam) et les délivrer si l'expéditeur est authentifié.

### **Comment tester le fonctionnement de la solution MailInBlack ?**

Si malgré des analyses conceptuelle et technique concluantes pour MailInBlack vous souhaitez vous conforter par un test, nous proposons un « Try and Buy » : cela vous permet de procéder à l'installation habituelle de MailInBlack ASP ou PRO et de tester gracieusement la solution pendant 3 semaines. Au terme de cette période, vous gardez la solution ou annulez sans frais. Veuillez contacter un revendeur pour mettre en place un « Try and Buy ».

## **3. Questions pratiques**

---

### **Comment accéder à l'Espace membre ?**

Grâce à un navigateur internet, taper l'adresse de la passerelle MailInBlack, puis entrer votre adresse email et votre mot de passe. Si la personne ne s'est pas déconnectée, elle entrera immédiatement dans son *Espace membre* sans avoir à entrer à nouveau ses identifiants.

### **Peut-on pré-autoriser des correspondants réguliers ?**

Oui. Il est conseillé de le faire avant la mise en service car seuls les gens qui écrivent habituellement à vos collaborateurs peuvent être surpris par une demande d'authentification. L'administrateur ou les utilisateurs peuvent pré-autoriser de manière globale ou un par un, les noms de domaine ou les adresses emails à pré-autoriser. De fait, ces gens n'auront pas à s'identifier.

### **Comment récupérer immédiatement un email stoppé par MailInBlack ?**

Se rendre dans son *Espace membre* et cliquer sur *Emails stoppés des 30 derniers jours*. Sélectionner l'email concerné et cliquer sur *Récupérer* ou *Autoriser*. Pour information, les emails stoppés depuis la dernière visite sur cette page apparaissent en gras.

### **Peut-on personnaliser la demande d'authentification ?**

Oui. Il est conseillé de le faire avant la mise en service avec notamment un logo. Cette image apparaît non seulement dans la demande d'authentification envoyée aux expéditeurs inconnus, mais aussi sur la page web où les expéditeurs inconnus s'authentifieront. La personnalisation peut se faire de manière uniforme pour tous les utilisateurs d'un même domaine, ou bien de manière individuelle.

### **Comment visualiser la demande d'authentification envoyée aux correspondants inconnus ?**

Rendez-vous dans l'*Espace membre* du gestionnaire de domaine, cliquez sur *Paramètres, Personnalisation du message* puis : (voir ce message).

### **Dans quelle langue est envoyée la demande d'authentification ?**

Le message d'authentification envoyé par MailInBlack aux expéditeurs inconnus est en deux langues à choisir parmi le français, l'anglais, l'allemand, l'italien et l'espagnol. Afin de paramétrer cela, rendez-vous dans votre *Espace membre*, cliquez sur *Paramètres* puis *Personnalisation du message*. La personnalisation peut se faire de manière uniforme pour tous les utilisateurs d'un même domaine, ou bien de manière individuelle.

### **Doit-on supprimer les spams stoppés par MailInBlack ?**

Non. Les spams sont stoppés sur le serveur MailInBlack, avant qu'ils n'atteignent votre serveur de messagerie, et s'auto-détruisent au terme de la période de quarantaine. Vous ne les voyez donc pas apparaître sur les postes utilisateurs et personne n'a d'intervention à faire ! C'est l'un des atouts de MailInBlack qui offre un gain de temps maximal, aussi bien pour l'utilisateur final que pour l'administrateur.

### **Peut-on interdire à une personne qui s'est authentifiée d'envoyer de nouveaux messages ?**

Oui. Pour cela, chaque utilisateur (pour son propre compte) ou l'administrateur (pour tous les comptes) peut bannir une personne qui se serait authentifiée mais dont vous ne souhaitez plus recevoir de message.

### **Comment bannir les adresses email des spammeurs ?**

Nul besoin de faire cela : les spams sont stoppés sur le serveur MailInBlack, avant qu'ils n'atteignent votre serveur de messagerie, et s'auto-détruisent au bout de la période de quarantaine (paramétrable jusqu'à 45 j). Vous ne les voyez donc pas apparaître sur les postes utilisateurs et personne n'a d'intervention à faire. Les bannir serait une pure perte de temps et ne servirait pas à rien car les spammeurs changent d'adresse d'expédition en permanence.

Avec MailInBlack, la notion de "Bannir" un expéditeur n'est utile que lorsqu'un expéditeur a pris la peine de s'authentifier, et dont on ne souhaite plus recevoir de messages. Pour cela, chaque utilisateur (pour son propre compte) ou l'administrateur (pour tous les comptes) peut se rendre dans son *Espace membre* et bannir un expéditeur authentifié.

