GUIDE D'UTILISATION COMPLET

MICROSOFT DEFENDER,

une solution de sécurité pour sécuriser votre environnement de travail

Guide pour utiliser votre solution DEFENDER

Découvrez dans cette fiche comment tirer parti des principales fonctionnalités de DEFENDER.

SOMMAIRE

À vos côtés, au quotidien pour la gestion de votre informatique et de votre téléphonie IP

Comment fonctionne Microsoft DEFENDER ?

Microsoft DEFENDER est un outil de sécurité intégré à Microsoft 365, conçu pour protéger les utilisateurs contre les menaces numériques telles que les virus, les ransomwares, le phishing et les attaques ciblées. Il agit en arrière-plan pour sécuriser les emails. Il agit sur plusieurs fronts :

- **Protection contre les logiciels malveillants (malwares, ransomwares, virus)** : DEFENDER analyse continuellement vos fichiers, vos applications et vos téléchargements pour détecter et neutraliser les menaces avant qu'elles n'affectent vos systèmes.
- **Sécurité des emails et des identités** : Il filtre les tentatives de phishing, les spams et les emails malveillants, tout en protégeant vos identifiants de connexion contre les compromissions.
- **Protection des appareils** : Que vous utilisiez un ordinateur portable, un poste de travail ou un appareil mobile, DEFENDER sécurise votre appareil contre les menaces externes.
- **Détection et réponse avancées** : Il surveille les comportements suspects et les activités anormales sur votre réseau, permettant une identification et une neutralisation rapide des menaces complexes.

Le portail de sécurité Microsoft DEFENDER : Une vision centralisée

En complément de cette protection en arrière-plan, Microsoft DEFENDER dispose d'un **portail de sécurité dédié**. Ce **tableau de bord unique**, accessible depuis n'importe quel navigateur web, est le **point de convergence** de toutes les informations de sécurité collectées par DEFENDER.

Ce portail offre une vision claire de la sécurité de votre environnement. C'est là que vous pouvez consulter et gérer vos emails mis en quarantaine, en plus de retrouver toutes les alertes et les statuts des menaces détectées.

→ ***En savoir plus sur l'utilisation du portail :*** *rendez-vous à la page 10* (ici)

CONSEILS : RETROUVEZ FACILEMENT VOTRE TABLEAU DE BORD, EN ENREGISTRANT LA PAGE WEB :

(HTTPS://SECURITY.MICROSOFT.COM/QUARANTINE)

- EN FAVORI DANS VOTRE NAVIGATEUR WEB
- OU EN RACCOURCI SUR VOTRE POSTE DE TRAVAIL

Comment Microsoft DEFENDER vous alerte ?

Microsoft DEFENDER ne se contente pas de bloquer les emails suspects dans votre messagerie : il vous informe activement par email lorsqu'une action de sécurité a été prise. Ces messages d'alerte vous permettent de rester informé et de garder le contrôle.

Quels types d'email pouvez-vous recevoir dans votre messagerie de la part de Microsoft DEFENDER ?

Selon votre configuration et vos licences, vous pourriez être amené à recevoir des :

1. **Alertes de sécurité** :

DEFENDER analyse continuellement vos fichiers, vos applications et vos téléchargements pour détecter et neutraliser les menaces avant qu'elles n'affectent vos systèmes.

2. **Rapports quotidiens/hebdomadaires** :

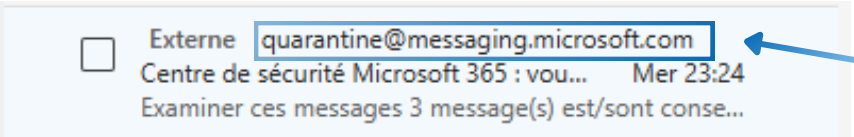
Ces emails récapitulent l'activité de sécurité de DEFENDER sur une période donnée (menaces bloquées, analyses effectuées, etc.). Ils sont purement informatifs.

3. **Notifications de quarantaine ou de blocage d'emails** :

Ces emails indiquent qu'un message a été mis en quarantaine ou bloqué parce qu'il a été jugé suspect (spam, phishing potentiel).

À quoi ressemblent ces messages d'alerte de Microsoft DEFENDER ?

Dans votre messagerie, vous verrez apparaître un email similaire à celui-ci :



L'adresse de l'expéditeur est : *quarantine@messaging.microsoft.com*

SOYEZ TOUJOURS VIGILANTS SUR LES ADRESSES DES EXPÉDITEURS, LES EMAIS DE DEFENDER PROVIENNENT DE

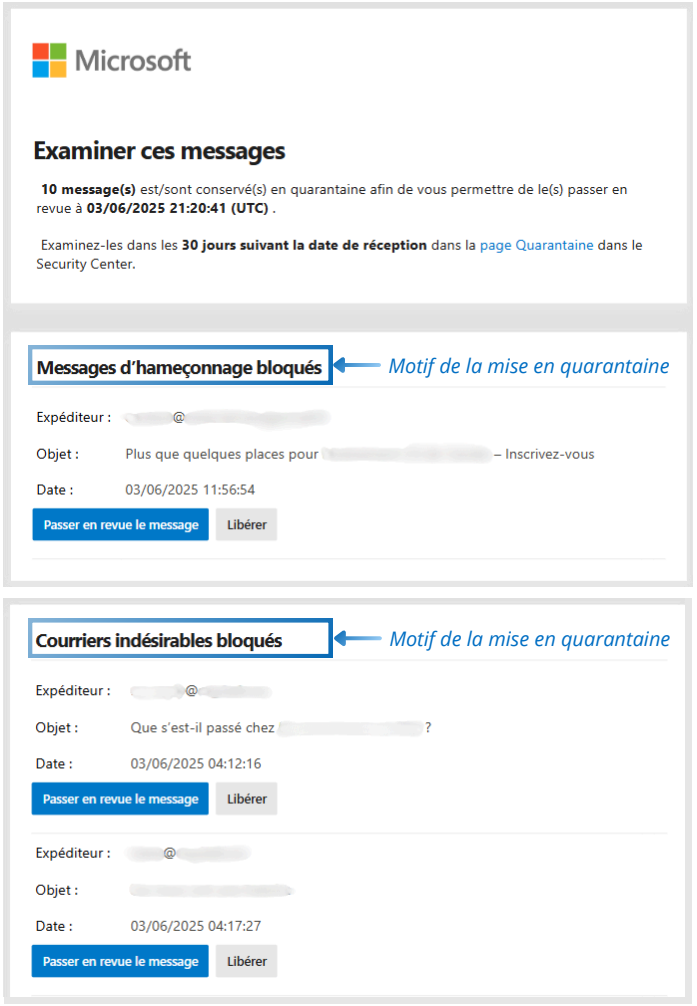
quarantine@messaging.microsoft.com

EMAILS QUE VOUS POUVEZ RECEVOIR DE LA PART DE MICROSOFT DEFENDER

Que contiennent ces emails ?

Ils vous informent que des messages que vous avez reçus dans votre messagerie ont été placés en quarantaine par Microsoft DEFENDER.

Voici un aperçu de ces emails :
Vous aurez l'indication du nombre de messages placés en quarantaine, ils sont listés selon le motif de la mise en quarantaine.



Chaque message est listé avec les informations suivantes :

- Expéditeur
- Objet du message
- Date de réception

Pour chaque message, vous avez généralement deux options :

- **Passer en revue le message** : pour consulter son contenu en toute sécurité.
- **Libérer** : pour le remettre dans votre boîte de réception s'il est légitime.

Ces emails sont envoyées automatiquement par Microsoft DEFENDER pour vous aider à :

- ☑ Identifier rapidement les messages bloqués,
- 🛠 Décider quoi faire (consulter le tableau de quarantaine, libérer des emails...),
- 🔒 Renforcer votre vigilance face aux menaces.

GARDEZ À L'ESPRIT QUE :

SI UN EMAIL DE DEFENDER VOUS SEMBLE SUSPECT OU SI VOUS AVEZ DES DOUTES, NE CLIQUEZ SUR AUCUN LIEN.

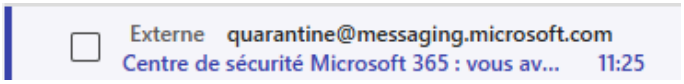
Quels sont les indicateurs que vous pouvez rencontrer dans les emails que vous recevez (autre que ceux de DEFENDER) ?

Selon votre configuration, votre version de Outlook (*afin de bénéficier des boutons d'action, privilégiez la nouvelle version de Outlook)*, Microsoft DEFENDER peut ajouter des indicateurs visuels et des options d'action directement dans les emails que vous recevez, pour vous aider à identifier et gérer les messages potentiellement dangereux.

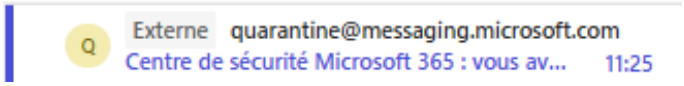
→ MENTION "**EXTERNE**" DANS L'OBJET OU L'ENTÊTE :

Certains emails affichent la mention "**EXTERNE**" pour signaler que le message provient d'un expéditeur extérieur à votre organisation. Cela vous incite à être plus vigilant, notamment en cas de tentative de phishing ou usurpation d'identité.

Dans l'application bureau Outlook (nouvelle version) :



Dans Outlook depuis votre navigateur Web :



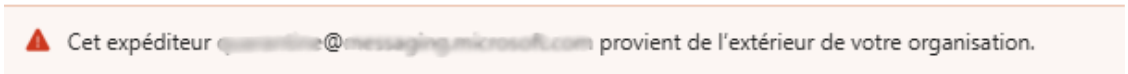
→ BANNIÈRE D'**AVERTISSEMENT** DANS LES EMAILS :

Des bannières d'alerte peuvent apparaître en haut des emails :

- **EXPÉDITEUR EXTERNE :**

  Vous pouvez apercevoir une bannière pour vous rappeler l'origine externe d'un email.

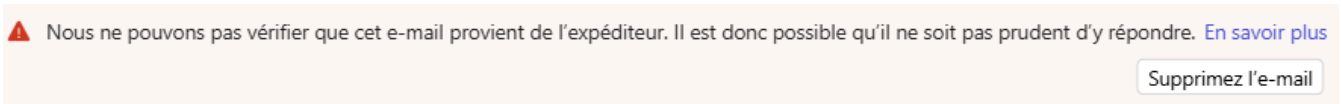
  Soyez prudent si vous ne reconnaissez pas l'expéditeur ou si le message contient des pièces jointes ou des liens.



- **EXPÉDITEUR NON RECONNU :**

  Vous pouvez rencontrer une bannière vous indiquant que Microsoft DEFENDER ne parvient pas à authentifier l'expéditeur du message.

  Soyez vigilant, ne répondez pas, ne cliquez pas sur les liens et n'ouvrez pas les pièces jointes si vous avez un doute.



- **PARTIELLEMENT BLOQUÉ :**

  Si un email contient des images, des liens ou des pièces jointes jugées suspectes par DEFENDER, leur affichage peut être bloqué par défaut pour votre sécurité. Vous verrez alors un message du type :

  > Le contenu de ce message a été partiellement bloqué car l'expéditeur ne figure pas dans votre liste d'expéditeurs approuvés.

- **PIÈCE JOINTE DANGEREUSE :**

  Si une pièce jointe est identifiée comme potentiellement malveillante, DEFENDER peut la bloquer ou la mettre en quarantaine, vous en informant directement dans l'email avec un message comme :

  > La pièce jointe [nom_fichier] a été bloquée car elle est potentiellement dangereuse.

Quels boutons d'action dans les emails ?

Lorsque vous recevez un email, Microsoft DEFENDER peut détecter des éléments suspects ou inhabituels. Pour vous aider à réagir de manière appropriée, des boutons d'action apparaissent directement dans certains emails.
Ces boutons vous permettent de gérer la sécurité de vos emails en quelques clics, sans avoir besoin d'aller sur le portail dédié.

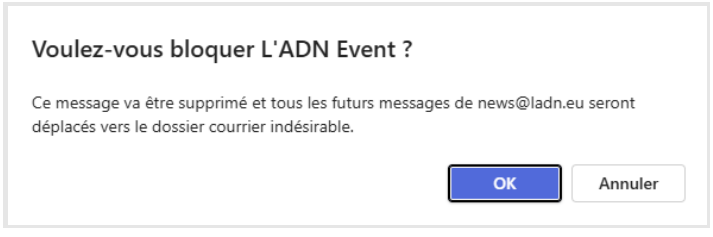
⚠ *Les boutons d'action, apparaissent pour les utilisateurs de la nouvelle version de Outlook*

✉ COMPRENDRE LES BOUTONS D'ACTION DANS VOS EMAILS

Bloquer l'expéditeur

Ce bouton permet de bloquer tous les futurs messages provenant de l'adresse email en question.

→ ***Lorsque vous cliquez sur le bouton :*** *l'expéditeur est ajouté à la liste des expéditeurs bloqués. Les futurs emails seront automatiquement bloqués*



La fenêtre suivante peut s'afficher pour vous demander de confirmer votre demande.

Cliquez sur OK *pour valider*

Afficher le contenu bloqué

Microsoft DEFENDER bloque par défaut certains contenus (images, scripts, liens) dans les emails provenant d'expéditeurs non approuvés.

→ ***Lorsque vous cliquez sur le bouton :*** *vous autorisez l'affichage des contenus bloqués pour ce message uniquement. Cela peut inclure des images distantes ou des liens désactivés.*

Gérer l'expéditeur

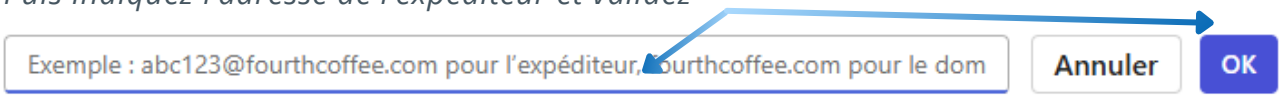
Ce bouton ouvre les options de gestion de l'expéditeur. Vous pouvez choisir d'ajouter l'expéditeur à la liste des expéditeurs approuvés ou bloqués, ou encore consulter les paramètres de sécurité associés à cet expéditeur.

→ ***Lorsque vous cliquez sur le bouton :*** *la fenêtre "**Courrier indésirable**" s'ouvre. Lorsque vous descendez plus bas dans la fenêtre, vous avez la possibilité d'ajouter des expéditeurs dans la liste des :*

Expéditeurs et domaines approuvés *ou* Domaines et expéditeurs bloqués

Cliquez sur le bouton + Ajouter un expéditeur *pour ajouter un expéditeur dans la liste de votre choix (approuvés ou bloqués).*

Puis indiquez l'adresse de l'expéditeur et validez



Expéditeur de confiance

Ce bouton permet d'indiquer que l'expéditeur est fiable.

→ ***Lorsque vous cliquez sur le bouton :*** *l'adresse est ajoutée à la liste des expéditeurs approuvés. Les futurs messages de cette adresse ne seront plus filtrés ni bloqués.*

Supprimez l'e-mail

Ce bouton permet de supprimer définitivement le message de la quarantaine.

→ ***Lorsque vous cliquez sur le bouton :*** *Lorsque vous cliquez sur ce bouton, l'email est effacé immédiatement et ne pourra plus être restauré.*

Comment retrouver les paramètres de gestion des expéditeurs dans votre messagerie ?

Depuis votre messagerie, à tout moment vous pouvez gérer vos expéditeurs bloqués ou autorisés.

→ ***Dans la messagerie Outlook en version classique*** **:** (Nouvelle version d'Outlook)

Accédez à l'onglet Accueil *dans le menu en haut de votre messagerie puis sur les options supplémentaires en cliquant sur* ··· *, sélectionnez ensuite* Bloquer *et* Options du courrier indésirable...

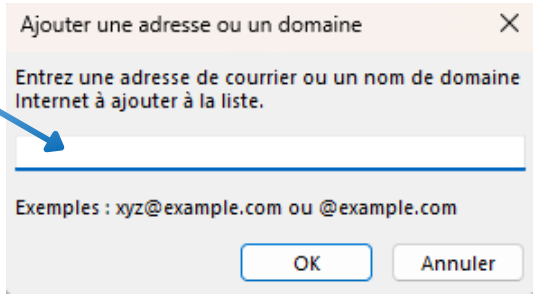
Dans la fenêtre qui s'ouvre, choisissez l'onglet de votre choix entre :

Expéditeurs bloqués *ou* Expéditeurs approuvés

Pour ajouter l'adresse email, cliquez sur le bouton Ajouter...

Dans la nouvelle fenêtre, indiquez l'adresse email dans la case prévue, puis OK

Depuis cette fenêtre, vous avez également la possibilité de modifier et supprimer des emails déjà présents dans la liste.



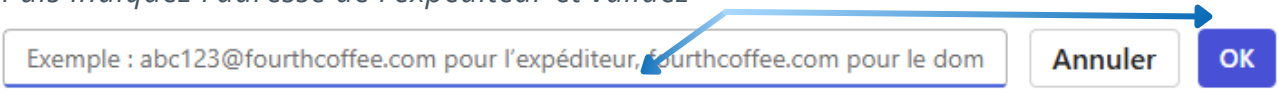
→ ***Dans la messagerie Outlook dans la nouvelle version*** **:** (Nouvelle version d'Outlook)

En haut à droite de votre messagerie, cliquez sur les paramètres ⚙ *, puis à gauche cliquez sur l'onglet* Courrier *et ensuite sur* Courrier indésirable

*La fenêtre "**Courrier indésirable**" s'ouvre. Descendez plus bas dans la fenêtre, pour sélectionner la liste de votre choix :* Expéditeurs et domaines approuvés *ou* Domaines et expéditeurs bloqués

Cliquez sur le bouton + Ajouter un expéditeur *pour ajouter un expéditeur dans la liste de votre choix (approuvés ou bloqués).*

Puis indiquez l'adresse de l'expéditeur et validez



Comment procéder pour effectuer un signalement d'un email ?

Depuis votre messagerie, vous avez la possibilité de signaler les emails. C'est un geste simple et important qui aide DEFENDER à améliorer ses filtres et à mieux vous protéger.

Dans votre messagerie Outlook

Sélectionnez l'email suspect, puis dans le ruban en haut de votre messagerie cliquez sur le bouton  *ou* 

afin de dérouler la liste d'actions proposées suivante :

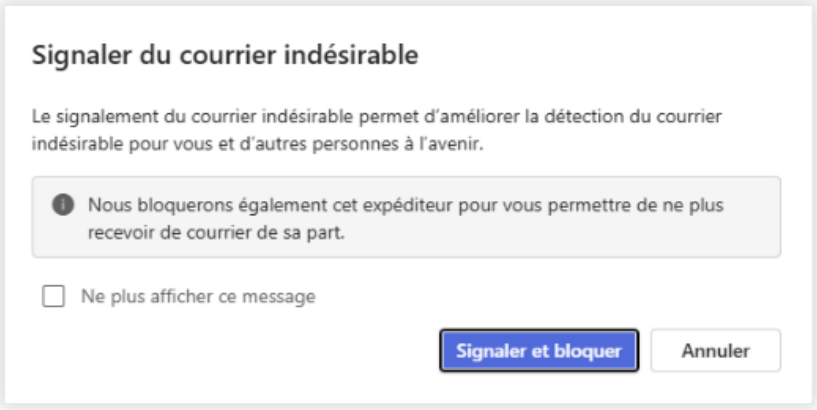
- 

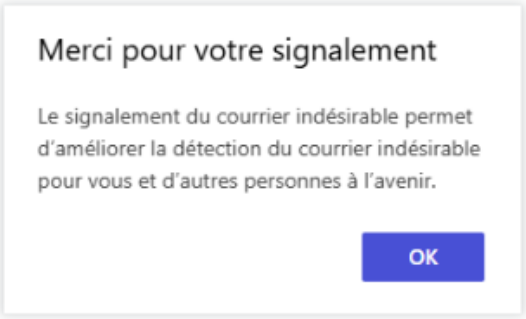
Email qui semble légitime, mais qui est en fait une tentative d'obtenir vos informations personnelles ou de voler votre argent.

- 

email non sollicité, souvent publicitaire ou frauduleux, qui peut nuire à la sécurité ou encombrer la boîte de réception.

Lorsque vous signaler un email, vous pouvez voir apparaître des fenêtres pour demander la confirmation de votre choix ou vous remercier peuvent apparaîtrent.





SE CONNECTER AU PORTAIL DE SÉCURITÉ MICROSOFT DEFENDER

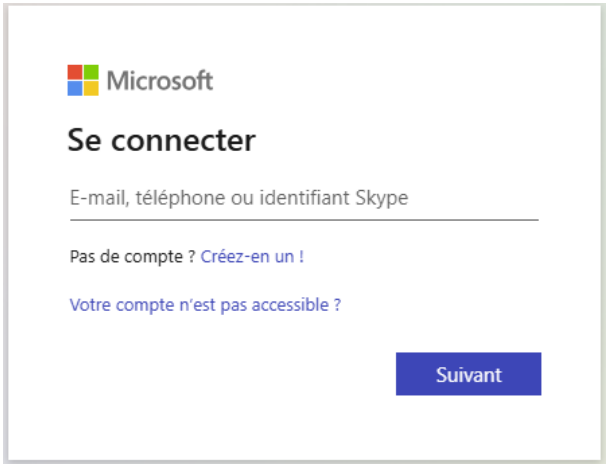
Le portail de Microsoft DEFENDER : votre tableau de bord sécurité

Le portail Microsoft DEFENDER est un espace centralisé qui permet de comprendre et de gérer la sécurité de votre environnement Microsoft 365.

Comment vous connecter au portail ?

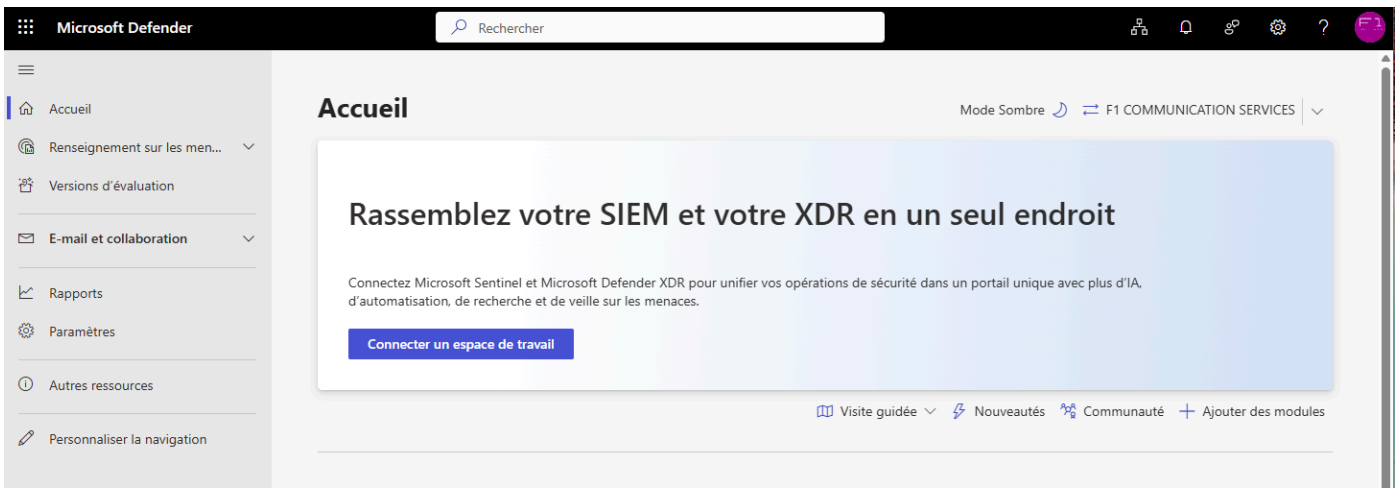
1. **Aller sur le portail dédié** : Ouvrez votre navigateur Internet et rendez-vous à l'adresse suivante : https://security.microsoft.com/

(*pour retourner facilement sur le tableau de bord, pensez à enregistrer la page dans les favoris de votre navigateur ou en raccourci sur votre poste de travail)*



2. **Utilisez vos identifiants Microsoft 365** : Connectez-vous avec les mêmes identifiants (adresse email et mot de passe) que ceux que vous utilisez pour votre compte Microsoft 365.

3. **Explorez le tableau de bord** : Une fois connecté, selon vos paramètres, vous accédez à un tableau de bord clair et synthétique.



Présentation des fonctionnalités du portail

Le contenu du menu et les fonctionnalités disponibles peuvent varier selon vos paramètres, les options activées et le choix de vos licences. Voici un aperçu des principales fonctionnalités que vous êtes susceptible de retrouver.

Pour information : vous pouvez personnaliser votre menu depuis l'onglet Personnaliser la navigation

Renseignement sur les men...

Objectif : Comprendre les menaces actuelles et anticiper les attaques.

- Analyse des menaces : *vue d'ensemble et recherche en temps réel.*
- Suivi : *investigations et analyses dans la durée.*

Versions d'évaluation

Objectif : Tester les fonctionnalités avancées de DEFENDER.

- Possibilité d'activer temporairement certaines fonctionnalités.
- Accès à des rapports de test et à des recommandations personnalisées.

E-mail et collaboration

Accédez à la gestion de vos emails en quarantaine : page 10

Objectif : Accéder à votre tableau de bord pour gérer la sécurité des emails.

- Consulter les emails bloqués dans la quarantaine.
- Suivre les menaces détectées et transmettre les éléments suspects à Microsoft.

Rapports

Objectif : Suivre l'état de la sécurité et les performances de DEFENDER.

- Vue d'ensemble : *synthèse des menaces, actions menées et utilisateurs à risque.*
- Personnalisation : *filtres par période, type de menace et service.*
- Export : *téléchargement en Excel ou PDF.*

Paramètres

Objectif : Configurer les règles de sécurité selon les besoins de votre organisation.

- Portail : personnalisation de l'affichage, langue et notifications.
- Sécurité & automatisation : règles de protection, connexions de données, actions via Sentinel.

Autres ressources

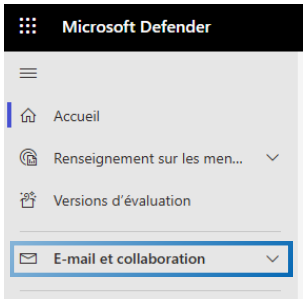
Objectif : Accéder à des outils complémentaires.

- Ressources avancées : *Microsoft Purview (données sensibles), portail Azure (configurations).*
- Support & apprentissage : *guides et tutoriels via Microsoft Learn.*

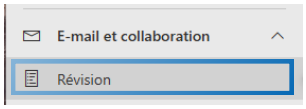
Pourquoi des emails sont en quarantaine ?

Lorsque Microsoft DEFENDER détecte un email suspect (phishing, spam, contenu malveillant), il est automatiquement placé en quarantaine. Cela signifie qu'il est mis de côté, sans être supprimé, pour vous permettre de l'examiner en toute sécurité.

Où retrouver les emails en quarantaine ?



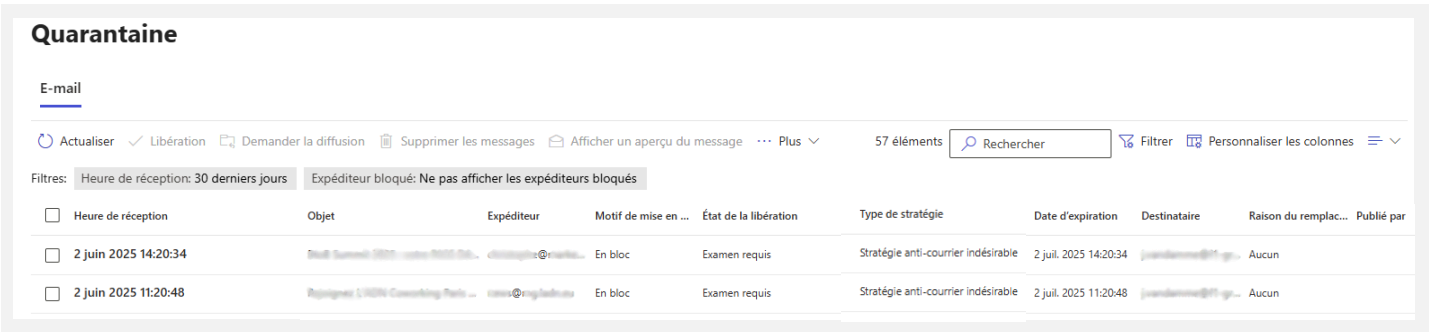
Dans le menu sur la gauche, cliquez sur "**email et collaboration**".
Lorsque vous cliquez, un sous-menu s'ouvre.



Cliquez ensuite sur "**Révision**"

À présent sur la droite, cliquez sur l'encadré pour consulter la liste des messages en quarantaine

Vous pouvez alors consulter le tableau qui liste vos emails mis en quarantaine :



Comprendre les colonnes du tableau de quarantaine

Le tableau des messages en quarantaine vous donne un aperçu des emails bloqués. Voici ce que signifie chaque colonne :

HEURE DE RÉCEPTION, OBJET, EXPÉDITEUR ET DESTINATAIRE

Ces colonnes fournissent les informations de base de l'email, elles sont simples à comprendre et permettent une première identification rapide du message.

MOTIF DE MISE EN QUARANTAINE

Cette colonne explique la raison précise pour laquelle Microsoft DEFENDER a mis l'email en quarantaine. Ainsi vous pouvez rencontrer les motifs suivants :

- **En bloc** : L'email a été détecté comme faisant partie d'un envoi massif, souvent indésirable (type newsletter non sollicitée).
- **Courrier indésirable** : Message détecté comme spam ou publicité non sollicitée.
- **Logiciel malveillant** : L'email contenant une pièce jointe ou un lien identifié comme dangereux (virus, ransomware, etc.).
- **Hameçonnage** : Il s'agit d'email dont le but est de voler vos informations (identifiants, mots de passe) ou de vous tromper.
- **Hameçonnage à haute fiabilité** : Une tentative d'hameçonnage très sophistiquée et dangereuse, jugée avec une forte probabilité de nuire.

ÉTAT DE LA LIBÉRATION

Cette colonne indique si l'email a été libéré (remis dans la boîte de réception), supprimé, ou toujours en quarantaine. Il existe plusieurs intitulés :

- **Examen requis** : Le message est en attente d'une décision (libération ou suppression).
- **Refusé** : La demande de libération du message a été refusée par un administrateur.
- **Libération demandée** : Une demande de libération a été effectuée et est en attente d'approbation.
- **Libéré** : Le message a été délivré avec succès de la quarantaine vers la boîte de réception du destinataire.

TYPE DE STRATÉGIE

Cette colonne indique quelle règle de sécurité de Microsoft DEFENDER a intercepté et mis l'mail en quarantaine.

- **Stratégie anti-programme malveillant** : L'email a été bloqué car il contenait un logiciel malveillant (virus, rançongiciel, etc.).
- **Stratégie de pièces jointes fiables** : Le message a été mis en quarantaine en raison d'une pièce jointe suspecte ou potentiellement dangereuse.
- **Stratégie anti-hameçonnage** : L'email a été détecté comme une tentative d'hameçonnage (phishing) visant à voler des informations.
- **Stratégie anti-courrier indésirable** : Le message a été identifié comme un spam ou un courrier indésirable.
- **Règle de transport** : L'email a été bloqué par une règle de flux de messagerie spécifique configurée par votre administrateur pour des raisons de sécurité.

DATE D'EXPIRATION

Montre la date après laquelle le message sera automatiquement supprimé de la quarantaine s'il n'a pas été libéré ou supprimé manuellement. Les messages en quarantaine sont conservés pendant une période limitée.

RAISON DU REMPLACEMENT DE L'ADRESSE DE L'EXPÉDITEUR

Cette colonne apparaît si l'adresse de l'expéditeur a été modifiée par DEFENDER pour des raisons de sécurité (par exemple, pour afficher le vrai domaine de l'expéditeur lors d'une usurpation). Elle explique pourquoi cette modification a été effectuée.

PUBLIÉ PAR

Indique la personne ou le système qui a effectué une action de libération ou de suppression sur le message en quarantaine. Si vous avez libéré un message, votre nom pourrait donc apparaître ici.

ACTIONS POSSIBLES DANS LE TABLEAU QUARANTAINE :

ACTIONS LIÉES AUX OPTIONS DU TABLEAU

Actualiser — Permet de mettre à jour le tableau et ainsi avoir les derniers emails reçus.

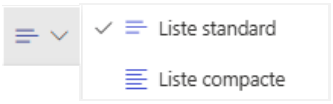
→ ***Lorsque vous cliquez sur le bouton :*** *si de nouveaux emails ont été reçus, ils apparaîtront alors.*

Personnaliser les colonnes — Les colonnes de ce tableau sont personnalisables, vous pouvez choisir les colonnes à afficher.

→ ***Lorsque vous cliquez sur le bouton :*** *vous pouvez sélectionner les éléments que vous souhaitez voir apparaître ou non dans votre tableau en les cochant ou en les décochant.*

Filtrer — Permet d'afficher uniquement les messages qui correspondent à vos critères.

→ ***Lorsque vous cliquez sur le bouton :*** *vous avez des options proposées pour filtrer tels que l'ID du message, adresse de l'expéditeur, objet de l'email, date, motif de quarantaine, état de la libération, type de stratégie, etc...*

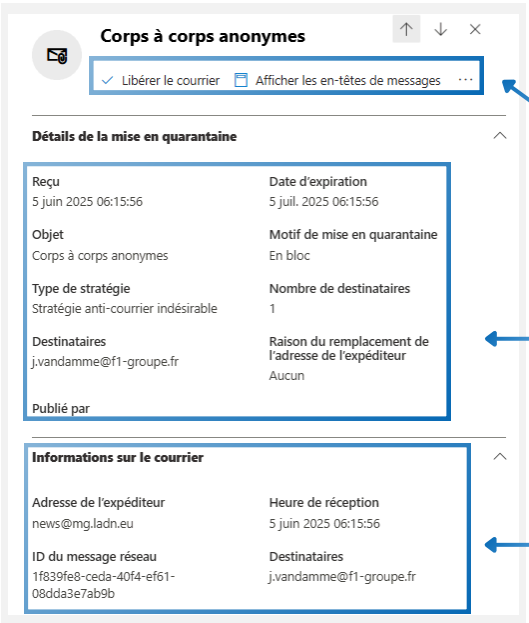


Permet de modifier l'espacement des lignes du tableau.

→ ***Lorsque vous cliquez sur le bouton :*** *lorsque vous sélectionnez "**Liste standard**", les lignes du tableau sont espacées. Si vous sélectionnez "**Liste compacte**", les lignes sont moins hautes.*

*Retrouvez la procédure pour afficher les emails en quarantaine d'une boîte aux lettres partagée **ici***

Vous avez la possibilité de consulter les détails d'un email, pour cela il faut cliquer sur une des colonnes d'un email de la liste.



→ ***Lorsque vous cliquez sur une colonne du tableau :*** *une fenêtre s'ouvre avec différentes informations :*

- *Des actions liées à l'email ; Libération, Aperçu de l'email ou des en-têtes, Supprimer de la quarantaine, Autoriser l'expéditeur... (voir le détail de ces options dans les pages 14 et 15)*
- *Les détails de la mise en quarantaine*
- *Les informations sur le courrier*

ACTIONS LIÉES AUX EMAILS :

Lorsque vous sélectionnez un email dans le tableau, d'autres d'options s'offrent à vous :

✓ Libération

Permet de délivrer le message mis en quarantaine directement dans votre boîte de réception.

→ ***Lorsque vous cliquez sur le bouton :*** *L'email est déplacé de la quarantaine vers votre dossier de réception habituel.*

Supprimer les messages

Utilisez cette option pour effacer définitivement le ou les emails sélectionnés de la quarantaine.

→ ***Lorsque vous cliquez sur le bouton :*** *Les emails choisis sont supprimés de manière irréversible.*

⚠️ ***À savoir :*** *tout élément non détruit dans la quarantaine le sera automatiquement après 30 jours.*

Afficher un aperçu du message

Permet de visualiser le contenu de l'email mis en quarantaine en toute sécurité, sans qu'il ne quitte la quarantaine. Cela permet de vérifier qu'il est légitime et qu'il ne contient pas de spam ou de phishing.

→ ***Lorsque vous cliquez sur le bouton :*** *Une fenêtre s'ouvre pour vous montrer le contenu de l'email sans risque pour votre système.*

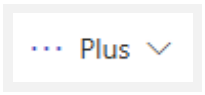
→ *Lorsque vous affichez l'aperçu d'un email mis en quarantaine, certaines ressources (comme des images, des liens ou des contenus hébergés en ligne) ne sont pas chargées automatiquement pour des raisons de sécurité. Vous avez néanmoins la possibilité d'afficher le contenu non visible en cliquant sur le bouton :*

Charger des ressources externes dans ce message

⚠️ ***Attention*** *:*

- *Ces ressources peuvent provenir de serveurs externes potentiellement malveillants.*
- *Leur chargement peut confirmer à l'expéditeur que votre adresse email est active, ce qui peut encourager d'autres tentatives de phishing.*
- *Il est recommandé de cliquer uniquement si vous êtes sûr de la légitimité de l'expéditeur.*

→ ***Une fois votre vérification terminée :*** *cliquez sur la croix dans le coin en haut à droite pour fermer la fenêtre et revenir à la quarantaine*

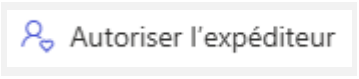


Ce bouton donne accès à des actions supplémentaires pour gérer le message en quarantaine.

→ ***Lorsque vous cliquez sur le bouton :*** *Un menu déroulant apparaît, proposant les options suivantes:*

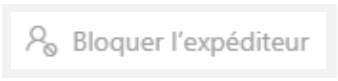
Affiche les détails techniques de l'email, utiles pour comprendre son origine et son cheminement.

→ ***Lorsque vous cliquez sur le bouton :*** *Une fenêtre s'ouvre pour vous montrer les informations d'en-tête complètes de l'email.*



Marquez l'expéditeur comme sûr, afin que ses futurs messages ne soient plus mis en quarantaine.

→ ***Lorsque vous cliquez sur le bouton :*** *L'adresse email de l'expéditeur est ajoutée à une liste d'expéditeurs approuvés, garantissant que ses prochains messages arrivent directement dans votre boîte de réception.*



Empêchez définitivement cet expéditeur d'envoyer des messages vers votre boîte de réception.

→ ***Lorsque vous cliquez sur le bouton :*** *L'expéditeur est ajoutée à une liste d'expéditeurs bloqués, et tous ses futurs messages seront automatiquement mis en quarantaine ou rejetés.*

CONSULTATION DES EMAILS D'UNE BOÎTE AUX LETTRES PARTAGÉE

Dans certains cas, il peut être nécessaire de consulter les messages en quarantaine d'une boîte aux lettres partagée. Voici comment procéder étape par étape pour y accéder via le portail Microsoft Defender.

COMMENT PROCÉDER POUR CONSULTER LES EMAILS D'UNE MESSAGERIE PARTAGÉE ?

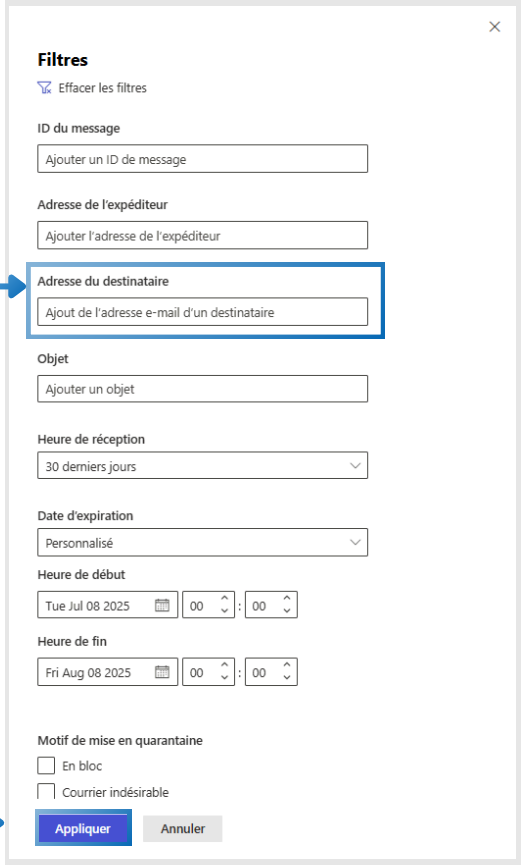
Dans le tableau des emails en quarantaine, cliquez en haut sur le bouton Filtrer, comme son nom l'indique, il permet de filtrer les emails du tableau.

Lorsque vous avez cliqué, un fenêtre apparaît avec plusieurs options de filtre.

Dans le champs "**Adresse du destinataire**", saisissez l'adresse email de la boîte aux lettres partagée

(ex. : support@entreprise.com)

Cliquez sur le bouton "Appliquer", en bas de la fenêtre pour valider.



Vous pouvez maintenant consulter les emails en quarantaine pour l'adresse email que vous avez indiqué dans les filtres.

Dans le tableau, cliquez sur un message pour en voir le contenu, le libérer, ou le signaler comme légitime ou malveillant selon le cas.

Vous pouvez ainsi facilement surveiller les messages en quarantaine d'une boîte partagée et intervenir rapidement en cas de besoin.

Vos questions sur DEFENDER : Nos réponses

Dois-je installer quelque chose pour Microsoft DEFENDER ?

Non, Microsoft DEFENDER est intégré à votre environnement Microsoft 365. Il est géré et configuré par F1 GROUPE, vous n'avez donc aucune installation à effectuer.

Puis-je désactiver Microsoft DEFENDER ?

Pour assurer une protection continue et optimale de votre entreprise, Microsoft DEFENDER est géré par nos équipes et reste actif en permanence. Il n'est pas recommandé de le désactiver.

Que faire si je pense qu'un email légitime est bloqué ou a été déplacé par erreur?

Si un email a été déplacé par erreur vers la quarantaine ou que vous souhaitez rendre un email légitime, connectez-vous au **portail de sécurité Microsoft DEFENDER** (page 10), allez ensuite dans **Email et collaboration** puis cliquez sur **Révision**, recherchez à présent le message dans la liste de quarantaine et utilisez l'option "Libération" (détails page 12 et suivantes).

J'ai cliqué sur un lien suspect dans un email, que dois-je faire ?

Si vous avez cliqué sur un lien douteux, déconnectez immédiatement votre appareil d'Internet (en débranchant le câble réseau ou en désactivant le Wi-Fi) et contactez le support F1 GROUPE en urgence. N'essayez pas de résoudre le problème seul.

👉 Créer un ticket de maintenance : **Cliquez ici**

Comment puis-je ajouter des contacts dans la liste des expéditeurs autorisés ?

Pour cela, il faut se rendre dans les paramètres de votre messagerie Outlook, vous avez alors la possibilité de gérer votre listes d'expéditeurs autorisés et votre liste d'expéditeurs bloqués. (Voir comment procéder à la page 8).

Comment signaler un email de phishing ou un spam ?

Dans votre messagerie Outlook, les boutons "Signaler un hameçonnage" ou "Signaler du courrier indésirable" sont disponibles. Cela aide Microsoft DEFENDER à améliorer ses filtres. (Plus d'informations sur la page 9).

Comment contacter le support F1 GROUPE ?

Pour toute question ou assistance concernant Microsoft DEFENDER ou votre infrastructure informatique, le moyen le plus efficace d'obtenir de l'aide et de suivre votre demande est de créer un **ticket de maintenance**.

Pour la création d'un ticket de demande de maintenance : **Cliquez ici**

Pour toutes autres questions, nos équipes sont disponibles au 04 42 93 06 98