



MAILINBLACK 

# L'offre de cybersécurité la plus complète



**U-Cyber 360°**

BY MAILINBLACK

Emails

Web

Mots de passe

Sensibilisation

Formation cyber

**20** ans

d'expertise en  
cybersécurité

**22 000**

organisations protégées  
par Mailinblack

**96%**

de nos clients  
renouvellent



Lauréat **Grand Défi**  
Cybersécurité



Conformité  
**RGPD**



Labellisé **Cybersecurity**  
Made In Europe



Catalogue  
**Tech.Gouv**

# Comment les hackers pénètrent-ils vos défenses informatiques ?

## Emails

- ✗ Incitation au clic sur des liens malveillants
- ✗ Invitation au téléchargement de pièces jointes infectées

90%



des cyberattaques passent par l'email

## Mots de passe

- ✗ Exploitation de mots de passe faibles
- ✗ Utilisation d'identifiants et mots de passe compromis

30%



des infections par ransomware sont dues à des mots de passe compromis

## Collaborateurs

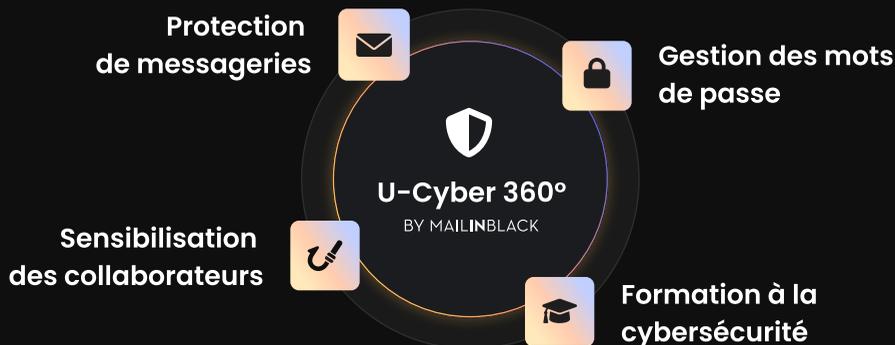
- ✗ Capitalisation sur le manque de connaissances cyber
- ✗ Manipulation via les biais cognitifs

9/10



attaques réussies impliquent une erreur humaine

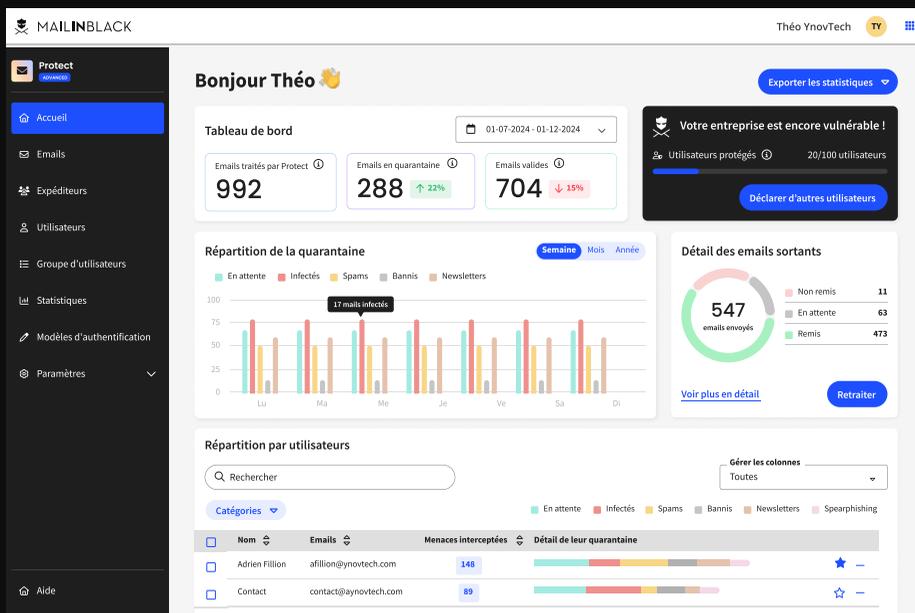
## Maitrisez le cyber-risque humain avec notre offre de cybersécurité complète





**Protect**  
BY MAILINBLACK

# La solution de protection des messageries professionnelles contre les cyberattaques



100% compatible avec votre hébergeur de messagerie



## Activation **CLOUD**

Datacenter sécurisé en France (RGPD)  
Supervision 24/7 & redondance des serveurs  
Aucune installation requise

## Installation **ON PREMISE**

Respect de votre politique d'hébergement  
100 % adaptée à votre infrastructure  
Installation simplifiée

ESSENTIAL

## La solution pour reprendre le contrôle de ses emails en toute simplicité

### Sécurité

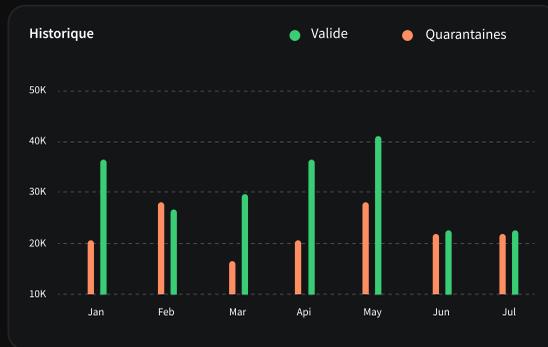
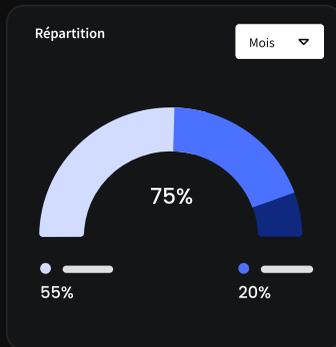
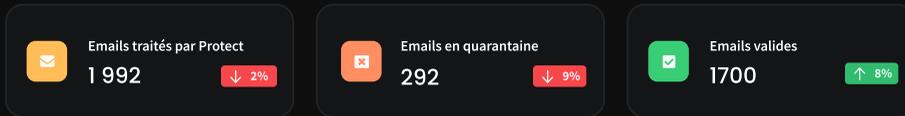
Protection continue de vos données grâce au blocage des spams, ransomwares, phishing, spearphishing et autres malwares.

### Performance

Technologies propriétaires, intelligence artificielle et innovations sont au cœur de notre solution pour une messagerie optimisée.

### Simplicité

Solution clé en main et interface de gestion intuitive, pour une adoption rapide et fluide de la cybersécurité.

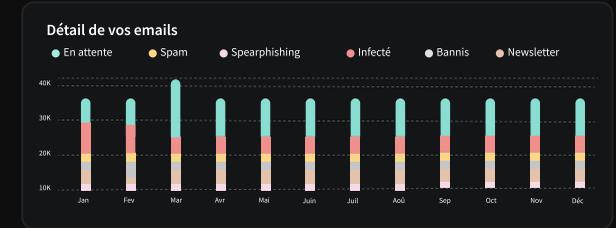


ADVANCED

## La solution conçue pour répondre aux exigences de sécurité les plus élevées

### Plus de puissance

Filtrage renforcé avec analyses heuristiques avancées et double antivirus pour bloquer les menaces sophistiquées.



### Plus de contrôle

Surveillez et gérez votre sécurité avec des alertes en temps réel, des bannières de contrôle des expéditeurs et un suivi détaillé des activités.

Derniers domaines autorisés

Domaines	👤	👤	🗑️
lemonde.fr	👤	👤	🗑️
aceo.com	👤	👤	🗑️
universal.io	👤	👤	🗑️
yahou.com	👤	👤	🗑️

### Plus de flexibilité

Personnalisez vos paramètres de sécurité selon vos besoins : contrôle granulaire, ajustement des règles de filtrage et gestion par groupe.

Derniers emails reçus

Expéditeur	Objet	Date	👤	👤	🗑️
---	---	---	👤	👤	🗑️
---	---	---	👤	👤	🗑️
---	---	---	👤	👤	🗑️
---	---	---	👤	👤	🗑️

### Plus de données

Accédez à des rapports approfondis, des analyses comportementales, et des informations détaillées pour une meilleure visibilité et prise de décision.

### Autonomie renforcée

Notre interface de gestion personnelle et les rapports quotidiens sur les emails stoppés impliquent activement vos collaborateurs dans la protection de votre organisation.

**40** min.

c'est le temps passé à trier nos emails par jour

### Productivité maximisée

Grâce à un filtrage anti-spam très puissant et à une classification automatisée de leurs emails, vos collaborateurs gagnent en moyenne 40 minutes par jour.

### Image de marque améliorée

Notre demande d'authentification renforce l'image sécuritaire de votre organisation, et la fonctionnalité "Droit à la déconnexion" démontre votre engagement envers le bien-être de vos collaborateurs.



### Protection web avancée

Notre solution Secure Link alimentée par notre intelligence artificielle offre une protection avancée en temps réel contre les menaces zero-day et garantie une navigation web sécurisée.

ESSENTIAL

VS

ADVANCED

## Deux niveaux de protection pour s'adapter à vos besoins

### Filtrage et sécurité

Analyse anti-virus .....

Analyse anti-spam .....

Détection de spearphishing .....

Protection contre la fraude par virement .....

Validation DKIM/DMARC .....

Détection des menaces Zero-day par IA .....

Analyse des pièces-jointes .....

Protection des emails sortants .....

Analyse des liens en temps réel .....

Demande d'authentification .....

#### ESSENTIAL

standard



entrant



standard

activable



active

#### ADVANCED

multi-moteurs



avec IA avancée



entrée + sortie



avancée

intégrée



désactivable

### Contrôle et alerting

Statistiques détaillées .....

Suivi des domaines autorisés .....

Alerting activité anormale .....

Prévisualisation emails quarantaine .....

Suivi des activités .....

Enrichissement SIEM .....



via filtrage



individuel



sur dashboard



individuel + groupe



### Autonomie sécurisée de l'utilisateur

Bannière d'avertissement utilisateur .....

Rapport d'emails stoppés .....

Gestion autonome de la quarantaine .....



Disponible avec U-Cyber 360°

La solution complète de Mailinblack pour réduire le cyber-risque humain



**Cyber Coach**  
BY MAILINBLACK

# La solution française de sensibilisation et d'entraînement des collaborateurs face aux cyberattaques

**Bonjour Théo !** Exporter les statistiques

**Cyberculture de votre entreprise**

24% d'utilisateurs piégés par les cyberattaques

1% d'utilisateurs piégés par les attaques clé USB

3% d'utilisateurs piégés par les attaques QR Code

**Comportement de vos utilisateurs**

- Idéal: 45% ont signalé l'email sans se faire piéger
- Neutre: 5% n'ont effectué aucune action
- Pas idéal: 26% ont ouvert l'email mais ne l'ont pas signalé
- Risqué: 24% ont été piégés

**Statistiques** (Vue: 30 derniers jours)

- Toutes Manuelles Automatisées
- 42 Potentielles menaces signalées
- Emails reçus: 145
- Simulations Cyber Coach signalées: 10
- Liens cliqués: 8
- Utilisateurs harçonnés: 3

Les indicateurs d'évolution couvrent les périodes sélectionnées depuis votre dernière connexion.

**Cyberattaque du moment**  
Le sujet ci-dessous a été repéré par notre IA, Mailinblack. Souhaitez-vous lancer une campagne massive sur ce sujet ?

**Paris 2024**  
Non éditable

[Tester mes utilisateurs](#)

## Auditez

Détectez les comportements à risque et ajustez votre stratégie en fonction des vulnérabilités réelles de vos collaborateurs.

## Sensibilisez

Créez des simulations d'attaques ultraréalistes et offrez à vos collaborateurs un accès à des contenus de sensibilisation pertinents.

**Personnalisable**

**Automatisé**

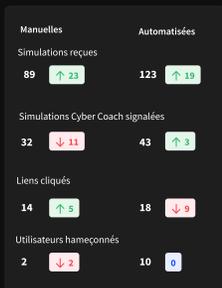
## Engagez

Impliquez vos collaborateurs en leur permettant de signaler instantanément toute menace grâce à notre bouton d'alerte phishing.

**Profitez du catalogue de simulation d'attaques le plus complet du marché**

# Réduisez le risque de vulnérabilités humaines avec Cyber Coach

Nos indicateurs clés vous offrent une visibilité en temps réel des risques cyber, vous permettant d'adapter la formation de vos collaborateurs et de renforcer la sécurité de votre organisation



✓ **Mesurez les risques**

✓ **Analysez les comportements**

✓ **Suivez les progrès**

**100% compatible avec votre hébergeur de messagerie**

Microsoft 365 Exchange OVHcloud G Suite IONOS

Datacenter sécurisé en France (RGPD)  
Supervision 24/7 & redondance des serveurs  
Aucune installation requise



**Optimisez la sécurité de votre organisation en combinant Cyber Coach avec Cyber Academy, notre plateforme de formation à la cybersécurité**



Conformité  
RGPD



Lauréat  
Grand Défi  
Cybersécurité



Catalogue  
Tech.Gouv

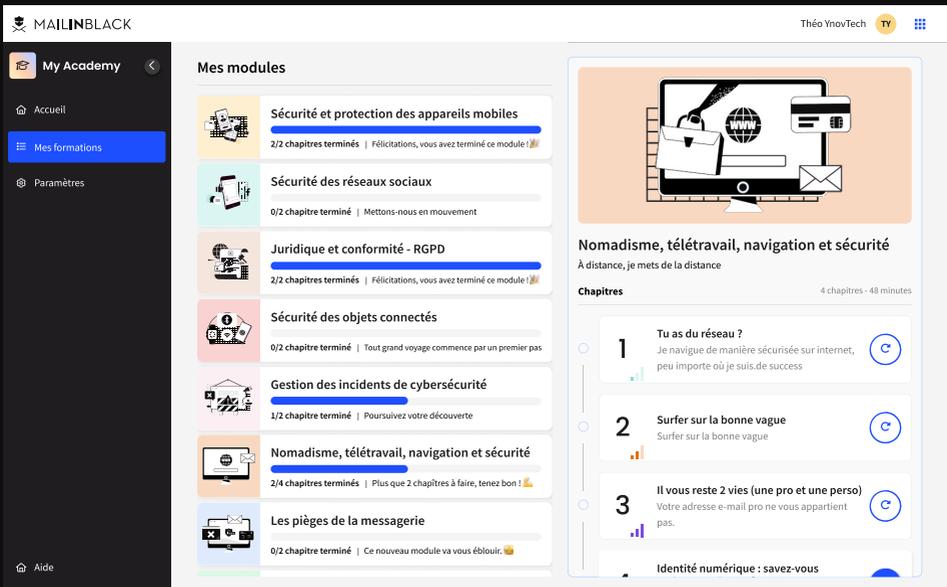


Labelisé  
Cybersecurity  
Made In Europe



**Cyber Academy**  
BY MAILINBLACK

# La plateforme de formation des collaborateurs à la cybersécurité



## 📍 Micro-learning

Optimisez la formation de vos collaborateurs avec des modules de formation adaptés à leur rythme d'apprentissage pour une maîtrise durable des fondamentaux de la cybersécurité.

## 🛡️ Sur mesure

Elevez le niveau de cyberculture de vos collaborateurs et développez leurs compétences tout en garantissant la sécurité de votre organisation grâce à nos formations sur mesure.

## 👍 Gamifié

Plongez vos collaborateurs dans une expérience d'apprentissage ludique et engageante grâce à nos contenus gamifiés et interactifs.

**Programme d'apprentissage conçu par des experts cyber**

# Maximisez l'engagement de vos équipes

## Multi-plateforme

Offrez à vos collaborateurs une plus grande liberté et flexibilité dans leur apprentissage (disponible sur mobile, ordinateur et tablette).

## Contenus captivants

Développez l'intérêt de vos collaborateurs grâce à une variété de contenus captivants qui couvrent à la fois des thèmes professionnels et personnels, disponibles sous format texte et vidéos.



## Formation active

Garantissez le succès de la formation de vos collaborateurs grâce à nos emails de relance automatique les incitant à poursuivre leur formation pour renforcer leurs compétences cyber.

On ne vous oublie pas 📧

Bonjour Théo 🐦

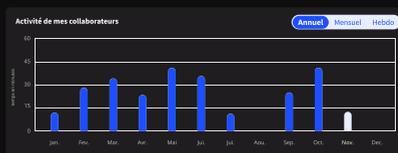
Cela fait quelques temps que nous ne vous avons pas vu sur l'application My Academy... Prenez 5 minutes et découvrez les nouveaux chapitres qui vous attendent !

[Aller sur My Academy](#)

## Valorisation de leurs efforts

Récompensez vos collaborateurs grâce à des badges de succès et des messages de félicitations.

# Et assurez la progression de vos collaborateurs



Grâce à une interface statistiques complète et intuitive



Optimisez la sécurité de votre organisation en combinant **Cyber Academy** avec **Cyber Coach**, notre solution de sensibilisation et d'entraînement des collaborateurs face aux cyberattaques



Conformité  
RGPD



Lauréat  
Grand Défi  
Cybersécurité



Catalogue  
Tech.Gouv



Labellisé  
Cybersecurity  
Made In Europe



**Sikker**  
BY MAILINBLACK

# Le coffre-fort numérique qui sécurise l'ensemble de vos mots de passe

The screenshot shows the Mailinblack Sikker interface. On the left is a navigation sidebar with options like 'Accueil', 'Coffres-forts', 'Tags', 'Gestion d'accès', 'Paramètres', 'Télécharger l'extension', 'Télécharger l'app mobile', 'Verrouiller', 'On vous écoute', and 'Aide'. The main area is titled 'Tous les coffres' and contains a search bar, a 'Recherche avancée' button, and a list of safes. Each safe entry includes a service icon, name, and email address. A detailed view of the 'Adobe' safe is shown on the right, displaying fields for 'Nom d'utilisateur', 'Mot de passe' (masked), 'Code TOTP', 'Lien du site web', 'Coffre' type, 'Tags' (design, outils graphiques, marketing, compte partagé), and a 'Description'.

## Sécurisez

Grâce à un chiffrement de pointe de vos mots de passe et informations sensibles, nous garantissons la protection de vos données confidentielles

## Partagez

Avec les coffres-forts partagés et l'envoi d'identifiants chiffrés par lien sécurisé, assurez une collaboration en toute sérénité au sein de votre organisation.

## Organisez

Vie privée et professionnelle, tous vos mots de passe sont centralisés, organisés par catégories et personnalisables, pour une gestion simplifiée et adaptée à vos besoins.

# Pourquoi choisir Sikker ?



## ✓ Sécurité avancée

Générez instantanément des mots de passe forts pour l'ensemble de vos accès et bénéficiez d'une défense anti-phishing automatique grâce à une détection intelligente des sites frauduleux.

## ✓ Protection de vos secrets

Centralisez et protégez vos mots de passe, notes sensibles, informations confidentielles et données bancaires dans un coffre fort numérique ultra-sécurisé, toujours à portée de main.

## ✓ Fluidité de navigation

Grâce à notre système d'auto-remplissage et l'accès simplifié aux mots de passe via l'application mobile ou l'extension web, optimisez la navigation en ligne de vos collaborateurs tout en sécurisant leurs données.



## ✓ Authentification intégrée

Gérez vos mots de passe et vos codes d'accès à usage unique (TOTP) dans un même outil. Profitez d'une authentification à deux facteurs rapide et centralisée pour renforcer simplement la protection de vos comptes.

## ✓ Gestion simplifiée

Notre tableau de bord intuitif permet aux administrateurs une gestion optimisée des mots de passe grâce à des alertes sur les usages de leurs collaborateurs et permet de garantir le respect des politiques de sécurité pour les coffres-forts partagés.

## ✓ Surveillance active

Sikker travaille en arrière-plan pour surveiller en continu les fuites de données et vous informer en cas de compromission, vous permettant d'agir rapidement pour protéger votre vie numérique.



## Une solution certifiée EN 17640

Certification Program (Type IA)

C'est la garantie d'une protection optimale de vos données sensibles, conforme aux standards de sécurité européens les plus stricts.

### Activation **CLOUD**

Datacenter sécurisé en France (RGPD)  
Supervision 24/7 & redondance des serveurs  
Aucune installation requise

### Installation **ON PREMISE**

Respect de votre politique d'hébergement  
100 % adaptée à votre infrastructure  
Installation simplifiée

# Limitez vos risques grâce à notre cockpit de pilotage

Bonjour Théo

Manager Utilisateur

Protect



Cyber Coach



Cyber Academy



Sikker

Vos statistiques

Vos utilisateurs

Ressources



Alerte cyberattaque

Une vague de cyberattaques est en cours et votre organisation risque d'être impactée.

Prévenir mes employés

Conseils

Votre taux de vulnérabilité est supérieur à la moyenne. Pour éviter cela, Mailblack vous propose quelques conseils.

Voir tout

Protect



Sécurisez vos liens

Activer Secure Link

Cyber Coach



Entrenez vos collaborateurs

Lancer une campagne ciblée

Cyber Academy



Formez vos collaborateurs

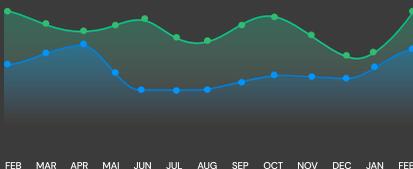
Découvrir les modules

13/02/23 - 13/02/24

Envoyer par email

Télécharger

Vulnérabilité de votre entreprise



FEB MAR APR MAI JUN JUL AUG SEP OCT NOV DEC JAN FEB

Votre organisation Moyenne de votre secteur

Origine des cyberattaques



Monde Votre organisation

Montant économisé

75k € ↑ 23%

Mois le plus critique

Juin

Jour et heure le plus critiques

Vendredi à 14h

Cyberattaques déjouées

86 ↑ 23%

Répartition des emails



Valides	32 %
Spearphishing	12 %
Bannis	11 %
Spams	25 %
Infectés	20 %

Emails signalés



Simulations	65 %
Faux positifs	9 %
Vraies attaques	26 %