4ème édition

BAROMÈTRE CYBER 2026

2025-2026

MAILINBLACK

Sommaire

L'ANNÉE

2025

a marqué un **tournant**

Non pas par le volume d’attaques, mais par **leur nouveau visage**.

Dès janvier, des emails impeccables, écrits par l'IA, ont trompé des organisations entières.

Du phishing 2.0 : crédible, personnalisé, presque indétectable.

Puis les ransomwares sont revenus : 74 groupes actifs, des attaques qui jouent autant sur la technique que sur la psychologie.

> Un clic dans une mairie.
> Une pièce jointe à l'hôpital.
> Un lien en industrie.
> Et tout peut basculer.

Une vérité s'impose :

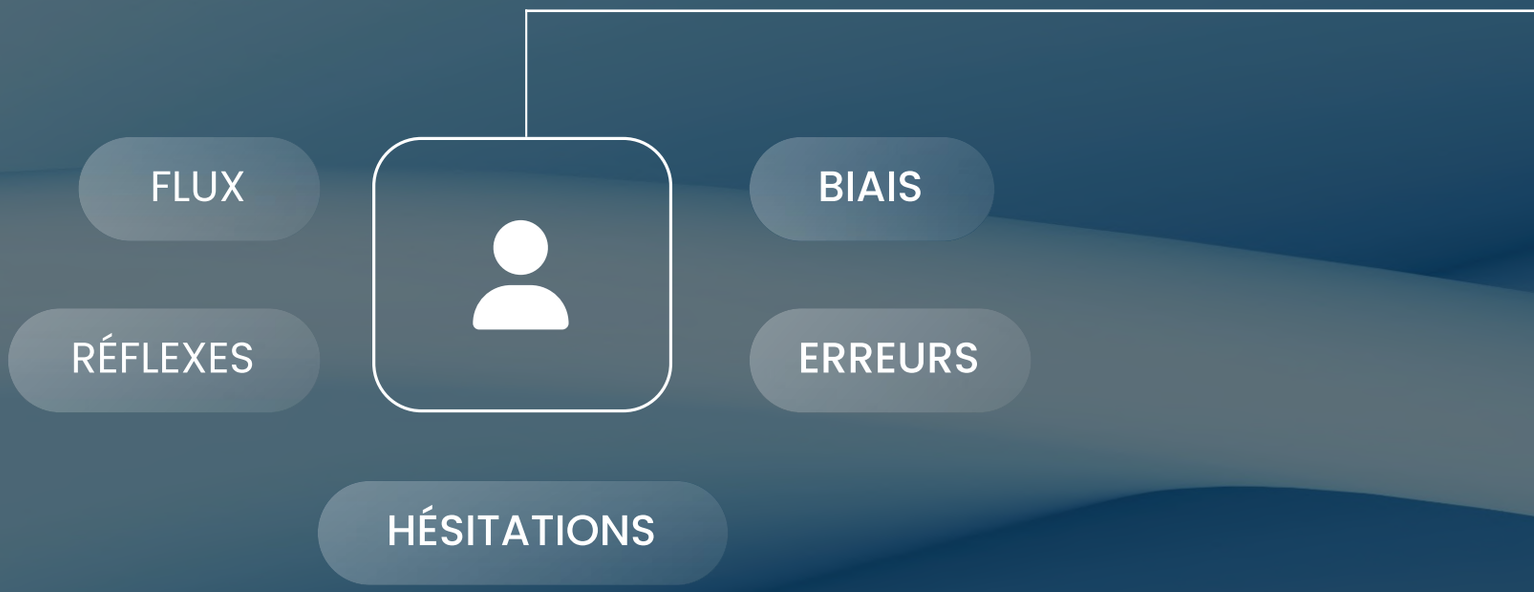
la cible principale n'est plus la machine, c'est l'humain.

Le collaborateur pressé, l'agent de nuit, le commercial en mouvement, le dirigeant tard le soir… Des micro-moments où la vigilance chute.

Protéger les systèmes ne suffit plus.
Il faut protéger l’humain.

Méthodologie

Avec nos solutions Protect, Cyber Coach, Cyber Academy et Sikker, nous observons chaque jour **ce que vivent réellement les collaborateurs** :



Nous analysons des milliards d’emails, des millions d’interactions, des milliers de parcours de formation…
Et au fil de ces données, une évidence s’est imposée :

Il n’existe pas UN utilisateur, mais DES utilisateurs

RYTHME · OUTILS · ATTENTION · FATIGUE

Chacun avec son rythme, ses outils, ses moments d’attention ou de fatigue, ses risques propres et donc sa propre exposition.

C’est cette réalité que raconte notre baromètre.

Non pas une moyenne, mais **quatre personas**, **quatre histoires**, **quatre manières de travailler**… et autant de manières d’être **ciblé**.

Parce que pour réduire le cyber-risque humain, il faut d’abord comprendre l’HUMAIN.

NOMBRE D'EMAILS **ANALYSÉS**

1 918 000 000

un milliard neuf cent dix-huit millions

Ce chiffre reflète le **périmètre d'analyse retenu** cette année, l'analyse s'étant concentrée sur une sélection d'emails en lien avec notre angle d'analyse.

NOMBRE D'EMAILS **MALVEILLANTS**

54 900 000

cinquante-quatre millions neuf cent mille

2,86%

Black

Emails bannis, explicitement malveillants, incluant des messages prédictifs et/ou du spam.

Spearphishing

Attaques ciblées et personnalisées.

Virus

Pièces jointes infectées (malwares, ransomwares).

NOMBRE D'EMAILS **INDÉSIRABLES**

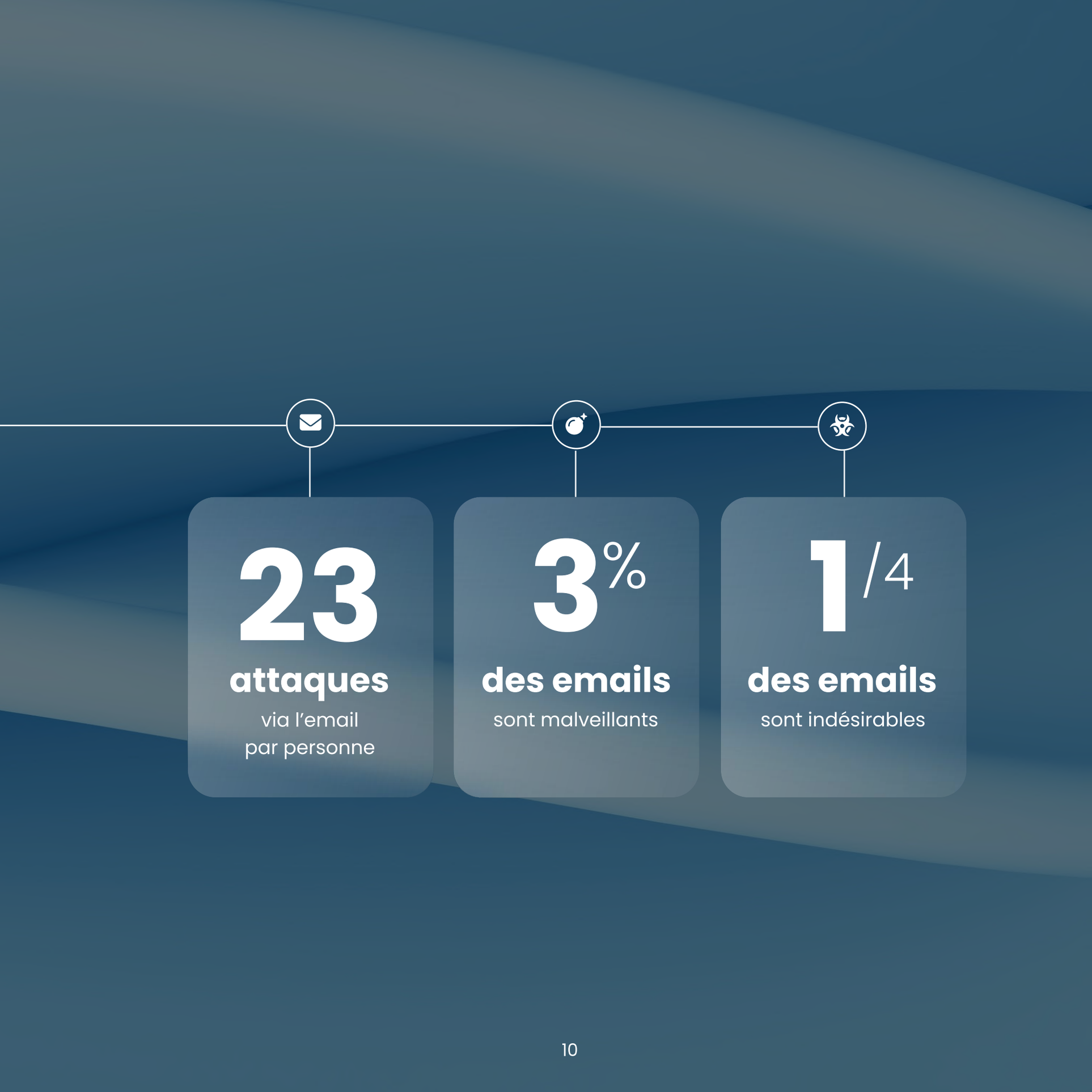
476 400 000

quatre cent soixante-seize millions quatre cent mille

24,8%

Spam

Indésirables non dangereux,
mais perturbateurs.


23
attaques
via l'email
par personne
3%
des emails
sont malveillants
1/4
des emails
sont indésirables

Les solutions Mailinblack

Il est important de connaître nos solutions, car l’ensemble des analyses et des données que nous partageons s’appuient directement sur les informations qu'elles collectent et traitent.

Elles constituent le socle de notre compréhension des comportements, des expositions et des risques observés.


MAILINBLACK
Protect
ADVANCED
Accueil
Emails
Expéditeurs
Utilisateurs
Groupe d'utilisateurs
Statistiques
Modèles d'authentification
Paramètres
Aide
Théo YnovTech
TY
Exporter les statistiques
Bonjour Théo 👋
01-07-2024 - 01-12-2024
Tableau de bord
Emails traités par Protect
992
Emails en quarantaine
288
22%
Emails valides
704
15%
Votre entreprise est encore vulnérable !
Utilisateurs protégés
20/100 utilisateurs
Déclarer d'autres utilisateurs
Détail des emails sortants
547
emails envoyés
Non remis 11
En attente 63
Remis 473
Retraiter
Voir plus en détail
Répartition de la quarantaine
Semaine
Mois
Année
En attente
Infectés
Spams
Bannis
Newsletters
17 mails infectés
100
75
50
25
0
Lu
Ma
Me
Je
Ve
Sa
Di
Répartition par utilisateurs
Rechercher
Gérer les colonnes
Toutes
Catégories
Nom
Emails
Menaces interceptées
Détail de leur quarantaine
Spearphishing
Adrien Fillion
afillion@ynovtech.com
148
Contact
contact@aynovtech.com
89
MacBook Pro

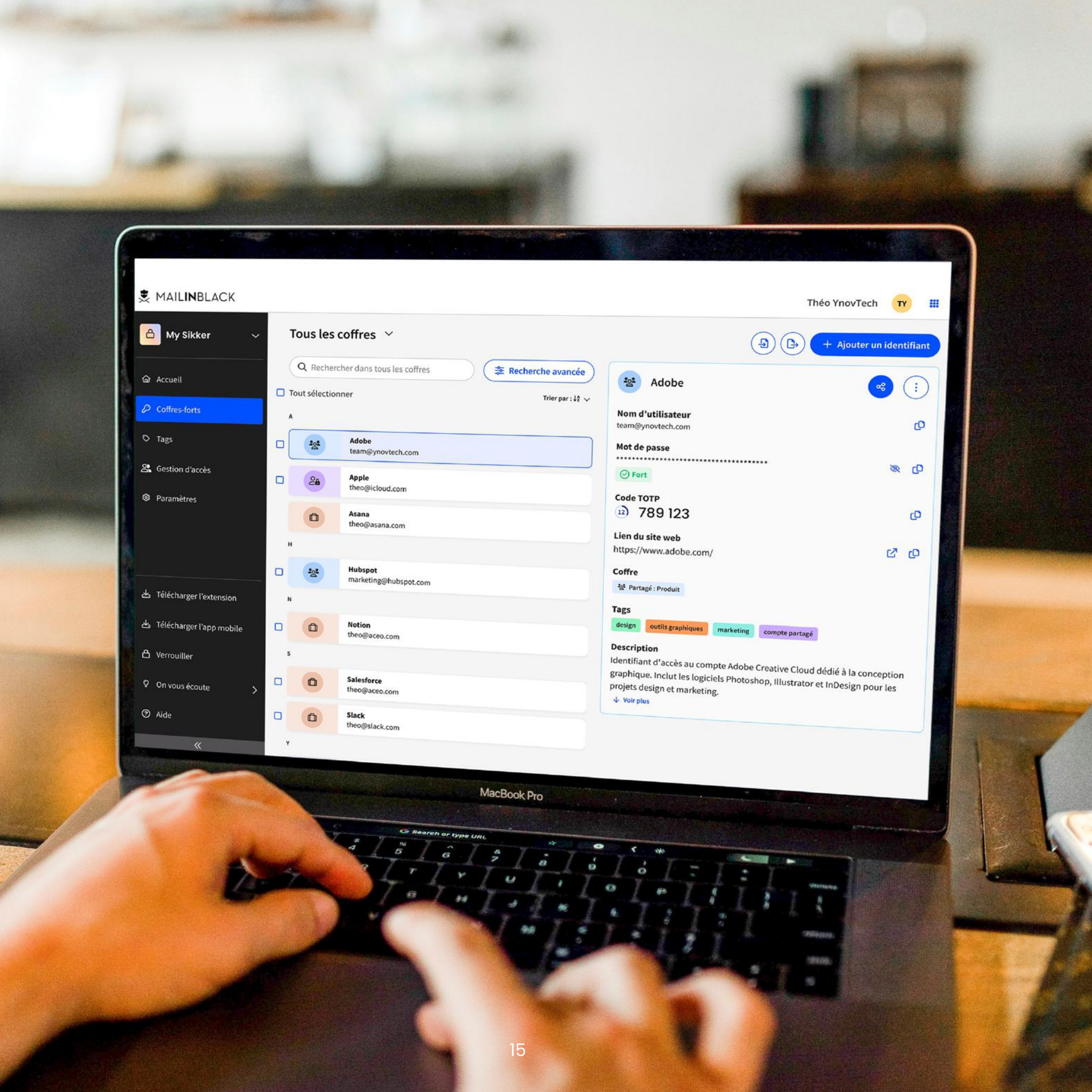
Protect

Protection des messageries

Protect utilise des **technologies de pointe** associées à l'**intelligence artificielle** pour sécuriser les organisations (entreprises, établissements de santé, administrations publiques) contre toutes formes de **cyberattaques véhiculées par email** (phishing, spearphishing, ransomware, etc.).

Elle **dépollue également les messageries** en éliminant les emails indésirables, tels que les **spams** et les **newsletters**.

En savoir plus


MAILINBLACK
Théo YnovTech
TY
My Sikker
Accueil
Coffres-forts
Tags
Gestion d'accès
Paramètres
Télécharger l'extension
Télécharger l'app mobile
Verrouiller
On vous écoute
Aide
Tous les coffres
Ajouter un identifiant
Rechercher dans tous les coffres
Recherche avancée
Tout sélectionner
Trier par :
A
Adobe
team@ynovtech.com
Apple
theo@icloud.com
Asana
theo@asana.com
H
Hubspot
marketing@hubspot.com
N
Notion
theo@aceo.com
S
Salesforce
theo@aceo.com
Slack
theo@slack.com
Y
Adobe
Nom d'utilisateur
team@ynovtech.com
Mot de passe
Fort
Code TOTP
789 123
Lien du site web
https://www.adobe.com/
Coffre
Partagé : Produit
Tags
design
outils graphiques
marketing
compte partagé
Description
Identifiant d'accès au compte Adobe Creative Cloud dédié à la conception graphique. Inclut les logiciels Photoshop, Illustrator et InDesign pour les projets design et marketing.
Voir plus
MacBook Pro

Sikker

Gestion des mots de passe

Sikker réinvente la sécurité numérique en alliant **simplicité et protection** sans compromis. Ce gestionnaire de mots de passe professionnel propose une **gestion centralisée des accès et des outils** de sécurité avancés, assurant une sérénité totale aux utilisateurs.

Les collaborateurs peuvent **générer des mots de passe complexes** sans effort, Sikker prenant en charge leur mémorisation et permettant leur utilisation directement dans les outils.

En savoir plus


Cyber Coach
Accueil
Programme automatisé
Simulations manuelles
Sensibilisation
Paramètres
Bonjour Théo !
Cyberculture de votre entreprise
10%
Vulnérabilité 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
Exporter les statistiques
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
Toutes
Manuelles
Automatisées
Vue
30 derniers jours
Emails reçus
145
42 Potentielles menaces signalées
Simulations Cyber Coach signalées
10
Cyberattaque du moment
Le sujet ci-dessous a été reperé par notre IA Mailinblack.
Souhaitez-vous lancer une campagne massive sur ce sujet ?

Cyber Coach

Simulation de cyberattaques

Cyber Coach est la solution de **sensibilisation et d'entraînement à la cybersécurité** la plus complète du marché. Elle aide les organisations à **réduire les risques liés aux erreurs humaines**, responsables de 90% des cyberattaques.

Grâce à des **simulations d'attaques variées** (phishing, ransomware, BitB, spearphishing, clé USB, QR Code), elle **entraîne** les collaborateurs de manière **automatisée et personnalisée**, en ciblant leurs vulnérabilités réelles.

En savoir plus


MAILINBLACK
My Academy
Accueil
Mes formations
Paramètres
Aide
Mes modules
De l'ordre naît... la cyberprotection
1/4 chapitre terminé | Souvenez-vous de tout
Sécuriser son poste de travail
0/3 chapitre terminé | C'est le moment !
Nomadisme, télétravail, navigation et sécurité
3/4 chapitres terminés | Un petit dernier pour la route
Les pièges de la messagerie
Félicitations, vous avez terminé les 2 chapitres de ce module ! 🎉
Mobilité et sécurité
0/3 chapitre terminé | C'est le moment !
Authentification dès l'ouverture de son appareil
3/4 chapitres terminés | Dernière ligne droite
Gérer vos données à caractère personnel
0/6 chapitre terminé | Commencez maintenant
Voir la vidéo
De l'ordre naît... la cyberprotection
Faire place nette !
Chapitres
1 Prends garde à tes sauvegardes
Vos données sont convoitées par les hackers... Mettez-les en sécurité !
2 Chacun ses droits, chacun ses datas
Données personnelles hautement sensibles.
3 De l'ordre c'est un ordre !
Personne ne doit pouvoir accéder à vos données, à vos fichiers et à vos dossiers.
4 Fermez la porte en sortant, merci !
Menaces sur vos terminaux fixes et mobiles.
MacBook Pro

Cyber Academy

Formation à la cybersécurité

Cyber Academy est une **plateforme e-learning** qui a pour objectif de contribuer à renforcer la cybersécurité des organisations en sensibilisant et en **responsabilisant leurs collaborateurs** grâce à la formation.

Son approche **interactive et ludique** permet aux collaborateurs de **se former à leur propre rythme**, tout en offrant un **suivi de progression**.

En savoir plus

Le cyberscore humain Mailinblack

Mailinblack **mesure le risque,** pas seulement au niveau **technique**, mais au niveau **humain**, via un cyberscore composé de **3 piliers** :

EXPOSITION **COMPORTEMENT** **CYBERCULTURE**

Chaque **utilisateur** obtient un niveau de risque basé sur ces trois dimensions :

FAIBLE MOYEN ÉLEVÉ

Chaque persona reçoit un score global :

RISQUE FAIBLE — RISQUE MOYEN — RISQUE ÉLEVÉ

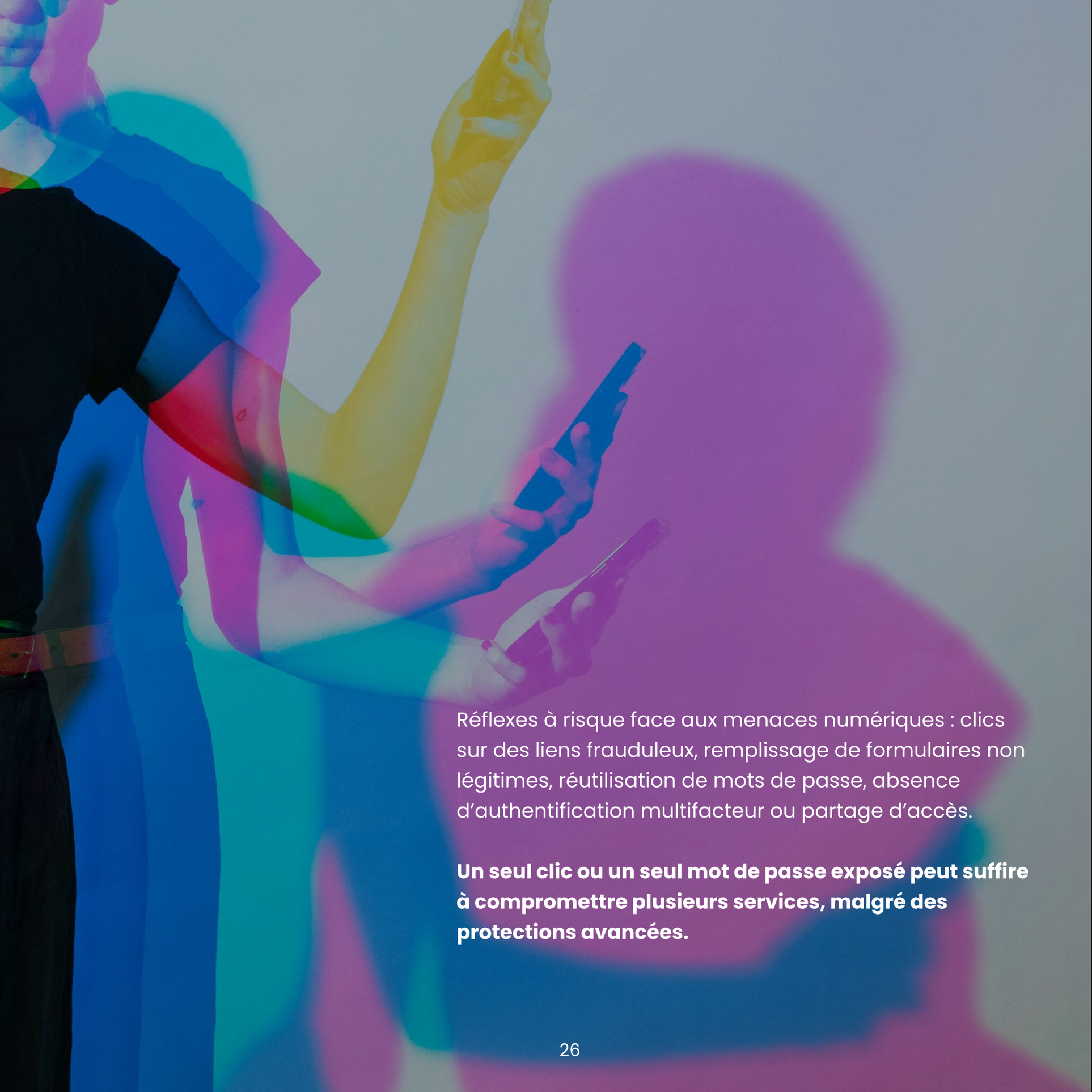
Ce qui permet de visualiser immédiatement les profils les plus vulnérables.

Exposition

Volume et sensibilité des emails reçus, outils utilisés (SaaS critiques), contexte (télétravail, Wi-Fi public, PC perso…).

Plus l’exposition augmente, plus la vulnérabilité grimpe, même si les comportements sont bons. Par exemple, un collaborateur très vigilant peut devenir une cible prioritaire si son exposition est élevée.

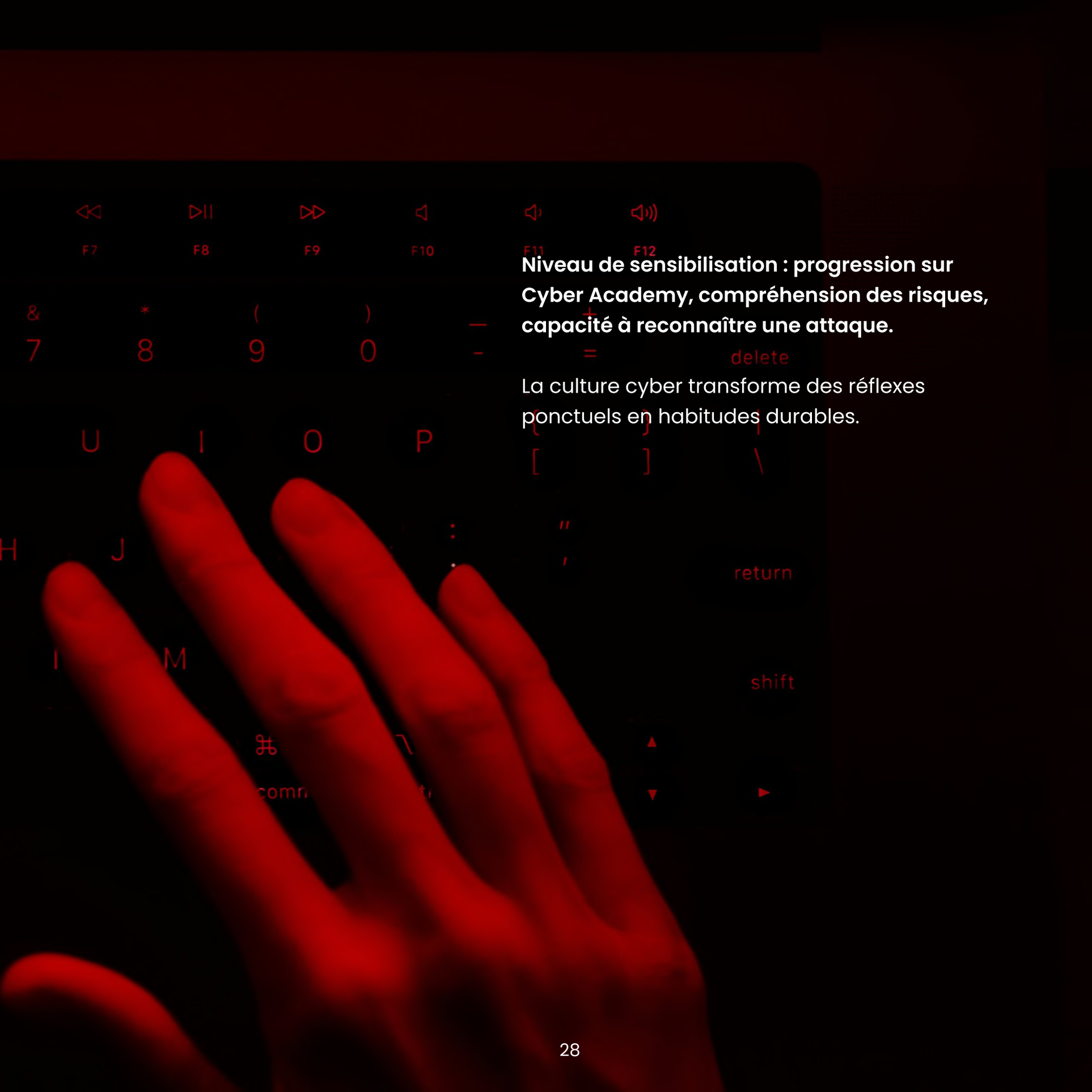
Comportement



Réflexes à risque face aux menaces numériques : clics sur des liens frauduleux, remplissage de formulaires non légitimes, réutilisation de mots de passe, absence d'authentification multifacteur ou partage d'accès.

Un seul clic ou un seul mot de passe exposé peut suffire à compromettre plusieurs services, malgré des protections avancées.


Cyberculture
esc
F1
F2
F3
F4
F5
F6
tab
Q
W
E
R
T
caps lock
A
S
G
shift
Z
B
fn



Niveau de sensibilisation : progression sur Cyber Academy, compréhension des risques, capacité à reconnaître une attaque.

La culture cyber transforme des réflexes ponctuels en habitudes durables.

Sur cette base, nous avons observé 4 grandes familles d’utilisateurs.

Ils n’ont ni les mêmes outils, ni les mêmes volumes et types d’emails reçus, ni les mêmes biais cognitifs.

Mais tous contribuent au risque cyber humain de l’organisation.

Lexique

Avant d’entrer dans l’analyse détaillée, il est important de partager un cadre de lecture commun. Certains indicateurs et mécanismes cognitifs seront mobilisés tout au long de la présentation ; les connaître permet de mieux comprendre les comportements observés et d’interpréter correctement les résultats.

BRUIT DE FOND

Tout ce qui est présent en arrière-plan mais qui n'est pas l'information principale. Les spams, alertes inutiles, pubs, etc. créent un flot constant de nuisances qui noient les vrais messages importants.

En clair, le bruit de fond est ce qui encombre, distrait ou pollue l'information utile.

TAUX DE FILL

Pourcentage d'utilisateurs qui, après avoir cliqué, **vont encore plus loin dans l'attaque**. Ils remplissent un formulaire, fournissent des informations, ou valident une action.

C'est l'indicateur le plus critique car il **mesure la profondeur de la compromission comportementale**. On peut le voir comme le taux de conversion d'un clic en compromission.

TAUX DE REPORT

Pourcentage d’utilisateurs qui **signalent la simulation de cyberattaque** via le bouton de report intégré.

C’est un indicateur de maturité : plus le report est haut, plus les utilisateurs développent un réflexe sain d’alerte.

Les biais cognitifs sont des **leviers psychologiques puissants** exploités par les attaquants pour **manipuler les utilisateurs** et **déclencher des comportements impulsifs**, comme cliquer sur un lien ou divulguer des informations sensibles.

BIAIS DE LA CURIOSITÉ

La curiosité humaine naît de la perception d'un vide dans notre savoir : lorsqu'une information manque, un besoin presque compulsif de la combler s'installe.

Les cyberattaquants exploitent ce mécanisme à l'aide d'appâts informationnels : document interne, message vocal, fichier « réservé ». Le clic devient alors quasi réflexe.

Un objet intriguant ou présenté comme confidentiel capte immédiatement l'attention.

Biais le plus puissant : le clic est avant tout motivé par l'envie de voir, notamment sur les pièces jointes et les liens.

BIAIS DE L'URGENCE

Face à une situation présentée comme critique ou immédiate, le cerveau cherche à agir vite plutôt qu'à vérifier.

Les messages évoquant une suspension de compte, un paiement à valider ou une action « à effectuer immédiatement » créent un stress et un effet tunnel : l'attention se focalise sur la menace, au détriment des contrôles habituels. Sous pression, le cerveau passe en mode automatique.

Le clic ou la validation devient impulsif, c'est le biais le plus exploité dans les attaques de type phishing et BEC.

BIAIS D’AUTORITÉ

Nous avons naturellement tendance à obéir aux figures perçues comme légitimes : direction, banque, administration.

Un message qui imite les codes de l’autorité (ton formel, vocabulaire institutionnel, signature crédible, etc.) réduit fortement l’esprit critique. Lorsqu’un « ordre » semble émaner d’un dirigeant ou d’un organisme officiel, le doute s’efface.

Combiné à l’urgence, ce biais devient particulièrement redoutable.

BIAIS DE L’APPÂT DU GAIN

La promesse d’un avantage (remboursement, bon d’achat, prime) active immédiatement le circuit de la récompense, un mécanisme cérébral qui pousse à rechercher le gain.

Ce biais affaiblit le raisonnement critique, surtout lorsque le gain paraît simple ou limité dans le temps.

Même en contexte professionnel, un message évoquant une prime, un remboursement ou un avantage social peut suffire à faire baisser la vigilance.

ANALYSE DU

PERSONA N°1

Collaborateur.rice transverse

ADMINISTRATIF

RH

COMPTA

HABITUDES & USAGES

Travaille principalement sur ordinateur, mais consulte régulièrement ses mails sur mobile (pauses, déplacements internes)

Forte utilisation d’outils bureautiques + SaaS (signature électronique, SIRH, portails RH).

MOMENTS DE FORMATION

13h → 15h

Connexion en début d’après-midi

Motivation déclenchée après :

- **un incident signalé**
- **une simulation d’attaque Cyber Coach**

ATTAQUES TYPES

SPAM

VIRUS

DOCUMENTS RH

BRUIT DE FOND

- CV
- RIB
- OneDrive
- DocuSign

EXPOSITION

1 210

EMAILS PAR UTILISATEUR
EN MOYENNE PAR AN

15,37%

dont 186 emails malveillants

PERSONA LE PLUS EXPOSÉ

Emails types

- CV
- RIB
- CONTRATS
- PIÈCES JOINTES

Ce persona reçoit principalement des **ransomwares**.

COMPORTEMENT & BIAIS

32%

D'UTILISATEURS ENTRAÎNÉS

RISQUE ÉLEVÉ

Pour les utilisateurs avec moins de 5 simulations de cyberattaque :

- TAUX DE CLIC : **11,8%**
- TAUX DE FILL : **9,6%**
- TAUX DE REPORT : **3%**

BIAIS EXPLOITÉ

URGENCE

“je dois agir tout de suite”

C’est le biais le plus exploité.

Un message qui annonce une suspension de compte ou une action immédiate crée du stress et un effet tunnel : on se focalise sur la menace et on perd nos réflexes de vérification.

Sous pression, le cerveau passe en mode automatique, et le clic devient impulsif.

MOTS DE PASSE

+ DE MOTS DE PASSE FAIBLES QUE FORTS

RISQUE ÉLEVÉ

Mais les **mots de passe forts progressent 2× plus vite** que les faibles

IMPACT POSITIF DE L'OUTIL

26%

DES UTILISATEURS ONT UN **COFFRE PRO À 0 MOT DE PASSE**

RISQUE ÉLEVÉ

CYBERCULTURE

64%

taux de progression moyen

MEILLEUR TAUX

Après la formation
Cyber Academy

TAUX DE FILL : **-33%**

TAUX DE REPORT

CYBERSCORE

EXPOSITION ÉLEVÉE | COMPORTEMENT MOYEN | BONNE CYBERCULTURE

Malgré une forte exposition et une prudence modérée, le niveau de formation est globalement solide. L'impact est direct : chaque module suivi réduit le nombre de formulaires malveillants complétés.

ACTIONS POUR AMÉLIORER LA COUVERTURE

Protect

- Durcir filtres anti-spam/virus pour réduire le bruit et la fatigue de vigilance

Cyber Coach

- Envoyer des scénarios ciblant la curiosité (CV, documents RH, faux Drive/SharePoint)

Cyber Academy

- Maintenir un socle de formation large
- Insister sur la vérification des destinataires (documents RH envoyés au mauvais contact).

Sikker

- Inciter à remplir le coffre pro
- Valoriser les mots de passe forts (feedback positif dans l'app)

ANALYSE DU

PERSONA N°2

Agent de terrain en structure publique

HÔPITAL

COLLECTIVITÉ

RÉGIE

LABORATOIRE

HABITUDES & USAGES

Très peu sur PC : usage ponctuel d'un poste partagé.

Forte dépendance au mobile pro/ perso pour lire des notifications rapides.

Horaires très variables : travail en rotations, équipes, nuits.

FENÊTRES D’ATTAQUE

La nuit

Les attaquants exploitent la fatigue et l’urgence pour augmenter leur taux de succès.

MOMENTS DE FORMATION

Avant ou après leur service

Souvent en session imposée

ATTAQUES TYPES

RANSOMWARE

Top 1 des attaques sur ce persona

DOCUMENTS RH

- Faux portails RH
- Faux bulletins de paie

PDF INTERNES

avec macros piégées

EXPOSITION

715

EMAILS PAR UTILISATEUR
EN MOYENNE PAR AN

15,1%

dont 108 emails malveillants

RISQUE ÉLEVÉ

Utilisation du numérique

PORTAIL RH

PAIE

MAILS INTERNES

RISQUE ÉLEVÉ

Persona rêvé pour les hackeurs car **mauvaise connaissance des outils numériques**

COMPORTEMENT & BIAIS

53%

D'UTILISATEURS ENTRAÎNÉS

RISQUE FAIBLE

Le secteur de la santé attire les cybercriminels en raison de la **valeur des données** qu'il gère, notamment les dossiers médicaux prisés pour les fraudes et extorsions. C'est pourquoi les enjeux liés à la **formation** et à la **sensibilisation** à la cybersécurité sont **particulièrement importants** pour ce persona.

Pour les utilisateurs avec moins de 5 simulations de cyberattaque :

- TAUX DE CLIC : **10,3%**
- TAUX DE FILL : **3,5%**
- TAUX DE REPORT : **0,15%**

COMPORTEMENT FACE AUX ATTAQUES

20%

de ransomware reçus de plus que le phishing

3 fois +

de clics sur le phishing que sur le ransomware

2 fois +

de conversions sur le ransomware quand ils cliquent

BIAIS EXPLOITÉ

AUTORITÉ & STRESS

“c’est une consigne officielle, il faut agir”

Dans le secteur santé et public, les interactions sont rares. **Mais lorsqu’un clic survient, il est le plus souvent lié au stress et à la pression hiérarchique.**

Les messages perçus comme officiels (consignes, procédures, urgences) activent le biais d’autorité. Le ton institutionnel et l’urgence réduisent l’esprit critique et favorisent une action rapide, parfois sans vérification.

MOTS DE PASSE

2 fois +

de mots de passe faibles que forts

RISQUE ÉLEVÉ

Après adoption de l'outil, **la part de mots de passe faibles baisse**

RISQUE FAIBLE

CYBERCULTURE

63%

taux de progression moyen

RISQUE FAIBLE

Les sujets activables pour eux sont très concrets :

- MOT DE PASSE
- FAUX PORTAILS
- RANSOMWARE

CYBERSCORE

EXPOSITION MOYENNE

COMPORTEMENT FAIBLE

FAIBLE CYBERCULTURE

Bien que ce persona soit connu pour son retard en culture cyber et l'obsolescence des systèmes informatiques qu'il utilise, notre analyse montre qu'une sensibilisation et une formation adaptées à la cybersécurité permettent de réduire significativement son exposition aux cyberattaques ; toutefois, sa cyberculture reste limitée : peu exposé aux outils numériques au quotidien du fait d'une activité majoritairement sur le terrain, il demeure particulièrement vulnérable sur les sujets liés aux mots de passe et au partage d'accès, notamment dans les espaces publics.

ACTIONS POUR AMÉLIORER LA COUVERTURE

Cyber Coach

- Insister sur les scénarios ransomware (les plus dangereux)
- Travailler le réflexe “je signale / je demande au support”

Cyber Academy

- Chapitres courts imposé et contextualisé au quotidien (badge, poste partagé, portail RH)

Sikker

- Proposer un accompagnement ultra-simplifié, sans jargon
- Favoriser l’usage de mots de passe forts générés automatiquement

ANALYSE DU

PERSONA N°3

Commercial.e

HABITUDES & USAGES

Usage majoritairement mobile, surtout en **situation de mobilité** : train, déplacements, hôtel, coworking, Wi-Fi public.

PC utilisé pour les devis et le CRM, mais les **emails** sont principalement consultés sur smartphone.

FENÊTRES D’ATTAQUE

Fin de journée

Fin de journée (18h–19h) : une fenêtre d’attaque propice au **spearphishing,** marquée par la fatigue et la mobilité.

MOMENTS DE FORMATION

Entre 2 rdv

Connexions irrégulières, souvent entre deux rendez-vous, à l'heure du déjeuner ou le soir dans le train.

ATTAQUES TYPES

SPEARPHISHING

FRAUDES FINANCIÈRES

OUTILS MÉTIERS

- Fausse connexion CRM
- Signature électronique

9,7

ATTAQUES PAR UTILISATEUR

RISQUE ÉLEVÉ

- Fraudes au RIB
- Faux bons de commande
- Paiement urgent

10,5% de plus

que la moyenne de nos autres personas

EXPOSITION

2 468

EMAILS PAR UTILISATEUR
EN MOYENNE
PAR AN

PLUS GROS FLUX

15,1%

dont 372 emails malveillants

RISQUE ÉLEVÉ

NIVEAU D'EXPOSITION

10,5% de +
de spearphishing que certains autres profils

3,75 fois +
de mails que la moyenne

4,25 fois +
de virus

COMPORTEMENT & BIAIS

45%

D'UTILISATEURS ENTRAÎNÉS

RISQUE MOYEN

Pour les utilisateurs avec moins de 5 simulations de cyberattaque :

- TAUX DE CLIC : **20,9%**
- TAUX DE FILL : **17,3%**
- TAUX DE REPORT : **4,8%**

BIAIS EXPLOITÉ

CURIOSITÉ & RÉACTIVITÉ

“Je regarde, je traite, j’avance”

Chez ce profil, la curiosité est le biais dominant, les autres restant à un niveau comparable. Les actions s’enchaînent rapidement : ouverture, clic, parfois même remplissage. Cette dynamique est cohérente avec un métier fondé sur la réactivité, la relation client et la pression du résultat.

L’envie de comprendre rapidement “de quoi il s’agit” prime, avant toute analyse approfondie du message.

MOTS DE PASSE

Tri actif des mots de passe

RISQUE FAIBLE

Gestion intensive de plusieurs outils (CRM, e-signature, etc.).

RISQUE ÉLEVÉ

Après adoption, **la part de mots de passe forts augmente**

RISQUE FAIBLE

CYBERCULTURE

55%

taux de progression moyen

RISQUE ÉLEVÉ

Alors qu'ils ont accès à la formation la plus complète

CYBERSCORE

EXPOSITION ÉLEVÉE

COMPORTEMENT FAIBLE

FAIBLE CYBERCULTURE

Fortement sollicité par les emails et les attaques ciblées, avec un taux de clic élevé et une formation insuffisante, ce persona constitue le niveau de risque le plus élevé.

ACTIONS POUR AMÉLIORER LA COUVERTURE

Protect

- Mettre en avant les statistiques de spearphishing bloqué pour ce profil
- Mettre en place une politique stricte sur les pièces jointes et liens de paiement

Cyber Coach

- Cibler la curiosité (faux bons de commande, urgences de fin de mois, etc.)
- Activer des scénarios de mobilité (Wi-Fi public, smartphone)

Cyber Academy

- Déployer un parcours “Commercial en mobilité” : court, concret, obligatoire
- Prioriser les menaces critiques : fraude au RIB, faux clients, BEC

Sikker

- Accompagner la gestion de nombreux accès multi-outils
- Imposer/recommander fortement la génération automatique de mots de passe forts

ANALYSE DU

PERSONA N°4

Dirigeant·e / COMEX

HABITUDES & USAGES

Les dirigeants naviguent entre mobile, **PC et tablette**, ce qui multiplie les points d'exposition et fait d'eux une cible prioritaire.

Ils doivent **traiter rapidement un volume élevé de documents**, avec des validations fréquentes et des accès critiques à sécuriser.

FENÊTRES D’ATTAQUE

20h → 22h

Tard le soir, les attaquants exploitent les moments où les dirigeants **valident plus rapidement**.

MOMENTS DE FORMATION

Le soir, en déplacement ou juste après un incident

TAUX DE FILL : **DIVISÉ PAR 10**

Impact majeur : le taux de remplissage des formulaires malveillants est divisé par 10 après la formation.

ATTAQUES TYPES

BEC

VALIDATION FALSIFIÉE

RANSOMWARE

Business Email Compromise

- Usurpation interne
- Usurpation partenaire

- Signature électronique
- Documents RH
- Documents financiers

EXPOSITION

2 209

EMAILS PAR UTILISATEUR
EN MOYENNE PAR AN

TRÈS GROS FLUX

12,5%

dont 276 emails malveillants

RISQUE ÉLEVÉ

Beaucoup de virus et attaques ciblées

BEC

IMPOSTURE DE PARTENAIRES

Les emails ont souvent un impact financier ou RH direct.

COMPORTEMENT & BIAIS

32%

D'UTILISATEURS ENTRAÎNÉS

RISQUE ÉLEVÉ

Pour les utilisateurs avec moins de 5 simulations de cyberattaque :

- TAUX DE CLIC : **9,1%**
- TAUX DE FILL : **6,4%**
- TAUX DE REPORT : **3,2%**

COMPORTEMENT FACE AUX ATTAQUES

PHISHING

TAUX DE CLIC : **PLUS ÉLEVÉ**

RANSOMWARE

TAUX DE FILL : **PLUS ÉLEVÉ**

26%

des utilisateurs tombent dans le panneau

RISQUE ÉLEVÉ

BIAIS EXPLOITÉ

CURIOSITÉ

“Je veux comprendre / vérifier”

C’est un biais fortement exploité chez les dirigeants. Un message évoquant un sujet sensible ou stratégique (résultats, acquisition, litige, document confidentiel) attise la curiosité et incite à ouvrir rapidement, souvent sans vérification approfondie.

Sous pression et par réflexe de contrôle, le dirigeant cherche à comprendre avant de douter, ce qui augmente le risque de clic ou de validation inappropriée.

MOTS DE PASSE

Persona qui **renforce le plus ses mots de passe au fil du temps**.

RISQUE FAIBLE

Gestion d'un **volume important d'accès critiques**.

RISQUE ÉLEVÉ

CYBERCULTURE

Accès plus restreint à la formation par manque de temps

59%

de taux de progression moyen

RISQUE MOYEN

Pour les dirigeants ayant fini leur formation

taux de fill divisé par 10 en simulation

RISQUE FAIBLE

CYBERSCORE

EXPOSITION ÉLEVÉE — COMPORTEMENT BON — BONNE CYBERCULTURE

Chez les dirigeants, le risque ne vient pas d'un mauvais comportement, mais de décisions prises sous pression : une heure de formation pour un COMEX permet de sécuriser des dizaines de décisions.

ACTIONS POUR AMÉLIORER LA COUVERTURE

Protect

- Protéger les flux sensibles (RH, financiers, prestataires)
- Sécuriser les validations et signatures externes

Cyber Coach & Cyber Academy

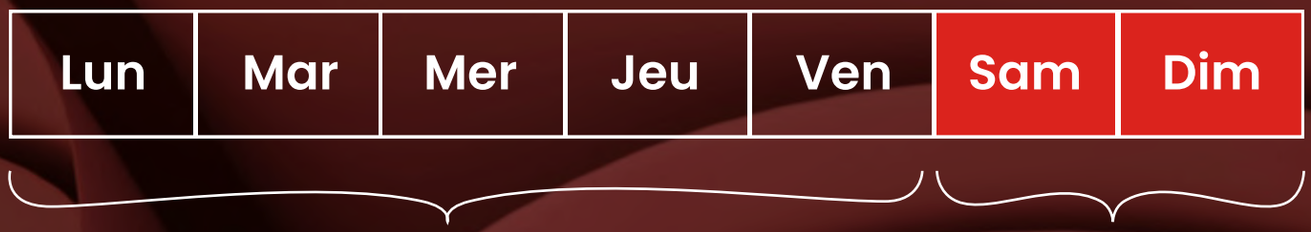
- Proposer des formats ultra courts, orientés décisions et délégations
- Prioriser les modules clés : BEC, fraude au président, validation de paiement

Sikker

- Généraliser le MFA sur tous les accès
- Encadrer la délégation des accès pour garantir la sécurité

Pics d’activité et **temporalité** des attaques


pic d'activité
JANVIER
Dim Lun Mar Mer Jeu Ven Sam
1 2 3
4 5 6 7 8 9 10
11 12 13 14 15 16 17
18 19 20 21 22 23 24
25 26 27 28 29 30 31
FÉVRIER
Dim Lun Mar Mer Jeu Ven Sam
1 2 3 4 5 6 7
8 9 10 11 12 13 14
15 16 17 18 19 20 21
22 23 24 25 26 27 28
MARS
Dim Lun Mar Mer Jeu Ven Sam
1 2 3 4 5 6 7
8 9 10 11 12 13 14
15 16 17 18 19 20 21
22 23 24 25 26 27 28
29 30 31
AVRIL
Dim Lun Mar Mer Jeu Ven Sam
1 2 3 4
5 6 7 8 9 10 11
12 13 14 15 16 17 18
19 20 21 22 23 24 25
26 27 28 29 30
MAI
Dim Lun Mar Mer Jeu Ven Sam
1 2
3 4 5 6 7 8 9
10 11 12 13 14 15 16
17 18 19 20 21 22 23
24 25 26 27 28 29 30
31
JUIN
Dim Lun Mar Mer Jeu Ven Sam
1 2 3 4 5 6
7 8 9 10 11 12 13
14 15 16 17 18 19 20
21 22 23 24 25 26 27
28 29 30
JUILLET
Dim Lun Mar Mer Jeu Ven Sam
1 2 3 4
5 6 7 8 9 10 11
12 13 14 15 16 17 18
19 20 21 22 23 24 25
26 27 28 29 30 31
AOÛT
Dim Lun Mar Mer Jeu Ven Sam
1
2 3 4 5 6 7 8
9 10 11 12 13 14 15
16 17 18 19 20 21 22
23 24 25 26 27 28 29
30 31
SEPTEMBRE
Dim Lun Mar Mer Jeu Ven Sam
1 2 3 4 5
6 7 8 9 10 11 12
13 14 15 16 17 18 19
20 21 22 23 24 25 26
27 28 29 30
OCTOBRE
Dim Lun Mar Mer Jeu Ven Sam
1 2 3
4 5 6 7 8 9 10
11 12 13 14 15 16 17
18 19 20 21 22 23 24
25 26 27 28 29 30 31
NOVEMBRE
Dim Lun Mar Mer Jeu Ven Sam
1 2 3 4 5 6 7
8 9 10 11 12 13 14
15 16 17 18 19 20 21
22 23 24 25 26 27 28
29 30
DÉCEMBRE
Dim Lun Mar Mer Jeu Ven Sam
1 2 3 4 5
6 7 8 9 10 11 12
13 14 15 16 17 18 19
20 21 22 23 24 25 26
27 28 29 30 31
pic d'attaques



2,4%

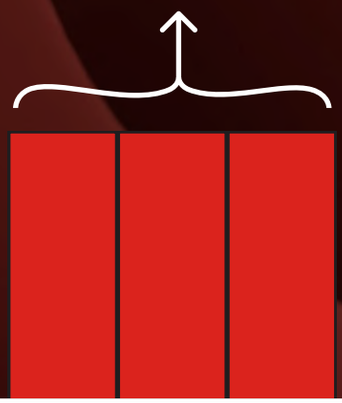
7,3%

La part d'attaques
triple le week-end

La proportion emails légitimes vs cyberattaques baisse

pic d’attaques

car les emails légitimes diminuent



Les attaquants connaissent les horaires de connexion. Ils tapent fort en journée, mais la nocivité relative explose la nuit et le week-end.

00h **01h** **02h** **03h** 04h 05h 06h 07h 08h 09h 10h 11h

12h 13h **14h** 15h 16h 17h 18h 19h 20h 21h 22h 23h

pic d’activité

D’où l’intérêt d'une protection email, d’un gestionnaire de mots de passe sécurisé 24/7, et de simulations de cyberattaque calées sur les pics réels.

Impacts croisés

- Cyber Coach
- Cyber Academy
- Sikker

Sur les utilisateurs **ayant reçu deux simulations ou plus avant et après formation**, on observe :

FORMATION → COMPORTEMENT

Collaborateur.rice transverse

TAUX DE FILL : **-33%**

REPORT : **EN HAUSSE**

Agent de terrain en structure publique et Commercial.e

TAUX DE FILL : **÷ PAR 2**

Dirigeant·e / COMEX

TAUX DE FILL : **÷ PAR 10**

Sans baisse notable du volume de simulations
→ très gros impact unitaire

Plus on forme, moins on clique et moins on remplit de formulaires malveillants. L'effet est particulièrement marqué chez les populations les plus exposées, notamment les équipes commerciales et le COMEX.

MOT DE PASSE & CULTURE DE L'ACCÈS

16 milliards

RISQUE ÉLEVÉ

d'identifiants de connexion exposés
ont été mis au jour par des chercheurs en 2025

Une partie provient des **navigateurs qui stockent les mots de passe quasi en clair**

L'autre vient de **mots de passe réutilisés, faibles, ou déjà compromis**

Identifiants : emails et mots de passe compilés dans des bases accessibles issues de fuites successives et de malwares "infostealers"

LE SAVIEZ-VOUS ?

Le **coût d'un gestionnaire de mots de passe** comme Sikker :

moins de

3€ par utilisateur et par mois

VS

Coûts d'un incident :

- FUITES DE DONNÉES
- AMENDES RGPD / NIS2 / DORA
- ARRÊT D'ACTIVITÉ
- PERTE DE CONFIANCE DES CLIENTS

Un coffre-fort sécurisé, c'est à la fois **une assurance cyber** et **un levier de conformité.**

MATURITÉ GESTION DES MOTS DE PASSE

Collaborateur.rice transverse, Commercial.e et Dirigeant·e /COMEX

RISQUE FAIBLE

Tendance nette à remplacer les mots de passe faibles par des mots de passe forts.

Agent de terrain en structure publique

RISQUE ÉLEVÉ

Population vulnérable, avec un usage encore limité de la génération de mots de passe et une forte proportion de mots de passe faibles.

Les collaborateurs adoptent le coffre pro pour gérer la complexité croissante de leurs accès, et certains profils montrent déjà une amélioration nette de la robustesse des mots de passe.

BONNES PRATIQUES

Ne pas stocker les mots de passe sensibles dans le navigateur

Utiliser un coffre-fort chiffré AES-256 avec synchronisation sécurisée

Générer des mots de passe longs, uniques et aléatoires

Activer systématiquement le MFA sur les accès critiques.

Conclusion

LE RISQUE EST **HUMAIN** AVANT D'ÊTRE TECHNIQUE

Ce n'est pas "l'entreprise" qui clique, ce sont :

- LE COMMERCIAL EN DÉPLACEMENT
- L'AGENT HOSPITALIER SOUS PRESSION
- LE RH DÉBORDÉ
- LE COMEX PRESSÉ

LA COMBINAISON DES SOLUTIONS MAILINBLACK AGIT SUR **TOUT LE TRIPTYQUE**

Protect

Réduit l'exposition brute (volume et dangerosité des emails)

Cyber Coach

Travaille le comportement en situation réelle, avec les biais cognitifs du quotidien

Cyber Academy

Construit la cyberculture dans la durée

Sikker

Sécurise les accès et réduit l'impact d'un clic raté (mdp forts, MFA, séparation pro/perso)

NOS PRODUITS SONT CONÇUS À PARTIR DE LA **DONNÉE RÉELLE**

« Nous ne construisons pas des produits pour un “utilisateur moyen”, parce qu’il n’existe pas. Par exemple, nos IA ne sont pas génériques. Elles apprennent à avoir des ***décisions adaptées*** *à chaque utilisateur en fonction de ses particularités.*

Nous concevons Protect, Coach, Academy et Sikker à partir de ***personas réels****, nourris par des* ***milliards d’emails*** *et des* ***millions d’actions****.*

Chaque évolution de nos produits part d’une question simple : *“****dans cette situation, qu’est-ce que ferait vraiment un humain ?****” »*

Justine DE UBEDA
Head of Product

Remerciements

Lab IA

Le **Lab IA** est au coeur de l'innovation technologique de Mailinblack. Notre équipe développe des solutions d'intelligence artificielle performantes pour rendre nos produits toujours plus sécurisés, intuitifs et efficaces.

Nos **data scientists** développent des algorithmes avancés pour détecter et prévenir les menaces, tandis que nos **data analysts** analysent les données pour extraire des insights stratégiques. Ensemble, ils conçoivent des solutions performantes pour protéger nos clients au quotidien.

Achraf HAMID
Data Scientist

Omar MOUNTAZ
Data Analyst

Communication

L'équipe **Communication** de Mailinblack est au service de la stratégie et de la créativité.

- Elle **analyse les chiffres** pour identifier les performances et les leviers d'action.
- Elle **capte les tendances**, met en lumière les insights et contextualise les résultats.
- Elle **traduit visuellement nos idées**, donnant vie à nos contenus.

Grâce à elle, les données se transforment en outils impactants pour sensibiliser et informer sur les enjeux de la cybersécurité.

Mélina GUILLEY
Graphic Designer

Juliette PIERRE
Communication Project Manager


MAILINBLACK