MAILINBLACK

Baromètre CYBER 2025

3ème édition

(2024-2025)

Méthodologie

Notre étude a été réalisée sur l'ensemble de nos clients utilisant indépendamment ou simultanément les solutions de notre offre U-Cyber 360°, la plateforme complète qui analyse et réduit le cyber risque humain.

Dans les faits, cela représente plus de **2 millions d'utilisateurs** et **6,16 milliards d'emails analysés** entre janvier et décembre 2024.

MAILINBLACK

U-Cyber 360°

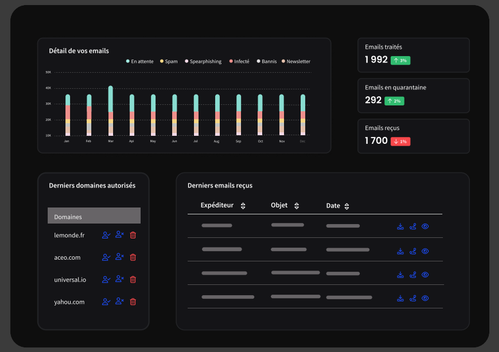
6,16 milliards

d'emails analysés entre janvier et décembre 2024, contre 5,9 milliards en 2023

Protect

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.).

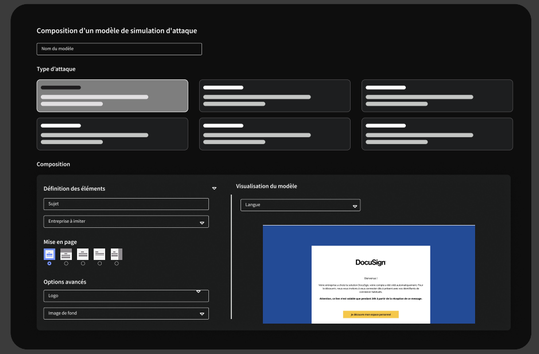
Elle **dépollue également les messageries** en éliminant les emails indésirables, tels que les spams et les newsletters.



Cyber Coach

Cyber Coach est la solution de sensibilisation et d'entrainement 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.

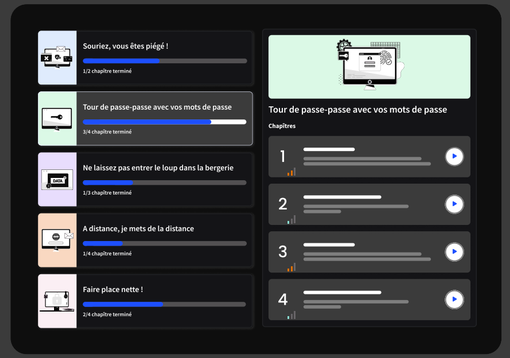
Grâce à des **simulations d'attaques variées** (phishing, ransomware, BitB, spearphishing, clé USB, QR Code), elle **entraîne les collaborateurs de manière automatisée et personnalisée**, en ciblant leurs vulnérabilités réelles.



Cyber Academy

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**.

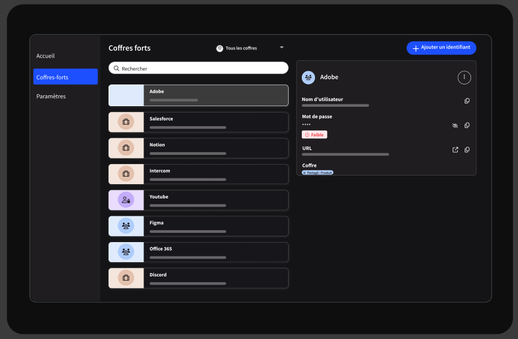
Son approche interactive et ludique permet aux collaborateurs de se former à leur propre rythme, tout en offrant un suivi de progression.



Sikker

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.



Sommaire

1 Répartition des emails

2 Cibles principales des cyberattaques et des spams

3 Temporalité

4 Ruses utilisées par les hackeurs pour tromper notre vigilance

5 Les pratiques cyber à améliorer

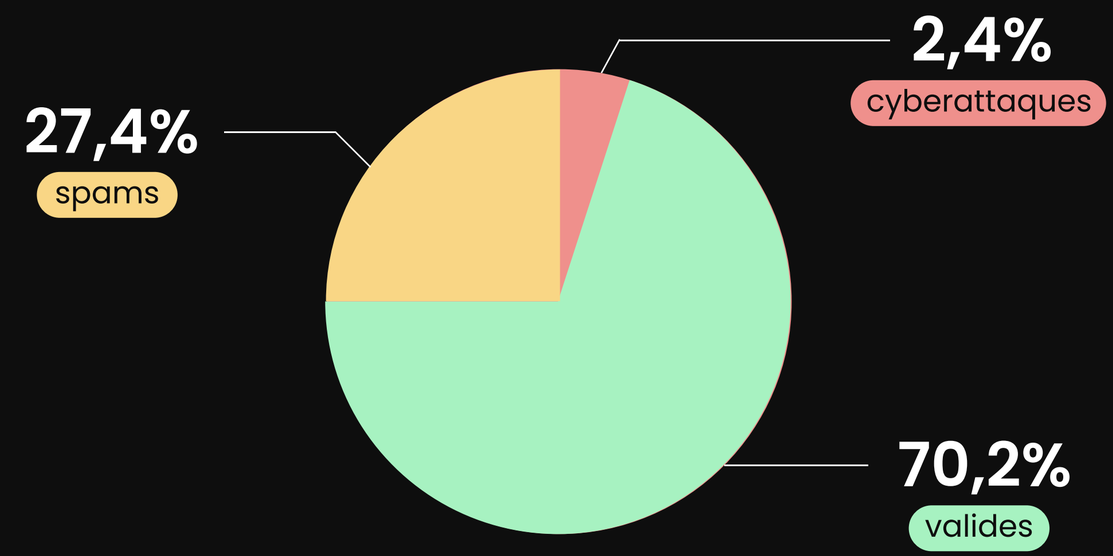
6 Email et empreinte carbone

7 Conclusion

1

Répartition des emails

Répartition des emails sur 2024



Zoom sur les cyberattaques

Analyse issue de la solution Protect

149 millions

de cyberattaques arrêtées par Mailinblack, contre 143 millions en 2023 (malware, phishing, virus)

Quelle est la part du spearphishing ?

De nouvelles formes de spearphishing se développent :

- **Whaling** : usurpation d'identité de hauts dirigeants pour accéder à des données sensibles ou détourner des fonds.
- **Usurpation de fils de conversation :** les attaquants se glissent dans des échanges d'emails légitimes via des boîtes compromises, insérant des liens ou fichiers malveillants pour exploiter la confiance contextuelle
- **IA générative** : elle permet aux hackeurs d'améliorer leurs tactiques d'ingénierie sociale, rendant les attaques plus sophistiquées et difficiles à détecter.

7,92%

des cyberattaques arrêtées par Protect en 2024 sont du spearphishing, contre 2,39% en 2023

soit

+231%

d'attaques de spearphishing en plus cette année

Zoom sur les spams

1,69 milliard

de spams bloqués par Mailinblack en 2024

soit

2,64 jours

de travail gagnés sur l'année par collaborateur

C’est le temps qu’un collaborateur gagne chaque année en n’ayant pas à trier les emails non sollicités.

2

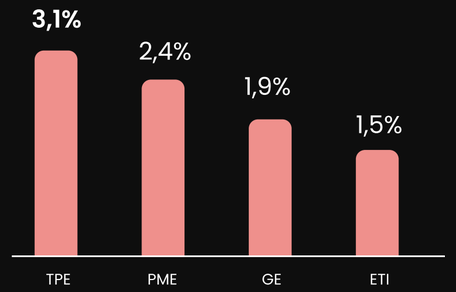
Cibles principales des cyberattaques et des spams

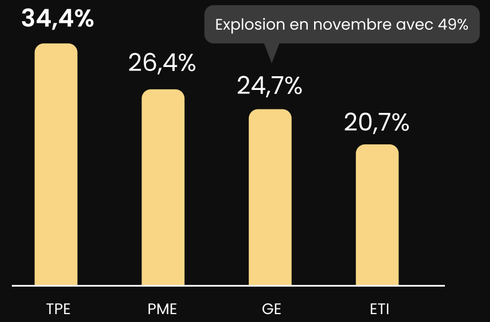
Répartition par type d’organisation

Dotées de systèmes informatiques moins sécurisés et d'une compréhension moindre des risques cyber que les grandes entreprises, les TPE et les PME sont la cible privilégiée des hackeurs.

Ces derniers ne se limitent pas à exploiter les vulnérabilités informatiques, mais tirent souvent parti d'erreurs humaines ou de négligences, telles que l'ouverture d'emails frauduleux ou la divulgation d'identifiants et de mots de passe.

Proportion de cyberattaques/spams arrêté(e)s par rapport au nombre total d’emails reçus



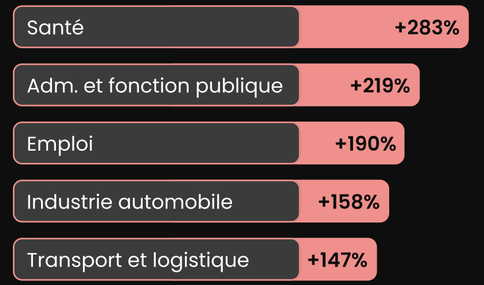


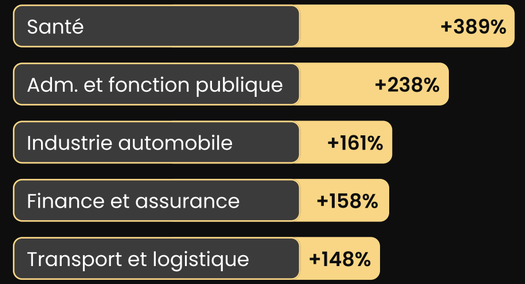
Répartition par secteur d’activité

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.

Ses infrastructures sont vulnérables, souvent dues à des systèmes obsolètes, un manque de formation en cybersécurité et des budgets limités. Les attaques, en particulier les ransomwares, peuvent paralyser les services, menaçant directement la vie des patients et forçant parfois les établissements à payer des rançons. La numérisation croissante et la télémédecine amplifient ces risques.

Évolution des cyberattaques/spams par rapport à la moyenne des secteurs





TOP 5

des métiers les plus visés

Les DSI et équipes IT, cibles privilégiées des cyberattaques en raison de leur accès aux systèmes critiques, sont particulièrement vulnérables aux attaques par ingénierie sociale, comme le spearphishing, et aux tentatives de compromission.

Nombre de **tentatives de cyberattaques** par mois :

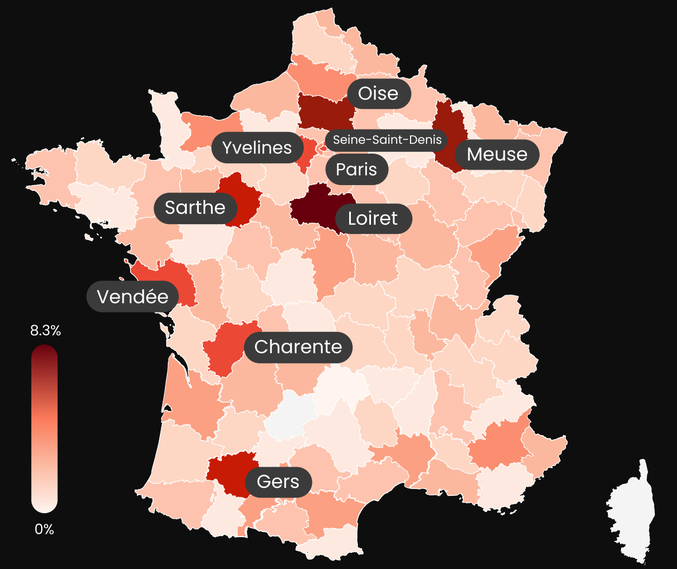
1. IT/DSI — 40
2. Direction — 39
3. Marketing — 27
4. RH — 24
5. Finance — 23

Moyenne de **spams bloqués** par mois :

1. RH — 468
2. IT/DSI — 431
3. Direction — 397
4. Marketing — 368
5. Finance — 312

TOP 10

des départements les plus attaqués



Nombres de cyberattaques en 2024 :

1. Loiret (45) — 838
2. Oise (60) — 767
3. Meuse (55) — 764
4. Gers (32) — 690
5. Sarthe (72) — 660
6. Yvelines (78) — 484
7. Vendée (85) — 469
8. Paris (75) — 469
9. Charente (16) — 459
10. Seine-Saint-Denis (92) — 458

3

Temporalité

Répartition sur l'année

Quels sont les mois où nous recevons **le plus de cyberattaques ?**

4,5%

2 points de plus que la moyenne

241
cyberattaques par mois en moyenne pour une entreprise française

464
cyberattaques en **novembre**

Quels sont les mois où nous recevons **le plus de spams ?**

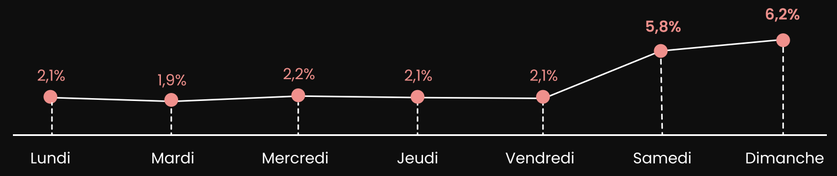
28,7%

2 752
spams par mois en moyenne pour une entreprise française

3 152
spams en **octobre**

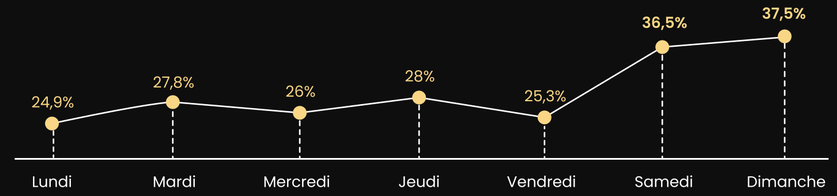
Répartition sur la semaine

Quels jours recevons-nous le plus de **cyberattaques** ?



Le week-end, **6% des emails reçus sont des cyberattaques** vs 2,1% la semaine. Pour éviter les risques de cyberattaques, nous vous conseillons de **ne pas ouvrir vos emails le weekend et d'être vigilant le lundi en les consultant**.

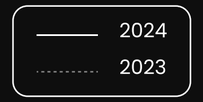
Quels jours recevons-nous le plus de **spams ?**



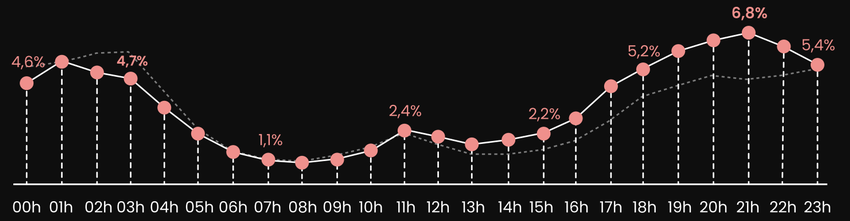
Le week-end, **37% des emails reçus sont des spams** vs 26,4% en semaine. Pourquoi ? **Nous recevons moins d'emails légitimes en dehors des jours de bureau (environ 5 fois moins).** Alors, raison de plus pour déconnecter le week-end !

Le droit à la déconnexion, pensez-y :)

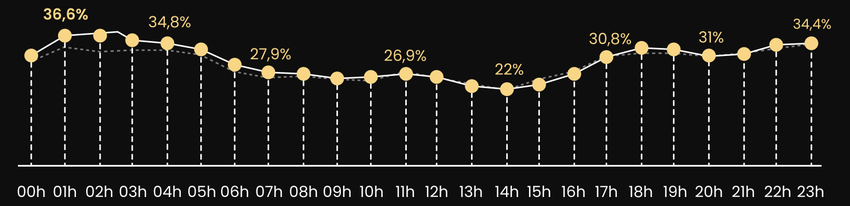
Répartition sur la journée



Et à quel moment de la journée sont reçues **les cyberattaques ?**



Et à quel moment de la journée sont reçus **les spams ?**



46,6% des cyberattaques sont reçues entre **18h et 7h du matin**.

33% des spams sont reçus entre **18h et 7h**.

Après 18h, le nombre d'emails légitimes reçus diminue, mais les tentatives de cyberattaques et de spam ne se réduisent pas, ce qui explique ces statistiques.

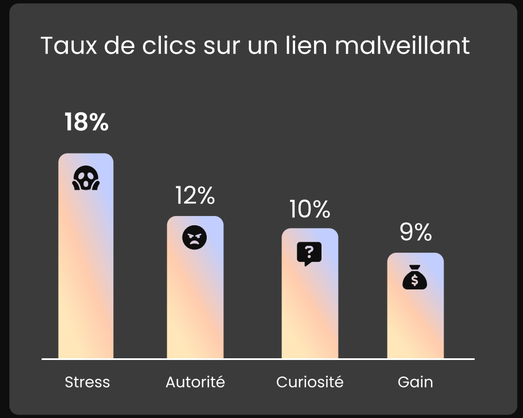
4

Ruses utilisées par les hackeurs pour tromper notre vigilance

Quels biais cognitifs font le plus réagir les utilisateurs ?

Analyse issue des simulations d'attaques envoyées par Cyber Coach

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.



TOP 5

des sujets qui piègent le plus de collaborateurs

contenant un virus

*proportion du nombre d'email contenant des virus sur les légitimes

1	**Appât des récompenses** "Nous voulons vous récompenser pour votre fidélité."	4,42%*	Les hackeurs utilisent l'appât du gain ou des récompenses pour inciter les utilisateurs à cliquer, exploitant **leur désir de recevoir des avantages ou des cadeaux**.
2	**Peur et menaces** "I RECORDED YOU!"	2,62%*	Les hackeurs jouent sur la peur et la menace, comme des accusations de comportement inapproprié, pour pousser les victimes **à réagir rapidement et sans réfléchir**.
3	**Problèmes techniques** "Mail delivery failed: returning message to sender"	2,43%*	Les hackeurs exploitent l'inquiétude liée à un problème technique ou à une erreur pour inciter les utilisateurs à **vérifier leurs mails et cliquer sur des liens malveillants**.
4	**Produits attrayants** "Un des meilleurs couteaux de cuisine au monde."	1,99%*	Les hackeurs attirent l'attention des victimes avec des offres de gadgets ou d'outils high-tech qui **paraissent utiles ou innovants**.
5	**Promotions de luxe** "Montres Rolex à -90 % ! Haute qualité à petit prix."	1,96%*	Les hackeurs ciblent les personnes attirées par des offres très avantageuses sur des produits de luxe, jouant sur **leur désir de faire de bonnes affaires**.

TOP 5

des sujets qui piègent le plus de collaborateurs

contenant un spam

*proportion du nombre d'email contenant un spam sur les légitimes

1	**Produits populaires** "L'oreiller X #1 en France"	2,10%*	Les spams publicitaires exploitent des produits connus pour **générer du trafic** vers des sites de vente en ligne ou **encourager des achats impulsifs**.
2	**Spams médicaux ou intimes** "Offre spéciale pour une perte de poids rapide"	2,07%*	Ces messages jouent sur **le désir d'améliorer rapidement la santé ou l'apparence**, ciblant les personnes vulnérables avec des promesses séduisantes.
3	**Urgence fictive** "URGENT: ACTIVEZ VOTRE NUMERO DE TELEPHONE"	1,94%*	Les spams exploitent un sentiment d'urgence pour inciter les victimes à **agir rapidement**, souvent pour voler des données personnelles.
4	**Appât des cadeaux** "Vous avez été sélectionné pour remporter l'ensemble 3 pièces..."	1,67%*	Les promesses de cadeaux ou d'offres gratuites **attirent l'attention en jouant sur l'appât du gain**.
5	**Publicités produits spécifiques** "Obtenez le dernier aspirateur sans fil pour 30 € seulement"	1,66%*	Ces messages exagèrent les avantages des produits pour **inciter à des achats impulsifs** ou **rediriger vers des sites douteux**.

TOP 10

des marques professionnelles les plus usurpées en France

dans un email de phishing, intercepté par Secure Link

HSBC	Amazon	DHL	FedEx	Apple	Zoom	Microsoft	Google	AXA	La Poste
1	2	3	4	5	6	7	8	9	10

Secure Link renforce la sécurité en vérifiant chaque lien au moment du clic pour bloquer toute tentative malveillante.

TOP 10

des marques les plus usurpées en France pendant le **Black Friday**

dans un email de phishing, intercepté par Secure Link

Nike	Nespresso	Leroy Merlin	Home Depot	Rituals	Louis Vuitton	SHEIN	Ray Ban	Rolex	Casino For You
1	2	3	4	5	6	7	8	9	10

Les consommateurs doivent **privilégier des sites sécurisés** (HTTPS), **éviter les liens suspects** et **renforcer leurs mots de passe**. Quant aux entreprises, elles doivent s'assurer de la robustesse de leurs infrastructures numériques pour prévenir les violations de données et protéger leurs clients.

Quelles thématiques provoquent le plus de clics ?

Analyse issue des simulations d'attaques envoyées par Cyber Coach

*taux de clics

1 Outil collaboratif — 19%*

Les emails usurpant un outil collaboratif sont les plus cliqués.

ShareFile Dropbox

2 Attaques internes — 16%*

Les attaques internes (avec le nom de l'entreprise) montrent une confiance excessive envers des communications perçues comme familières.

3 Marque professionnelle — 9%*

Les emails usurpant une marque professionnelle piègent efficacement avec des taux de remplissage élevés.

DocuSign

5

Les pratiques cyber à améliorer

Signalement des emails à risque

SEULEMENT

1 à 2%

des utilisateurs signalent des emails jugés suspect

Cela démontre **un manque de réflexe et de sensibilisation** à la remontée d'incidents.

Pourtant, le signalement est un enjeu clé puisqu'il **renforce la vigilance collective** et **les comportements proactifs** face aux cybermenaces.

Gestion des mots de passe par secteur

Analyse issue des utilisateurs de la solution Sikker

60 mots de passe

professionnels par utilisateur en moyenne dans des secteurs comme l'**immobilier**, les professions **juridiques**, les **études et conseils**, et la **finance/assurance**

soit

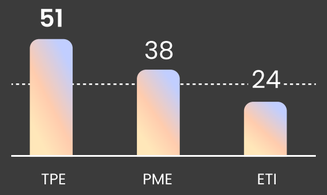
2 fois + que la moyenne

Ces métiers nécessitent de **nombreux accès numériques pour gérer des données critiques**, ce qui fait d'eux des secteurs particulièrement exposés aux cybermenaces. La gestion sécurisée des mots de passe y est donc un enjeu majeur.

Gestion des mots de passe par type d’organisation

Analyse issue des utilisateurs de la solution Sikker

Mots de passe **professionnels** :

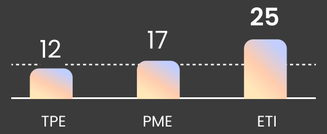


MOYENNE = 31

mots de passe professionnels en moyenne tous segments confondus

Les TPE jonglent avec un nombre plus élevé de mots de passe, souvent lié à leur **forte dépendance à une variété d'outils numériques**. Les ETI, mieux structurées, rationalisent leurs accès, mais cela ne signifie pas qu'elles sont à l’abri des mauvaises pratiques.

Mots de passe **partagés** :



MOYENNE = 14

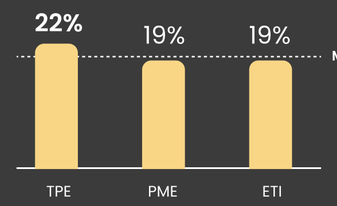
mots de passe partagés en moyenne tous segments confondus

Plus une entreprise est grande, plus les mots de passe partagés augmentent, reflétant la nécessité de coordonner des équipes plus nombreuses et des processus plus complexes.

Malgré les outils de cybersécurité comme les gestionnaires, une part importante de mots de passe faibles ou réutilisés subsiste, ce qui constitue un risque non négligeable. Les gestionnaires de mots de passe réduisent ces dangers, mais l’adoption des bonnes pratiques reste un levier crucial pour améliorer la sécurité.

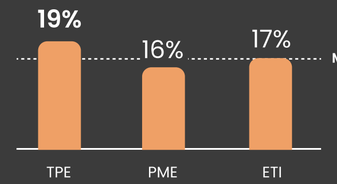
Ces données montrent à quel point les mots de passe sont omniprésents et variés dans la vie numérique professionnelle. Elles soulignent aussi que des efforts supplémentaires, combinant sensibilisation et outils adaptés, sont indispensables pour sécuriser les entreprises face aux cybermenaces croissantes.

Mots de passe **faibles** :



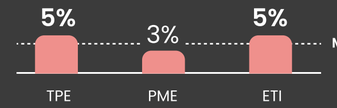
MOYENNE = 20%

Mots de passe **réutilisés** :



MOYENNE = 17%

Mots de passe **compromis** :



MOYENNE = 4%

Formation à la cybersécurité par secteur

Analyse issue des utilisateurs de la solution Cyber Academy

Les secteurs les plus impliqués dans la sensibilisation à la cybersécurité :

- Adm. publique **22,5%**
- Finance **14,08%**
- Santé **10,20%**

Ces secteurs, **particulièrement exposés aux risques cyber**, montrent une volonté accrue de former leurs équipes face aux menaces.

La forte présence des administrations publiques souligne l'importance de **protéger les données citoyennes**, tandis que le secteur de la finance et de la santé doivent **gérer des informations financières et médicales critiques**.

Formation par type d'organisation

Former les collaborateurs reste un défi, même avec des formats modernes comme le micro-learning ou des contenus gamifiés, conçus pour rendre la sensibilisation plus engageante et accessible.

État des lieux **après 6 mois** de mise en place de **formation à la cybersécurité** :

TPE	**22%** de progression moyenne	**15%** des utilisateurs l'ont terminée
PME	**16%** de progression moyenne	**11%** des utilisateurs l'ont terminée
GE	**12%** de progression moyenne	**5%** des utilisateurs l'ont terminée

Malgré des formations interactives, les grandes entreprises mobilisent moins leurs collaborateurs, tandis que les petites, plus agiles et proches, engagent mieux, même sur des modules longs. L'environnement reste clé pour le succès des formations.

6

Email et empreinte carbone

EMPREINTE CARBONE

Impact positif de Mailinblack sur l'environnement

55,5 tonnes

d'émission de CO2

sauvées par Mailinblack
ces 12 derniers mois

Ce qui équivaut à **122 544 litres** d'eau en bouteille

La solution Protect de Mailinblack analyse les emails reçus par l'utilisateur et place les messages non désirés et potentiellement malveillants en quarantaine.

Pour éviter l'accumulation de données inutiles, après 30 jours, les emails non récupérés sont automatiquement supprimés, réduisant ainsi les émissions de CO2 liées au stockage à long terme des emails.

7

Conclusion

Des attaques plus ciblées, plus difficiles à détecter

Si le volume global des cyberattaques semble stable, leur nature s'est profondément transformée.

Les hackeurs délaissent les campagnes massives pour **des attaques ultra-ciblées comme le spearphishing, qui a augmenté de 231% en un an**.

Cette évolution leur permet de **maximiser leurs chances de succès** tout en réduisant le volume, rendant ces attaques plus discrètes et difficiles à repérer. Chaque email devient une opération minutieusement calculée, exploitant des failles spécifiques pour contourner les protections traditionnelles.

Exploiter la psychologie humaine, avec encore plus de finesse

Les cybercriminels ne se contentent pas de réutiliser leurs tactiques : ils les poussent à leur paroxysme.

Le **stress** (18% des victimes) ou l'**autorité** (12%) restent des biais cognitifs exploités avec une efficacité redoutable. À cela s'ajoute l'**usurpation de marques connues**, comme Microsoft Teams ou Dropbox, qui piègent jusqu'à 19% des destinataires.

Ces techniques, combinées à des campagnes de spearphishing personnalisées, **augmentent considérablement l'impact des attaques**. Pourtant, les entreprises qui investissent dans la sensibilisation de leurs équipes réduisent ces risques et renforcent leur défense collective.

Les TPE et PME : des cibles conscientes et engagées

Les TPE et PME continuent de subir un volume disproportionné de cyberattaques : **3,1% des emails reçus par les TPE et 2,4% par les PME sont malveillants**, contre 1,9% pour les grandes entreprises. Cependant, elles redoublent d'efforts pour contrer cette vulnérabilité.

En prenant conscience de leur exposition, elles se mobilisent pour former leurs équipes : dans les entreprises de moins de 50 salariés, 22% des formations à la cybersécurité sont complétées, contre 12% seulement dans les grandes structures.

Cette prise de conscience **démontre leur capacité à se protéger malgré des moyens souvent limités**, et illustre une **dynamique positive dans leur adaptation aux menaces**.

Santé : des données critiques et convoitées

Les **données de santé** figurent parmi les cibles les plus lucratives pour les cybercriminels, valant **jusqu'à trois fois plus que des données personnelles classiques sur le marché noir**.

Pourquoi une telle attractivité ?
Ces informations permettent **un large éventail d'utilisations frauduleuses** : chantage basé sur des données médicales sensibles, falsification de dossiers pour des fraudes à l'assurance, espionnage industriel de recherches innovantes, ou même prescription illégale de médicaments.

Avec un risque près de 3 fois supérieur à la moyenne, **les établissements de santé sont doublement exposés**, entre systèmes parfois obsolètes et manque de sensibilisation des équipes. Investir dans des infrastructures modernes et des programmes de formation dédiés devient essentiel pour protéger à la fois les données et les patients.

Mots de passe : essentiels mais vulnérables

Les mots de passe, bien qu'omniprésents, restent un défi majeur pour la cybersécurité.

En moyenne, un utilisateur gère 31 mots de passe professionnels, mais ce chiffre atteint 60 dans des secteurs comme la finance ou l'immobilier. Cette gestion fragmentée reflète la multiplication des outils numériques et la complexité croissante des environnements professionnels.

Cependant, les pratiques restent perfectibles : 20% des mots de passe sont faibles et 17% sont réutilisés. Ces lacunes ne sont pas seulement techniques, elles traduisent **une insuffisance de sensibilisation sur l'impact des mots de passe compromis**. Renforcer cette prise de conscience, intégrer des solutions comme l'authentification multifactorielle et encourager l'utilisation de gestionnaires sont des étapes cruciales pour sécuriser durablement les entreprises.

Le mot de la fin

Face à des cyberattaques toujours plus sophistiquées, les entreprises progressent, notamment dans **leur prise de conscience** et **leurs efforts de sensibilisation**. Cependant, les cybercriminels exploitent sans relâche **la vulnérabilité humaine** et **les failles organisationnelles**, rappelant que la cybersécurité ne peut plus se limiter aux outils techniques.

La clé réside dans une approche **centrée sur l'humain**, combinant **formation continue**, **sensibilisation ciblée** et **adoption d'une protection globale** intégrant des solutions avancées. Renforcer les capacités des collaborateurs, les outiller pour anticiper et contrer les menaces, tout en sécurisant les infrastructures, permettra de construire une résilience à 360°, essentielle pour relever les défis de demain.

Le 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

L'équipe Marketing et Communication

L'équipe **Marketing & 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.

Romuald LAISNEY
Product Marketing Manager

Juliette PIERRE
Communication Officer

Mélina GUILLEY
Graphic Designer

MAILINBLACK

contact@mailinblack.com

+33 (0)4 88 60 07 80

www.mailinblack.com

4 place Sadi Carnot, 13002 Marseille