MAILINBLACK

Baromètre CYBER 2024

2ème édition

Méthodologie

MAILINBLACK

Notre étude a été réalisée sur l'ensemble de nos clients utilisant la solution de protection de messagerie Protect et/ou la solution de sensibilisation des collaborateurs à la cybersécurité Cyber Coach. Dans les faits, cela représente plus de **2 millions d'utilisateurs** et **5,9 milliards d'emails analysés** entre janvier et décembre 2023.

Protect
BY MAILINBLACK

La solution Protect, basée sur des technologies de pointe couplées à de l'intelligence artificielle, sécurise les organisations (entreprises, établissements de santé, administrations publiques) contre toutes formes de cyberattaques qui transitent par email (phishing, spearphishing, ransomware, ...) et dépollue les messageries des emails indésirables (spams, newsletters, ...).

Cyber Coach
BY MAILINBLACK

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), Cyber Coach entraîne les collaborateurs de manière automatisée et personnalisée.

1 Répartition des emails

Zoom sur les cyberattaques

143 millions

de cyberattaques arrêtées par Mailinblack

dont

77,5%

de phishing

Zoom sur les spams

1,6 milliard

de spams bloqués par Mailinblack

dont

7,6%

contiennent des virus

Les spams ne sont donc pas seulement non-productifs, ils peuvent également être **malveillants**.

2

Ruses utilisées par les hackeurs pour tromper notre vigilance

TOP 5

des sujets qui piègent le plus de collaborateurs

1

Promotions et événements spéciaux

“Profitez de notre offre exclusive Black Friday ! Des surprises incroyables vous attendent - cliquez pour découvrir !”

2

Facturation et paiements

“Alerte de facture impayée ! Votre paiement pour l'année 2023 est en retard. Veuillez confirmer votre paiement immédiatement pour éviter des pénalités.”

3

Offres d'entreprise et bien-être

“Améliorez le bien-être de votre équipe ! Découvrez nos solutions exclusives pour la santé en entreprise. Contactez-nous maintenant !”

4

Logistique et livraison

“Alerte de colis en attente ! Vous avez un colis prêt à être livré. Veuillez confirmer vos détails de livraison immédiatement pour éviter des frais supplémentaires.”

5

Sécurité et authentification

“Action requise pour votre sécurité ! Veuillez confirmer votre numéro de téléphone pour une authentification forte et protéger votre compte.”

Quels biais cognitifs font le plus réagir les utilisateurs ?

Analyse issue des simulations d'attaques envoyées par Cyber Coach

STRESS

Le psychotype "Stress" est celui qui fait réagir le plus les destinataires d'emails de phishing, avec un **taux de clics de 12,4%** et un **taux d'hameçonnage* de 6,3%**.

Les emails jouant sur le stress font prendre des décisions précipitées et risquées, ce qui permet aux hackeurs d'augmenter le taux d'efficacité de leurs attaques.

CURIOSITÉ

La curiosité est le principal facteur influençant le téléchargement de pièces jointes dans les emails associés aux ransomwares, avec un **taux significatif de 9,2%**.

Les emails qui prétendent contenir des informations sur les salaires des employés ou les business plans de l'entreprise sont particulièrement efficaces pour attirer l'attention des utilisateurs, qui sont alors plus susceptibles de télécharger les pièces jointes de ces types de messages.

GAIN

Les personnes motivées par le gain sont particulièrement vulnérables au spearphishing, avec un **taux de clics de 21,8%** et un **taux d'hameçonnage* de 12,9%**.

De plus, la personnalisation utilisée dans les attaques de spearphishing rend ces attaques particulièrement trompeuses et redoutablement efficaces.

*pourcentage de personnes ayant rempli leurs informations suite à la réception d'une simulation d'attaque

TOP 5

des marques les plus usurpées en France

dans un email de phishing, intercepté par Secure Link

La Poste	WeTransfer	Amazon	Microsoft	Google
1	2	3	4	5

Qu'est-ce que Secure Link ?

Utilisée dans la lutte contre l'hameçonnage, Secure Link est une technologie propriétaire de Mailinblack.

Cette fonctionnalité réécrit et chiffre les liens entrants pour les soumettre à une vérification instantanée au moment du clic.

Grâce à l'IA présente au cœur de la solution, **Mailinblack permet d'augmenter la protection au moment du clic de 80%**, contrairement aux vérificateurs de liens qui reposent uniquement sur une consultation des bases de données.

3

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.

*mois le plus sensible

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

1	TPE	2,99%	Mai*
2	PME	2,66%	Août*
3	Adm. publiques	1,98%	Juin*
4	Ets. de santé	1,59%	Mai*
5	GE	1,37%	Novembre*
6	ETI	1,36%	Novembre et Mai*

1	TPE	32,65%	Juillet*
2	Ets. de santé	31,13%	Avril et Mai*
3	Adm. publiques	30,02%	Novembre*
4	PME	26,18%	Mai*
5	ETI	19,77%	Avril*
6	GE	14,03%	Avril*

Répartition par secteur d'activité

*mois le plus sensible

82%

des attaques utilisant des macros dangereuses intégrées dans des documents Word, Excel, XML, RTF ou JS ciblent spécifiquement le **secteur du commerce**

Pourquoi ?

Dans le secteur du **commerce**, les bons de commande (Word), les rapports de vente (Excel), les bases de données clients (Excel) ou encore les feuilles de calcul pour le suivi des stocks (Excel) circulent fréquemment. Les hackeurs profitent de cette routine pour **propager discrètement** des fichiers infectés par des macros malveillantes**.

**Ces macros sont conçues pour s'activer lors de l'ouverture du document, compromettant ainsi votre système d'exploitation.

1	**Commerce**	Novembre*
2	**Étude et conseils**	Septembre*
3	**Adm. et fonction publique**	Juin*
4	**Fabrication matériels**	Novembre*
5	**Santé**	Mai*

1	**Commerce**	Novembre*
2	**Adm. et fonction publique**	Septembre*
3	**Etude et conseils**	Juin*
4	**Santé**	Novembre*
5	**Construction**	Mai*

Zoom sur les administrations publiques

Les **Chambres de Commerce et d'Industrie** (CCI) sont les administrations publiques qui **reçoivent le plus d'emails malveillants**.

3 fois + de cyberattaques

Chaque mois, un utilisateur au sein d'**une CCI reçoit en moyenne 9 cyberattaques contre 3** dans les autres administrations publiques.

De plus en plus visées par les hackeurs, ces administrations renfermant **les données ultra confidentielles des entreprises** sont la cible rêvée des attaquants.

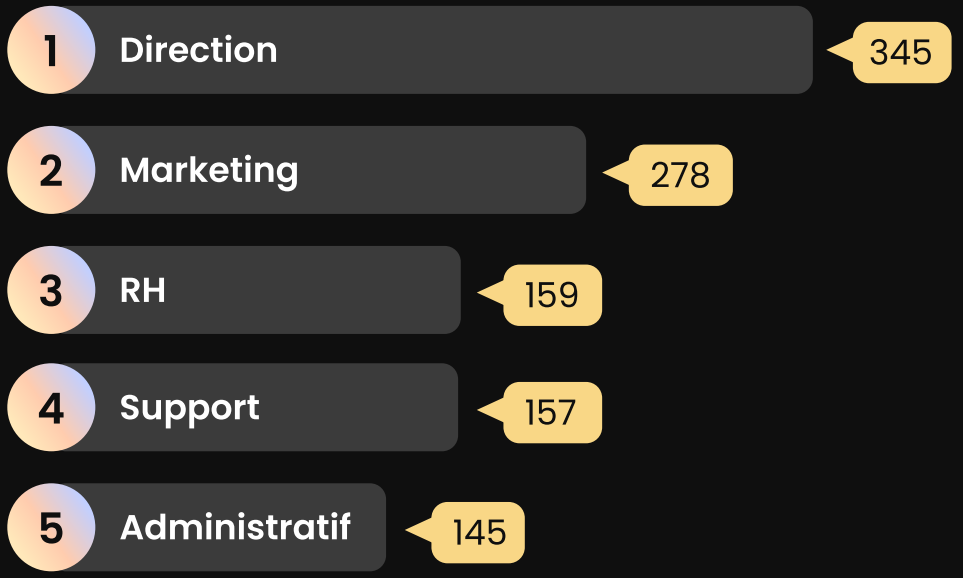
Il est donc primordial qu'elles soient vigilantes et qu'elles s'équipent de solutions de cybersécurité.

TOP 5

des métiers les plus visés

Nombre de tentatives de cyberattaques par mois :

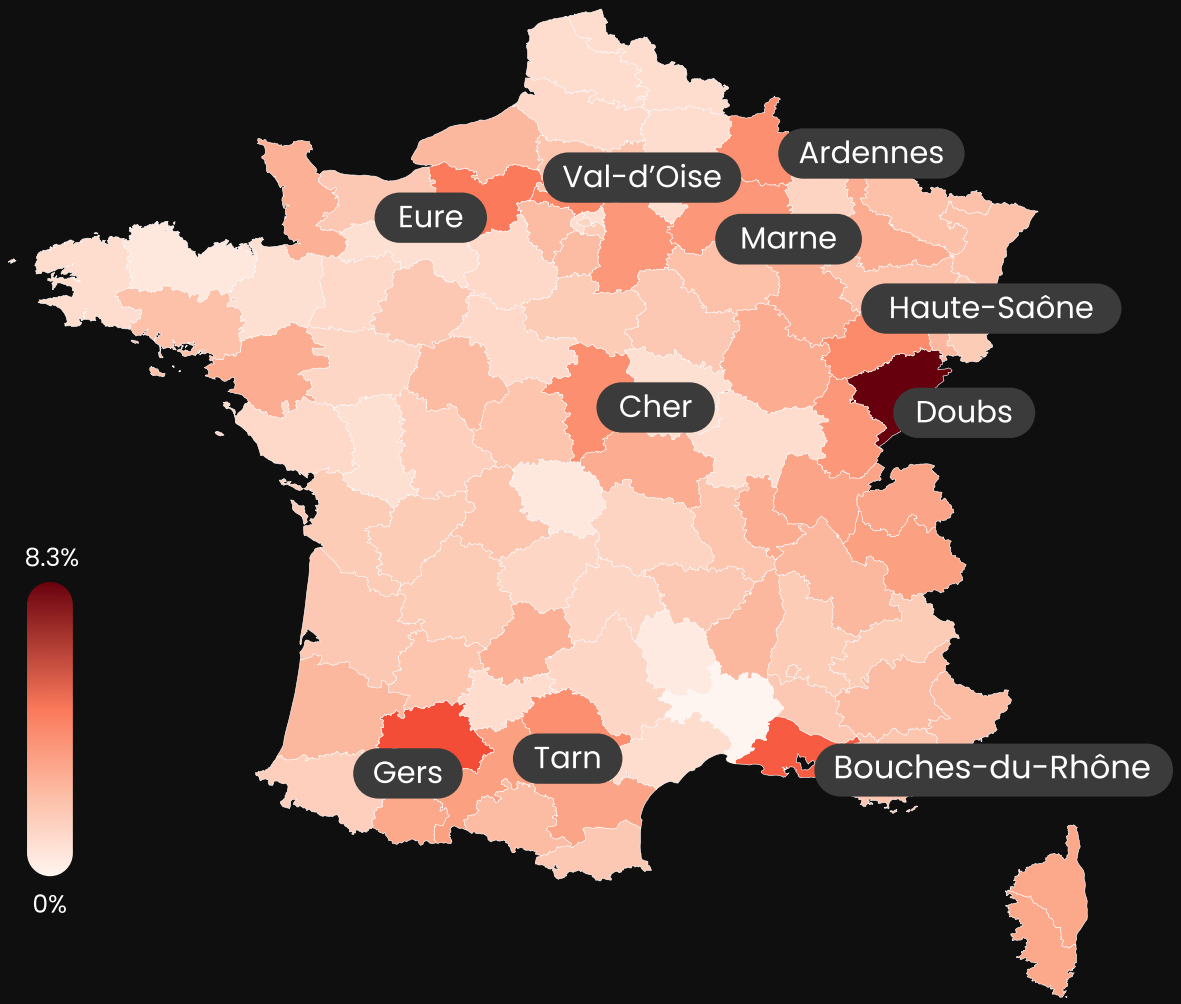
Nombre de spams bloqués par mois :



TOP 10

des départements les plus attaqués

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

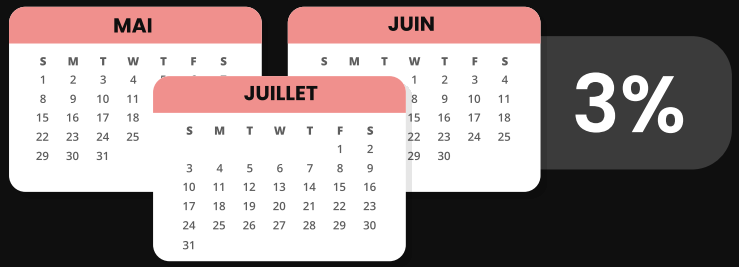


1. Doubs (25) — 8,3%
2. Gers (32) — 5%
3. Bouches-du-Rhône (13) — 4,7%
4. Eure (27) — 4%
5. Val-d'Oise (95) — 3,7%
6. Haute-Saône (70) — 3,6%
7. Cher (18) — 3,5%
8. Ardennes (8) — 3,5%
9. Tarn (81) — 3,5%
10. Marne (51) — 3,3%

4 Temporalité

Répartition sur l'année

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



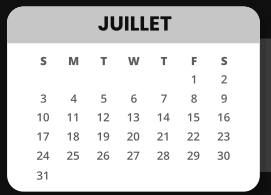
3%

De mai à juillet, le ratio de cyberattaque a été élevé (autour de 3%) contre une moyenne à 2,4% les autres mois de l'année.

1,75%

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

28,3%



26,4%

Répartition sur la semaine

Quels jours de la semaine recevons-nous **le plus et le moins de cyberattaques ?**

LUNDI | MARDI | MERCREDI | JEUDI | VENDREDI | **SAMEDI** | **DIMANCHE** → **5%**

Le week-end, 5% des emails reçus sont des cyberattaques vs 2% 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 de la semaine recevons-nous **le plus et le moins de spams ?**

LUNDI | MARDI | MERCREDI | JEUDI | VENDREDI | **SAMEDI** | **DIMANCHE** → **39%**

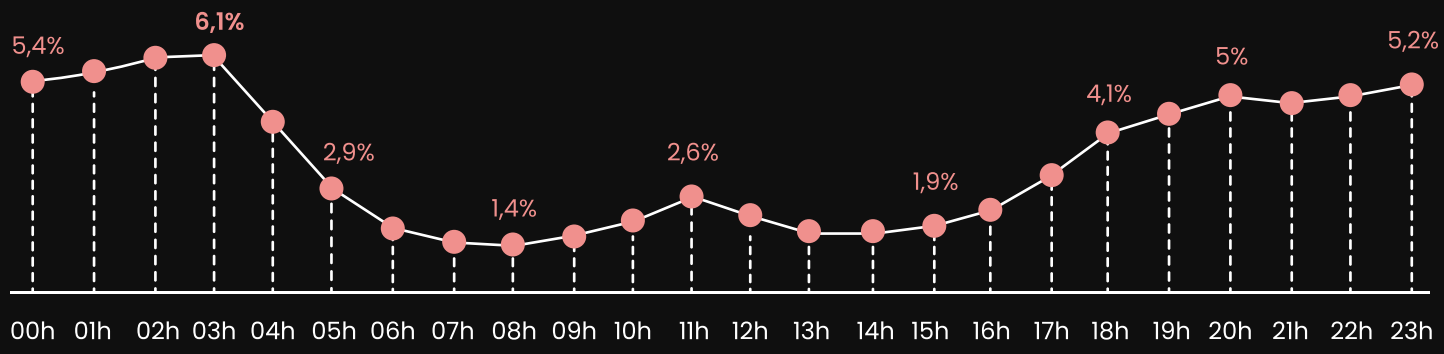
Le week-end, 39% des emails reçus sont des spams vs 26% en semaine. Pourquoi ? **Nous recevons moins d'emails légitimes en dehors des jours de bureau (environ 5 fois moins).** Alors, raison de plus pour déconnecter le week-end !

Pensez-y !

Le droit à la déconnexion >

Répartition sur la journée

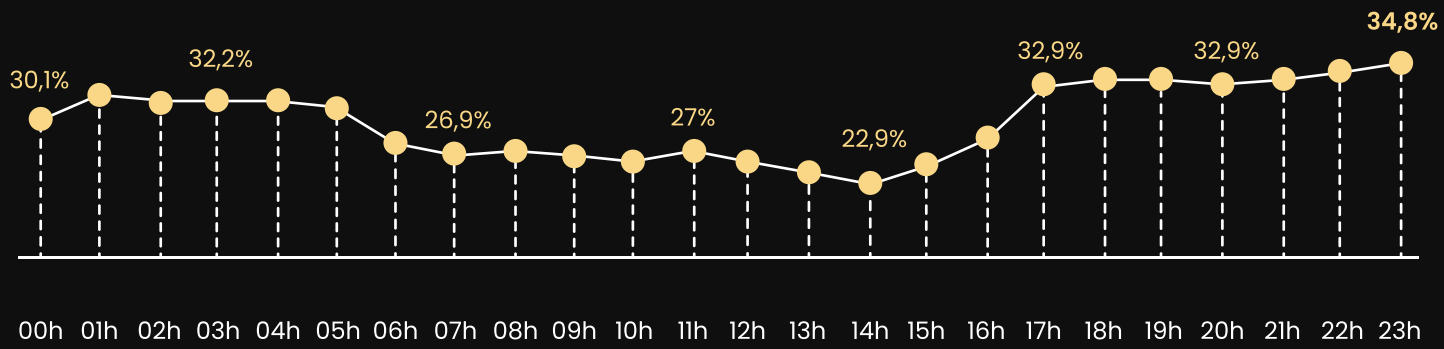
Et à quel moment de la journée sont reçus **les cyberattaques ?**



Pic de 6% à 2h et 3h du matin, moyenne à 2% pendant les heures de travail (7h et 17h).

Après 18h, nous recevons moins d'emails professionnels mais les tentatives de cyberattaques ne diminuent pas, ce qui augmente le taux.

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



Le ratio moyen de spams reçus vs emails légitimes est de 26% entre 6h et 17h et monte à 32,7% entre 18h et 5h, avec un pic à 34,8% de 23h à 00h.

5

Email et empreinte carbone

EMPREINTE CARBONE

Impact positif de Mailinblack sur l'environnement

53 tonnes

d’émission de CO2

sauvées par Mailinblack
ces 12 derniers mois

Ce qui équivaut à **115 942 litres** d’eau en bouteille

soit 6 tonnes en + qu’en 2022

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.

MAILINBLACK

contact@mailinblack.com

+33 (0)4 88 60 07 80

www.mailinblack.com

4 place Sadi Carnot, 13002 Marseille