JANVIER 2025

Rapport Santé 2024

Sensibilisation cybersécurité

conscio Technologies

Synthèse

Depuis plusieurs années, nous accompagnons le secteur de la santé dans ses efforts pour sensibiliser les collaborateurs aux bonnes pratiques en matière de cybersécurité. A l'aide de notre plateforme de sensibilisation, nous contribuons à renforcer la vigilance des agents face aux cybermenaces.

Une progression remarquable du nombre d'agents sensibilisés

Notre collaboration avec les établissements de santé, les établissements médico-sociaux, et les professionnels de santé libéraux connaît une croissance significative. En trois ans, le nombre d'agents sensibilisés est passé de 133 783 en 2022 à 529 537 en 2023, pour atteindre 625 473 en 2024. Cette augmentation témoigne de l'engagement croissant des acteurs régionaux, notamment les Agences Régionales de Santé (ARS) et les Groupements régionaux d'appui au développement de la e-santé (GRADeS). Nous accompagnons aujourd'hui 15 des 18 régions françaises.

Perspectives

Les résultats obtenus jusqu'à présent sont prometteurs, mais ils appellent à un travail continu pour maintenir cette dynamique.

Nos priorités incluent :

- L'augmentation de la participation aux campagnes de sensibilisation.
- La réduction du taux de clics sur les tests phishing.
- Le renforcement des partenariats existants avec les différentes régions.
- Le continuité de nos groupes de travail collaboratifs pour répondre aux exigences du secteur et notamment celles de la HAS.

Activité globale sur Sensiwave

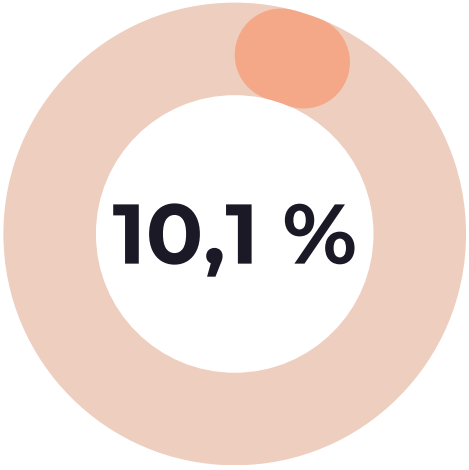
NOMBRE D'AGENTS INSCRITS

625 473

Agents ont été inscrits sur notre plateforme de sensibilisation à la cybersécurité en 2024

Il étaient **529 537** agents en 2023

PARTICIPATION



Le taux de participation moyen aux campagnes de sensibilisation est de 10,1% en 2024.

Campagnes de sensibilisation

Résultats au national

Une participation encourageante aux sensibilisations

Avec un taux de participation de 10,1 % en 2024, nous sommes sur une trajectoire motivante, marquée par des progrès réguliers et des bases solides pour l'avenir.

Ce chiffre, qui pourrait sembler modeste à première vue, s'inscrit dans un contexte d'expansion significative de notre plateforme, avec l'arrivée de plus de 95 000 nouveaux apprenants cette année. Cette croissance rapide témoigne d'un intérêt croissant pour nos campagnes, même si mobiliser un large public demande nécessairement du temps et de la persévérance.

Plusieurs réalités propres au secteur expliquent ce taux de participation et orientent nos axes d'amélioration :

- Certains agents n'ont pas d'accès direct à un poste de travail, ce qui limite leur disponibilité pour participer.
- Dans certains cas, les notifications ne leur parviennent pas directement, notamment lorsque les adresses mail servent uniquement d'identifiants et ne sont pas consultées régulièrement.
- La fiabilité des annuaires utilisateurs peut être optimisée : les comptes génériques, les mises à jour irrégulières ou incomplètes des profils sont des aspects à améliorer.
- L'arrivée significative des professionnels de santé libéraux, un public qui demeure difficile à atteindre et à mobiliser.

Malgré ces défis, nous sommes confiants dans notre capacité à faire évoluer ces indicateurs. Les efforts collectifs déployés pour enrichir les contenus et instaurer des bonnes pratiques permettront de renforcer l'engagement des apprenants.

Intégrer la sensibilisation à la cybersécurité dès les études (notamment dans les IFMS, IFSI, IFSA) permettrait de préparer les futurs professionnels de santé à adopter des pratiques sécurisées dès le début de leur carrière.
Cette pratique, observée en 2024 dans l'une de nos régions partenaires, a obtenu des résultats intéressants avec une participation des étudiants à hauteur de 54%.

Enfin, les thématiques généralistes sur les grands enjeux cyber restent les incontournables et remportent le plus d'adhésion sur l'année 2024.

Les thématiques les plus abordées en 2024

Campagnes de phishing

Résultats au national

Tests de phishing : une vigilance à renforcer

Nos campagnes de tests phishing permettent d'évaluer la vigilance des collaborateurs face aux cyberattaques et nous apportent une base précieuse pour ajuster nos stratégies et concevoir des approches plus ciblées.

Sur l'année 2024 :

- 538 campagnes de tests phishing ont été envoyées,
- 482 811 agents ont été ciblés par au moins une campagne.

Les campagnes de phishing en lien avec Microsoft restent les tests les plus utilisés par les acteurs de la santé, à égalité cette année avec la thématique des Jeux Olympiques.

Distinction par population

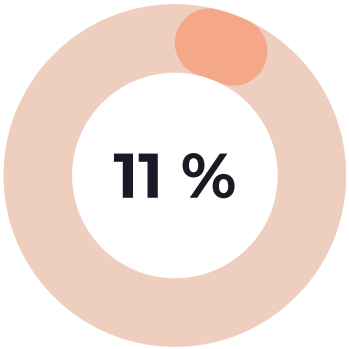
ES / ESMS / Libéraux

Pour la première fois, notre rapport distingue les résultats obtenus parmi les trois principales populations du secteur de la santé : les établissements de santé (ES), les établissements médico-sociaux (ESMS) et les professionnels de santé libéraux.

Cette segmentation, réalisée à partir d'échantillons représentatifs, met en lumière des dynamiques spécifiques à chaque groupe.

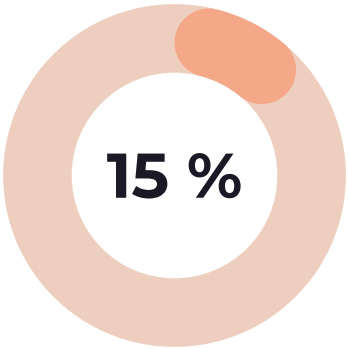
Ces résultats confirment l'importance de personnaliser nos campagnes de sensibilisation pour mieux répondre aux spécificités de chaque population, en tenant compte de leurs contraintes et environnements professionnels.

PARTICIPATION MOYENNE AUX SENSIBILISATIONS



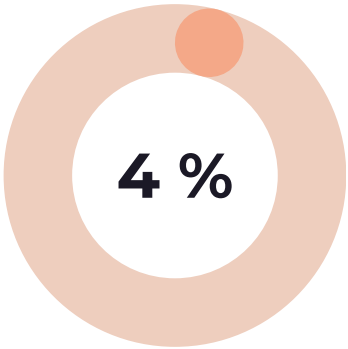
pour les ES

Sur un échantillon de 100 000 utilisateurs ES



pour les ESMS

Sur un échantillon de 40 000 utilisateurs ESMS



pour les libéraux

Sur un échantillon de 70 000 utilisateurs libéraux

Conclusion

Maintenir et amplifier nos efforts pour une cybersécurité durable dans le secteur de la santé.

Les résultats obtenus en 2024 témoignent d'un élan indéniable dans la sensibilisation du secteur de la santé aux enjeux de cybersécurité. Avec des campagnes récurrentes, une augmentation constante du nombre d'agents inscrits et une participation encourageante, les efforts collectifs déployés portent leurs fruits.

Les défis restent cependant nombreux et il est crucial de ne pas relâcher nos efforts mais au contraire, de les intensifier.

La cybersécurité est un enjeu collectif nécessitant une mobilisation continue des établissements de santé, des établissements médico-sociaux, des professionnels de santé libéraux, ainsi que de leurs partenaires institutionnels.

Pour engager davantage les agents et renforcer leur vigilance face aux cybermenaces, il apparaît essentiel de diversifier les approches et les outils de sensibilisation. Une communication adaptée, une éducation progressive, l'utilisation de canaux multiples, l'intégration de formats originaux et engageants joueront un rôle central. Ces leviers permettront de transformer la sensibilisation en une démarche proactive et participative où chaque collaborateur devient un maillon fort de la chaîne de sécurité.

Par ailleurs, les résultats différenciés selon les populations sensibilisées notamment entre les établissements médico-sociaux et les professionnels de santé libéraux, montrent que l'adaptation de nos messages et de nos méthodes à des contextes spécifiques est un facteur clé de succès. Une approche personnalisée pour chaque groupe continuera d'être un axe prioritaire.

Pour aller encore plus loin, le renforcement de nos partenariats avec les GRADeS et les ARS

s’impose comme une évidence. Ces acteurs jouent un rôle essentiel pour coordonner les actions à l’échelle régionale et garantir une proximité avec les agents. En collaborant encore plus étroitement, nous pourrons non seulement élargir notre impact, mais aussi adapter nos solutions aux besoins réels du terrain.

Enfin, la sensibilisation à la cybersécurité ne sera pleinement efficace qu’avec l’engagement actif des directions d’établissement. En communiquant régulièrement sur l’importance de ce sujet, la direction joue un rôle clé pour renforcer l’implication des agents et leur faire prendre conscience des risques liés aux cybermenaces. Insister sur le rôle individuel de chacun dans la protection des données et des systèmes contribue à responsabiliser les agents tout en créant une culture collective de vigilance.