KnowBe4

Go Phish : Quelle est la vulnérabilité des employés français face aux attaques malveillantes ?

Comprendre la résilience des employés face aux attaques malveillantes et l'impact de la formation et des simulations

WWW.KNOWBE4.COM

KnowBe4, Inc. | 33 N Garden Ave, Suite 1200, Clearwater, FL 33755
Tel: 855-KNOWBE4 (566-9234) | Email: Sales@KnowBe4.com

Pouvons-nous réduire le risque d'hameçonnage ?

Le Ministère de l'Education Nationale, de l'enseignement supérieur et de la recherche a lancé ce qui est probablement la simulation d'hameçonnage la plus ambitieuse au monde. Grâce à un projet pilote l'année dernière, une simulation d'hameçonnage à plus de 2,5 millions de collégiens et lycéens dans plus de 4 700 établissements scolaires a été envoyée début 2025.

Baptisé "Opération Cactus", ce projet vise à tester la résilience des élèves face au phishing et à renforcer leur sensibilisation aux menaces d'hameçonnage pour améliorer leur cybersécurité personnelle et mieux les préparer à leur future entrée dans le monde du travail.

Mais qu'en est-il de la résilience des collaborateurs qui font déjà partie de la population active ?

Dans ce rapport, nous examinons la confiance des employés français dans leur capacité à détecter les cyberattaques — et si cette confiance correspond à la réalité ! Nous analysons également l'efficacité des formations fondées sur les bonnes pratiques, notamment les simulations d'hameçonnage, pour réduire les risques organisationnels.

Dans ce rapport

Repérer l'hameçonnage : Quel est le niveau de résilience des employés face au phishing ?

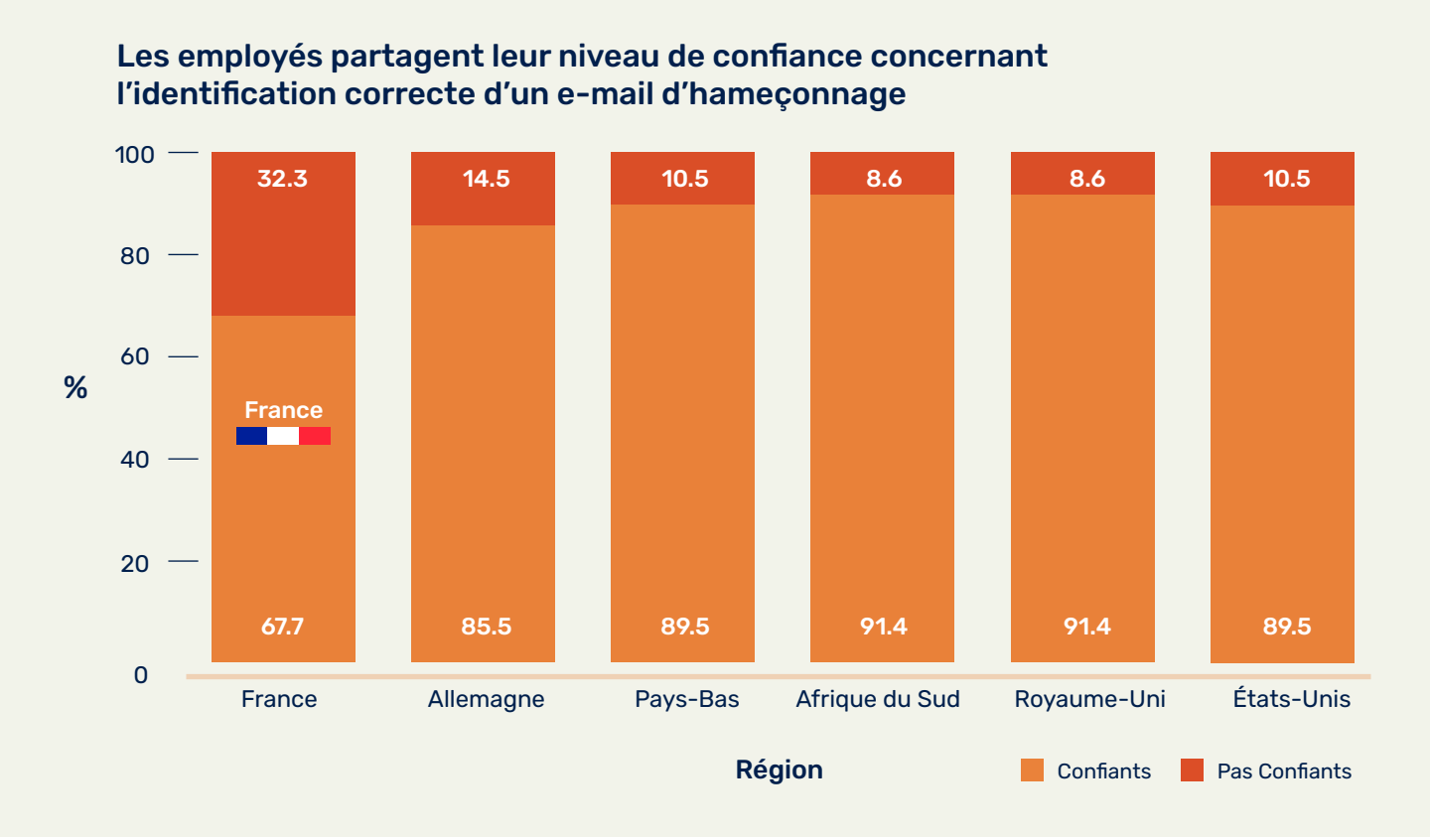
Les personnes interagissent de manière alarmante avec les attaques d'hameçonnage. Dans son Rapport Data Breach Investigations 2024, Verizon a constaté qu'en moyenne, il ne faut que 21 secondes pour que quelqu'un clique sur un lien malveillant dans un e-mail d'hameçonnage et seulement 28 secondes pour saisir ses identifiants sur un site web.

Ainsi, en moins d'une minute, votre organisation pourrait être compromise par un simple e-mail d'hameçonnage.

Améliorer la résilience des employés face aux menaces d'hameçonnage est aussi crucial que de s'assurer que vous disposez des bonnes défenses techniques avancées. Bien que l'objectif soit de toujours utiliser des produits de sécurité des e-mails comme première ligne de défense, il existe de nombreux scénarios où ces défenses pourraient ne même pas entrer en jeu - comme les attaques envoyées via les réseaux sociaux ou vers des adresses e-mail personnelles, toutes deux généralement accessibles sur les appareils professionnels.

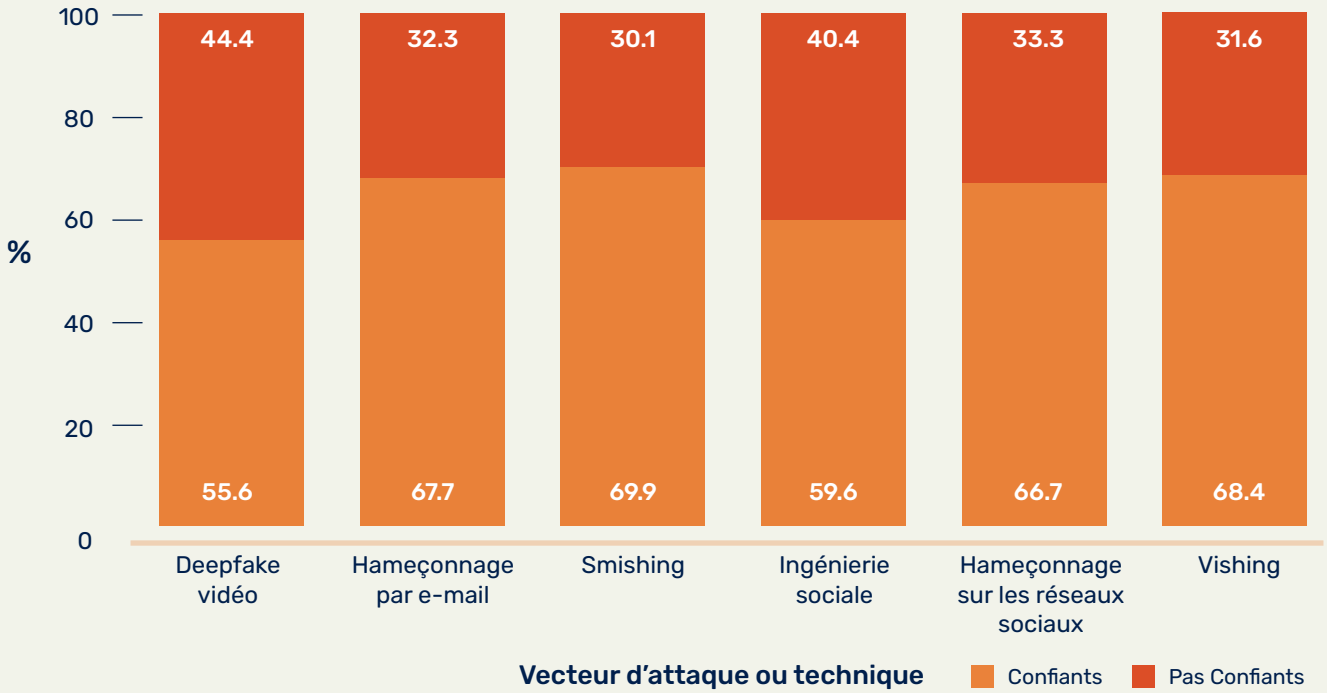
Les collaborateurs manquent de confiance pour identifier les attaques d'hameçonnage

Nous avons interrogé des employés du monde entier pour savoir dans quelle mesure ils se sentaient confiants dans leur capacité à repérer correctement les attaques d'hameçonnage. En France, seulement 67,7 % se sentaient confiants, alors que la moyenne mondiale est de 86 %. Cela place la France en dernière position des régions que nous avons étudiées, avec un pic de confiance atteignant 91,4 % à la fois au Royaume-Uni et en Afrique du Sud.



Il n'existe aucun type d'attaque que les employés français se sentent confiants d'identifier. Dans l'ensemble, au moins un tiers d'entre eux ont déclaré qu'ils auraient des difficultés - allant jusqu'à près de la moitié des employés dans certains cas. Les attaques impliquant des deepfakes vidéo sont celles qui suscitent le plus d'inquiétude, avec seulement 55,6 % des employés affirmant qu'ils seraient capables de les repérer.

Les employés en France partagent leur niveau de confiance concernant l'identification correcte des attaques malveillantes



Dans chaque catégorie, les employés qui se sont identifiés comme des hommes étaient plus confiants dans leur capacité à repérer les attaques malveillantes. Cet écart était le plus important en matière d'ingénierie sociale, avec 67,6 % des employés masculins se sentant confiants de pouvoir repérer ces techniques de manipulation contre seulement 54,7 % des employés s'identifiant comme des femmes. Des écarts plus importants étaient également présents pour l'hameçonnage sur les réseaux sociaux (71,3 % des hommes se sentaient confiants pour les repérer contre 63,7 % des femmes) et l'hameçonnage par e-mail (71,3 % des hommes se sentaient confiants contre 65,3 % des femmes).

L'âge des répondants a également influencé leur niveau de confiance. Fait intéressant, les plus jeunes (16-24 ans) et les plus âgés (55 ans et plus) se sentaient les moins confiants. La confiance a atteint son maximum chez les 25-34 ans, suivis par les 45-54 ans. Au niveau le plus élevé, trois quarts (74,3 %) des 25-34 ans se sentaient confiants dans leur capacité à repérer les attaques d'hameçonnage par e-mail et par vishing. Pour les 55 ans et plus, seulement 60,5 % ont déclaré pouvoir identifier correctement une attaque par e-mail et 64,1 % ont dit la même chose pour le vishing.

En moins d'une minute, votre organisation pourrait être compromise par un simple e-mail de phishing

L'hameçonnage par e-mail reste la principale cause d'incidents, avec 19,3 % des employés français déclarant avoir été victimes de ce type d'attaque.

Bien que ce résultat reflète le pourcentage d'employés qui ont été ciblés par des attaques et qui sont prêts à reconnaître en avoir été victimes, le profil de risque d'une organisation est généralement plus élevé.

Dans le Phishing By Industry Benchmarking Report 2025 de KnowBe4, nous avons analysé les données de simulation d'hameçonnage par e-mail de la plateforme KnowBe4 HRM+ à travers trois phases :

1

Référence :
Avant toute formation KnowBe4, une simulation d'hameçonnage initiale est envoyée à tous les employés pour calculer le "pourcentage de vulnérabilité à l'hameçonnage" (PPP) de référence ou taux de clics.

2

Après 90 jours :
Une autre simulation est envoyée pour calculer l'amélioration du taux de clics après que les employés ont participé à une formation sur les bonnes pratiques.

3

Après 12 mois :
Après un an de formation, le PPP est calculé à nouveau.

En 2025, le taux de clics de référence pour les organisations européennes a été évalué à 32,5 %. Ainsi, sans formation, un tiers des employés sont automatiquement susceptibles d'être victimes d'attaques d'hameçonnage.

Pour boucler la boucle : ce taux de clics de 32,5 % dans les simulations correspond parfaitement aux 32,5 % d'employés français qui déclarent ne pas être confiants pour identifier les attaques d'hameçonnage par e-mail. Ce tiers avait donc probablement raison dans l'évaluation de leurs capacités initiales !

Un peu moins de la moitié des employés admettent avoir été victimes d'une attaque malveillante

Dr. Martin Kraemer
Défenseur de la sensibilisation à la sécurité

Analyse d'expert : Qu'est-ce qui rend les personnes vulnérables aux attaques malveillantes ?

De multiples facteurs influencent la probabilité qu'une personne interagisse avec un e-mail d'hameçonnage - et, comme nous l'avons vu dans le rapport de Verizon, tout peut se produire extrêmement rapidement. Ces facteurs peuvent être divisés en deux éléments : la conception de l'attaque et le contexte de la victime.

L'e-mail d'hameçonnage et l'état d'esprit de la personne qui le reçoit changent au cas par cas. Par exemple, différentes attaques utiliseront différentes techniques d'ingénierie sociale, mais elles suivent généralement la même recette : exiger une action spécifique, avec un sentiment d'urgence et un déclencheur émotionnel pour l'escalade. Les attaquants usurpent généralement l'identité d'une marque ou d'une personne pour donner plus de crédibilité à leur attaque, et ils jouent sur des émotions telles que l'avidité, la serviabilité ou l'intérêt personnel. D'autres aspects de la conception de l'attaque incluent la charge utile et le type d'attaque, qu'il s'agisse d'hameçonnage par e-mail, de smishing ou de vishing (ou autre !).

Quant au contexte de la victime, le comportement humain n'est pas aussi rationnel que nous aimerions le croire. Les utilisateurs peuvent réagir différemment à des scénarios identiques selon leur état d'esprit et niveau de stress. Un utilisateur est plus susceptible d'agir sans prêter une attention totale à chaque petit détail.

Par nature, les traits et habitudes humains ne peuvent évoluer que lentement au fil du temps. Ces facteurs personnels incluent le sentiment de contrôle sur son propre destin et les habitudes formées lors de l'utilisation des e-mails, ainsi que les influences culturelles (comme la langue et les attitudes envers l'autorité et la confiance). Les hommes, par exemple, se perçoivent souvent comme plus compétents en matière de technologie et de cybersécurité, tandis que les femmes sont souvent des apprenantes plus diligentes. La perception de ses capacités ne se traduit pas automatiquement par un comportement sûr.

Fait intéressant, une étude académique a montré que les personnes ayant une grande confiance dans leurs capacités à identifier les e-mails d'hameçonnage sont plus susceptibles d'être des "cliqueurs récidivistes" qui interagissent régulièrement avec les simulations et les attaques. D'autres recherches suggèrent qu'il existe plus de 30 facteurs individuels qui contribuent à la vulnérabilité d'une personne face à l'hameçonnage.

Tout le monde est susceptible d'être victime d'attaques malveillantes. Il n'y a pas d'exceptions. Cependant, la vulnérabilité varie d'une personne à l'autre et selon les différents contextes et moments. Bien que certaines personnes soient naturellement plus résilientes que d'autres, elles peuvent toujours être victimes d'un e-mail d'hameçonnage bien conçu qui arrive dans leur boîte de réception au bon moment. C'est pourquoi il est crucial de suivre une approche centrée sur l'humain, en s'appuyant sur des défenses techniques pour limiter l'exposition aux risques, en autonomisant les personnes grâce à la formation et à la pratique, et en fournissant des politiques utilisables et exploitables qui fonctionnent pour les individus.

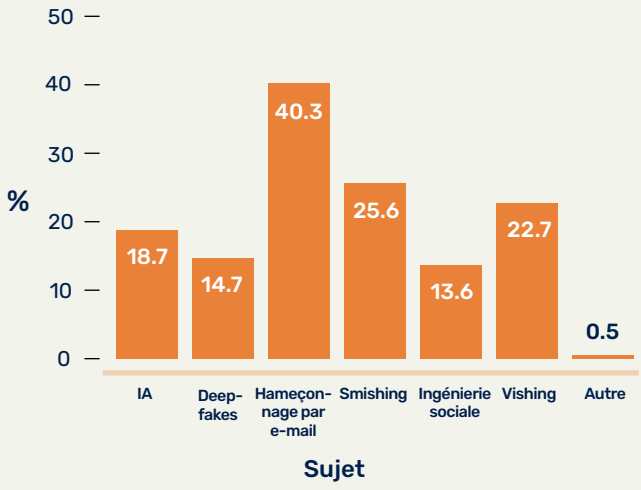
La formation et les simulations peuvent-elles réellement réduire les taux de clics ?

La réponse courte est oui, l'utilisation de formations et de simulations fondées sur les bonnes pratiques dans le cadre de votre programme de gestion du risque humain peut réduire les taux de clics.

Malheureusement, parmi les employés français interrogés, 33,3 % ne reçoivent actuellement aucune formation. Parmi eux, 18,2 % ont déclaré ne pas reconnaître certains termes courants de cybersécurité, tels que "hameçonnage", "ingénierie sociale" et "messages d'hameçonnage sur les réseaux sociaux".

Comme on pouvait s'y attendre, l'hameçonnage par e-mail est le sujet sur lequel la plupart des répondants (40,3 %) se souviennent avoir reçu une formation. Cependant, comme il s'agit du vecteur d'attaque le plus courant, cela laisse 59,7 % des collaborateurs potentiellement non préparés. Les autres sujets étaient considérablement moins couverts, avec un minimum de 13,6 % pour l'ingénierie sociale, ce qui est également préoccupant étant donné la prolifération de ces tactiques dans les attaques avancées.

Les employés partagent les sujets sur lesquels ils se souviennent avoir reçu une formation



Prouver l'efficacité de la formation

Comme mentionné, pour le Phishing Benchmarking 2025 Rapport pour l'Europe de KnowBe4, nous générons des données sur trois phases. Les phases ultérieures se produisent après 90 jours et un an de formation basée sur les bonnes pratiques.

Pour les organisations européennes, le taux de clics initial de référence de 32,5 % diminue considérablement au fil du temps. Après seulement trois mois de formation KnowBe4, il descend à 20,7 %. Après un an, le taux de clics d'hameçonnage chute à seulement 5 %.

Cela représente une réduction de 85 % du risque d'hameçonnage.

Et les nouvelles continuent d'être positives. Nos données montrent qu'en poursuivant votre programme de formation, vous pouvez maintenir les taux de clics à un niveau bas année après année.

Comment les employés évaluent-ils les simulations d'hameçonnage ?

Les simulations d'hameçonnage sont une caractéristique des formations basées sur les bonnes pratiques, visant à aider les employés à reconnaître les menaces directement dans leurs boîtes de réception. Auparavant, il existait certaines perceptions négatives concernant les simulations - par exemple, qu'elles sont conçues pour piéger les employés ou qu'elles abordent des sujets inappropriés, comme des augmentations de salaire ou des primes qui ne se matérialisent jamais.

Cependant, grâce à l'amélioration de la culture de cybersécurité, à une sensibilisation accrue et à l'adoption de normes de formation fondées sur les bonnes pratiques, les attitudes des employés envers les simulations sont extrêmement positives.

Parmi les employés français qui reçoivent des simulations d'hameçonnage dans le cadre de leur formation, 87,5 % déclarent trouver les simulations pertinentes pour leur travail et les menaces auxquelles ils pourraient être confrontés. En outre, 86,5 % affirment également que les simulations qu'ils reçoivent améliorent leur sensibilisation aux véritables attaques d'hameçonnage.

Il est essentiel pour les équipes de cybersécurité de préserver ce sentiment positif envers les simulations dans le cadre de leur programme plus large de gestion du risque humain.

Cinq façons de garantir que vous proposez un programme de formation basé sur les bonnes pratiques

Ce rapport démontre une marge de progression en ce qui concerne la sensibilisation et la formation. Les employés ont des niveaux de confiance faibles quant à la reconnaissance des attaques d'hameçonnage, un tiers sont automatiquement enclins à interagir avec des e-mails malveillants, et un nombre alarmant - 47,7 % - affirment avoir été victimes d'une attaque réelle. De plus, ils se souviennent peu des sujets de formation.

Face à cette situation, voici cinq façons de vous assurer que vous améliorez la résilience des employés face à l'hameçonnage et réduisez les risques pour votre organisation.

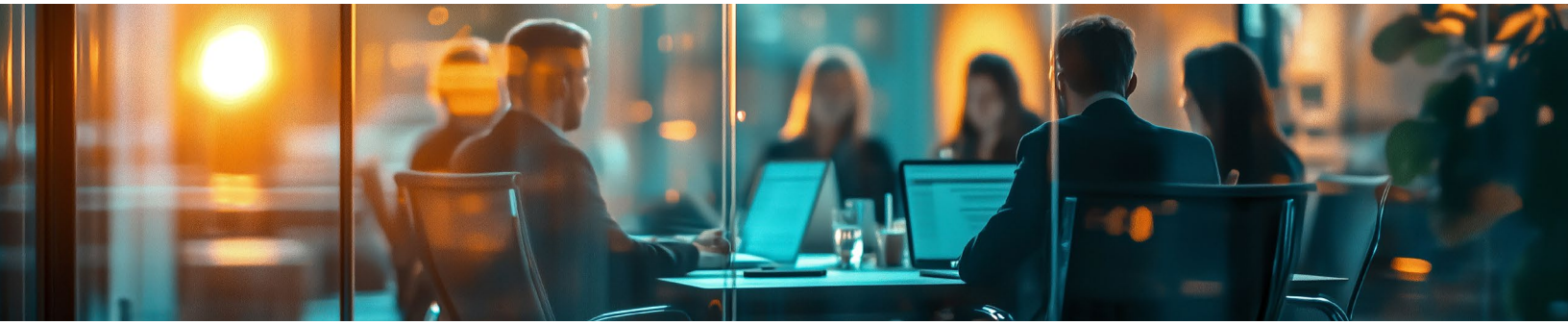
1. **Personnaliser. Personnaliser. Personnaliser.**
   La formation est plus efficace lorsqu'elle est pertinente pour le rôle d'une personne et les menaces réelles auxquelles elle est confrontée. Avec l'essor des plateformes de gestion du risque humain pilotées par l'IA, il est désormais possible d'adapter la formation à chaque individu au sein de votre organisation.

2. **Utilisez de vraies menaces (mais neutralisez-les d'abord !)**
   Là encore, cela fait écho à la pertinence de la formation. Il est désormais possible de transformer des e-mails d'hameçonnage neutralisés en simulations et de former les personnes en utilisant les menaces qui ciblent réellement votre organisation.

3. **Un coaching continu est essentiel**
   Une formation continue est essentielle pour modifier les comportements et renforcer les politiques de sécurité. En analysant et en comprenant le comportement des utilisateurs, vous pouvez fournir une micro-formation contextuelle continue dans le cadre de votre programme régulier, augmentant ainsi la pertinence de votre message de sécurité et améliorant la compréhension des employés.

4. **N'oubliez pas les facteurs culturels**
   Différents lieux auront différentes considérations culturelles qui peuvent façonner la façon dont les employés s'engagent dans la formation. Une solution unique ne convient pas à tous, alors communiquez avec les équipes pour comprendre les facteurs qui pourraient influencer leurs opinions et comportements, et pour trouver des ambassadeurs locaux.

5. **Perturbez les comportements de sécurité négatifs**
   La formation ne s'arrête pas aux simulations et aux modules en ligne. Avec l'essor des plateformes de gestion du risque humain qui agrègent le comportement des utilisateurs et les renseignements sur les menaces, vous pouvez déployer des technologies qui interrompent les personnes au moment du risque et leur permettent de prendre des décisions plus sécurisées.



À propos de KnowBe4

KnowBe4 offre au personnel les moyens de prendre au quotidien des décisions plus éclairées en matière de sécurité. Avec la confiance de plus de 70 000 clients à travers le monde, KnowBe4 aide les organisations à consolider leur culture de la sécurité et à gérer le risque humain grâce à sa plateforme complète pilotée par l'IA. Ce produit de pointe crée une couche de défense adaptative qui renforce les comportements des utilisateurs face aux toutes dernières menaces de cybersécurité. La plateforme HRM+ comprend des modules couvrant la formation sur la sensibilisation et à la conformité, la sécurité des e-mails dans le cloud, le coaching en temps réel, la lutte collective contre l'hameçonnage, les agents de défense basés sur l'IA, et bien plus encore. Seule plateforme de sécurité universelle de ce type, KnowBe4 s'appuie sur des contenus, des outils et des techniques de cybersécurité personnalisés et pertinents capables de mobiliser le personnel et de faire de lui non plus la plus grande surface d'attaque, mais un atout incontournable de l'organisation.

Pour en savoir plus, consultez la page **www.KnowBe4.com/fr**

Méthodologie

Ce rapport utilise des données provenant de deux enquêtes indépendantes auprès d'employés français commandées par KnowBe4 et réalisées par Censuswide. L'enquête A a interrogé 2 001 employés qui utilisent un ordinateur au travail sur leur expérience concernant l'identification et la victimisation d'attaques malveillantes. L'enquête B a interrogé 200 employés français qui reçoivent des simulations d'hameçonnage dans le cadre de leur formation à la sensibilisation à la sécurité pour comprendre leur attitude envers ces simulations. En outre, les données sur le pourcentage de vulnérabilité à l'hameçonnage (taux de clics) ont été générées par la plateforme KnowBe4 HRM+ et publiées pour la première fois dans le Phishing By Industry Benchmarking Report 2025.

KnowBe4

KnowBe4 NL, BV | Central Park, Stadsplateau 27-29, 3521 AZ Utrecht, Pays-Bas
Tél. : +31 (0)30 7996074 | www.KnowBe4.com/fr | Sales@KnowBe4.com