KnowBe4

Série Leadership éclairé : réflexions sur les comportements en matière de sécurité

Le partage d'informations sur la cybersécurité, vecteur d'une culture de la sécurité durable

Par Martin Kraemer

Une formation efficace des employés repose principalement sur trois éléments : le contenu, l'expérience et les relations. Le bon contenu doit être diffusé via les canaux appropriés aux bons destinataires et au bon moment.

Occupés à relever ce défi, les employeurs tendent à oublier que les employés consomment et partagent déjà des informations sur la cybersécurité, aussi bien dans la sphère privée que professionnelle. Ce comportement est non seulement souhaitable, mais il témoigne également d'une culture en cybersécurité bien ancrée. Les professionnels de la sensibilisation à la cybersécurité et de la culture de la sécurité le savent bien. Ils reconnaissent l'importance de collaborer avec le personnel pour comprendre leurs pratiques de sécurité et leur donner les moyens d'adopter de meilleurs comportements.

Partage d'informations sur la cybersécurité : motivations, méthodes et contenus

L'adoption proactive des bonnes pratiques, l'entraide et le soutien mutuel entre collègues, ainsi qu'une vision claire de la valeur et du rôle de la cybersécurité au sein de l'organisation sont les signes d'une solide culture de la sécurité. Cette culture se reflète aussi dans la volonté des employés de partager les informations. Il n'en reste pas moins que la culture de la cybersécurité s'inscrit dans la culture organisationnelle, qui est elle-même influencée par la culture sociale. Notre environnement culturel façonne nos idées, nos valeurs et nos habitudes.

Un élément crucial de toute stratégie de cybersécurité est l'efficacité de la communication avec les parties prenantes. C'est le fondement même de toute formation sur le lieu de travail. Pour réduire le risque humain, nous devons rallier nos employés à notre cause, tant sur le plan émotionnel qu'intellectuel, afin d'influencer leurs comportements. C'est une tâche ardue qui consiste à diffuser l'information, à la transformer en connaissances, à souligner les responsabilités de chacun afin d'encourager des attitudes qui renforceront la motivation. La réunion de tous ces éléments est la clé pour mettre en place de bons comportements face à la sécurité.

La relation entre communication proactive parmi les employés et culture robuste de la sécurité se retrouve dans le modèle de maturité de la culture de la sécurité de KnowBe4. Le partage proactif des informations sur la cybersécurité est le signe d'une culture de la sécurité bien ancrée. Les bons comportements en matière de sécurité forment la structure même d'une culture saine de la sécurité, présente tant dans la vie privée que professionnelle. Cette culture favorise l'adoption de pratiques plus sûres, au travail et à la maison, comme l'utilisation d'un gestionnaire de mots de passe.

La maturité de la culture de la sécurité : une dimension mesurable

Les employés d'une organisation dotée d'une solide culture de la sécurité ont davantage tendance à s'impliquer proactivement dans la protection de leur entreprise, par exemple en détectant des attaques par ingénierie sociale ou en signalant des incidents de cybersécurité. KnowBe4 a élaboré une enquête sur la culture de la sécurité incluant sept dimensions. Nos clients sont nombreux à l'utiliser pour déterminer la maturité de la culture de la cybersécurité dans leur organisation. Selon le Rapport 2024 de KnowBe4 sur la culture de la sécurité, les organisations basées en Europe sont légèrement moins performantes dans la plupart de ces dimensions, en l'occurrence les attitudes, la cognition, la communication, la conformité et les normes. En revanche, elles obtiennent de meilleurs résultats que les organisations américaines en ce qui concerne la dimension du comportement. Les différences en matière de culture de la sécurité entre organisations sont mesurables. Plus la culture de la sécurité est solide, mieux l'organisation est protégée.

Faciliter le partage d'informations sur la cybersécurité

Tant que les enjeux de cybersécurité sont considérés comme prioritaires, les employés tendent davantage à mettre à profit la formation reçue lorsqu'ils en ont besoin : c'est le phénomène de rappel des connaissances. Une communication active et multifacettes diffuse les connaissances, nourrit les relations et accentue le sentiment d'appartenance.

Le Dr Martin J. Kraemer (notre spécialiste attitré de la sensibilisation à la sécurité pour la région Europe et Moyen-Orient) a fait équipe avec le Dr William Seymour (maître de conférences en cybersécurité au King's College de Londres). Ensemble, ils ont étudié la façon dont les employés consomment les informations sur la cybersécurité et les partagent avec leurs amis, leurs proches et leurs collègues. Ils ont également cherché à comprendre l'impact des formations sur le lieu de travail dans quatre grands pays occidentaux : les États-Unis, le Royaume-Uni, l'Allemagne et la France.

Leur objectif : comprendre les motivations, les méthodes utilisées, ainsi que la nature des informations sur la cybersécurité consommées et partagées par les individus, et déterminer comment ces données peuvent nous aider à améliorer la sensibilisation à la cybersécurité et la culture de la sécurité.

Cybersécurité : passer du savoir à l'action

Une prise de conscience ne mène pas forcément à un engagement. C'est une réalité humaine souvent constatée. Connaître une menace et vouloir s'en protéger, sans parler de vouloir agir, sont des choses différentes. Les professionnels de la sensibilisation à la sécurité en sont bien conscients. Aussi, ils cherchent davantage à influencer les comportements qu'à diffuser des connaissances et des informations.

Pour autant, cela ne signifie pas que les individus modifient leur comportement sans raison. Au contraire, connaître ses motivations est souvent à l'origine de l'adoption de nouvelles habitudes et routines positives, y compris en matière de sécurité. D'où l'importance d'une communication efficace, capable d'exposer clairement les risques et les dangers, tout en proposant des conseils et des solutions : un pilier de la culture de la sécurité.

Notre enquête montre que la cybersécurité est un thème de discussion récurrent. La cybersécurité est entrée dans nos vies. Nous voulons en savoir plus sur la cybersécurité, la comprendre et partager les informations utiles pour notre propre protection et celle d'autrui. Presque tous les répondants (95 %) avaient spontanément lu ou regardé du contenu sur la cybersécurité au moins une fois, et 77 % avaient reçu directement des informations à ce sujet.

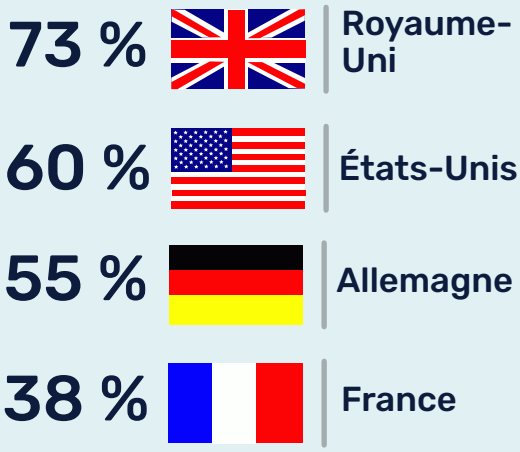
Pourquoi la cybersécurité suscite-t-elle autant d'intérêt ?

Les dernières informations sur la cybersécurité dont nos répondants se souvenaient tombaient dans une des nombreuses catégories définies : les violations de données (22 %), l'hameçonnage (17 %) et le piratage (15 %) figuraient parmi les thèmes les plus courants. Ce n'est guère surprenant. Les violations de données et le piratage font fréquemment la une des médias. Quant à l'hameçonnage, il fait fréquemment l'objet de mises en garde de la part des banques et des boutiques en ligne. C'est aussi une préoccupation majeure en entreprise.

Où trouvons-nous des informations sur la cybersécurité ?

La sensibilisation à la sécurité est aussi l'art de transmettre les bonnes connaissances au bon moment, aux bons destinataires et dans le bon format. Les professionnels de la sensibilisation à la sécurité mettent tout en œuvre pour faciliter l'assimilation des informations par leur public cible. D'après les réponses à l'enquête, les sources d'information varient selon les tranches d'âge. Si l'employeur reste la principale source d'information toutes tranches d'âge

57 % des personnes interrogées ont suivi une formation sur la cybersécurité



Données démographiques

Après nettoyage des données des réponses à l'enquête, nous avons obtenu un jeu de données final composé comme suit : 277 réponses en provenance de France (âge moyen 31 ans), 238 d'Allemagne (âge moyen 32 ans), 288 du Royaume-Uni (âge moyen 41 ans) et 292 des États-Unis (âge moyen 41 ans). La plupart des répondants occupaient un emploi à plein temps (56 %). Le reste se répartissait comme suit : emploi à temps partiel (18 %), sans emploi (7 %) ou activité non rémunérée (7 %), prise d'un nouveau poste prévu pour le mois suivant (2 %), et autres situations ou sans réponse (9 %). Parmi les répondants de France et d'Allemagne, 52 % occupaient un poste à temps plein. Ce chiffre atteignait 63 % au Royaume-Uni et 67 % États-Unis.

confondues, d'autres canaux sont privilégiés selon les profils comme les réseaux sociaux (18-29 ans), les sites web (30-39 ans et 60-69 ans), le partage direct (40-49 ans) et les émissions et podcasts (50-59 ans). Ces différences de préférences ont un impact sur les informations trouvées, car tous les contenus ne circulent pas de façon égale sur tous les canaux. Nous le verrons plus en détail dans la suite de ce document.

Pourquoi partageons-nous des informations sur la cybersécurité ?

L'enquête a révélé que les répondants consommaient des informations sur la cybersécurité provenant de diverses sources, mais choisissaient aussi de partager ces informations avec d'autres personnes (25 %). Cette pratique est un comportement de sécurité très souhaitable. Elle témoigne d'un réel engagement des individus, déjà sensibilisés au problème, qui souhaitent à leur tour informer et faire réfléchir leur entourage sur les enjeux liés à la cybersécurité.
D'après nos répondants, si des personnes (conjoints, membres de la famille, amis ou collègues) ont partagé avec eux des informations sur la cybersécurité, c'était principalement dans le but de les aider à se protéger. La deuxième motivation exprimée était le potentiel lien entre les informations partagées et l'expérience personnelle de l'expéditeur. Les répondants partageaient des contenus en cybersécurité parce qu'ils estimaient que les personnes concernées étaient exposées aux mêmes risques. Ils souhaitaient se protéger, aider les autres à se protéger ou faire part de leur expérience personnelle.

Points à retenir : la sensibilisation est un facteur clé pour influencer le comportement

Un engagement fort nourrit l'envie de partage.

Plus nous nous informons et nous formons, plus nous sommes enclins à nous impliquer et à partager. Cependant, si nous ignorons la nature des menaces, il est impossible de savoir que nous devons, ou même pouvons, modifier nos comportements.

Notre enquête montre que les répondants qui ont obtenu les scores les plus élevés sur les questions de sécurité et de vie privée partageaient plus d'informations sur la cybersécurité avec leurs partenaires, leur famille, leurs amis et leurs collègues. Une preuve concrète que la connaissance joue un rôle clé dans la promotion d'une culture de la sécurité.

C'est la raison pour laquelle il est important de pouvoir répondre aux questions suivantes :

- Comment proposer aux utilisateurs un contenu utile, qui leur plaise et qu'ils doivent absolument connaître ?
- Comment le diffuser de façon à encourager sa consommation et son partage ?
- Comment concevoir un contenu qui renforce les liens avec l'équipe de la sécurité de l'information, mais aussi entre les utilisateurs ?

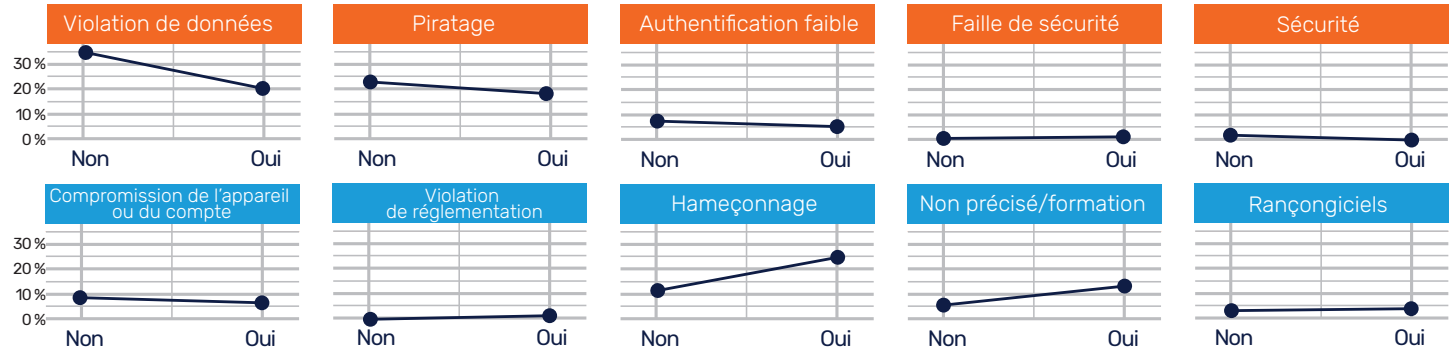
Les sources d'informations et leur rôle

La plupart des répondants ont trouvé du contenu sur la cybersécurité sur des sites web (22 %) et par le biais de leurs employeurs (21 %). Les autres sources sont les réseaux sociaux (16 %), le partage direct (15 %) et les émissions et les podcasts (12 %). Les communications émanant d'autres entreprises (8 %) et les autres sources (5 %) sont moins courantes.

Les répondants ont consulté des sources diverses pour se renseigner sur les différents sujets. Les combinaisons les plus courantes source/sujet sont les suivantes : communication des employeurs sur l'hameçonnage (7 %), sites web sur les violations de données (5 %) et formations sur la sensibilisation (sans autres précisions) dispensées par les employeurs (5 %). Viennent ensuite les partages en privé ou les émissions présentant des informations sur les violations de données (4 %), ainsi que des discussions sur les incidents de piratage sur les réseaux sociaux (4 %).

La formation sur l'hameçonnage reçue sur le lieu de travail est nettement mise en avant par rapport aux autres contenus. Les personnes ayant suivi une telle formation se souvenaient généralement mieux du contenu sur l'hameçonnage (+10,3 %) et mentionnaient beaucoup moins les violations de données (-10,1 %). Celles qui avaient bénéficié d'une formation avaient aussi mieux mémorisé les connaissances de leur cursus de formation que les données provenant d'autres sources.

La formation sur le lieu de travail a un effet significatif sur le souvenir que les participants ont des types de menaces rencontrés dans leurs conversations ou leurs lectures dernièrement



Recevoir et partager des informations sur la cybersécurité

Un bon contenu de formation doit proposer des informations exploitables. De l'avis des répondants, leurs organisations l'ont bien compris. Les employeurs sont en effet plus nombreux que toutes les autres entités à partager des « solutions ». Les actualités de la cybersécurité, en revanche, proviennent en général d'émissions et de podcasts.

Informations sur la cybersécurité : un partage issu de l'entourage et de différents médias

En général, les informations sur la cybersécurité ont été partagées avec les répondants par message (45 %), en face à face (34 %), sur les réseaux sociaux (13 %), par téléphone (1 %) ou par d'autres moyens (7 %). Ce sont la plupart du temps des amis (32 %) qui ont communiqué des informations sur la cybersécurité aux répondants, au sujet de violations de données (7 %) ou d'incidents de piratage (7 %). 9 % ont mentionné que le thème du « piratage » résultait de partages sur les réseaux sociaux par des interlocuteurs qu'ils ne connaissaient pas personnellement.

Dans les cas où les répondants ont reçu des informations sur la cybersécurité de la part de tiers, les thèmes principaux différaient selon les expéditeurs. Les informations reçues des collègues de travail concernaient surtout les violations de données (5 %) ou l'hameçonnage (4 %). Les informations sur les violations de données (7 %), le piratage (7 %) ou une authentification faible (4 %) provenaient principalement d'amis et non d'autres sources. Ce choix semble délibéré, car les organisations souhaitent que leurs employés soient sensibilisés sérieusement aux violations de données et à l'hameçonnage.

Point à retenir : la répartition des différents thèmes de cybersécurité est inégale

Tous les thèmes ne sont pas traités de la même façon par toutes les sources

Chacun a ses préférences en matière de recherche et de consommation d'informations en ligne. Il est notoire que certaines plateformes favorisent certains types d'informations : on sait par exemple que les réseaux sociaux proposent des informations plus polarisantes.[1]

Il en va de même pour les informations sur la cybersécurité trouvées par nos répondants. Les thèmes étaient répartis de façon inégale entre les différentes sources. La formation sur le lieu de travail a exercé un impact très net sur le type d'informations recherchées et consommées.

Il est important de noter que les employés consomment des informations sur la cybersécurité sur leur lieu de travail, mais aussi ailleurs. Les professionnels peuvent tirer parti de cette réalité en orientant et en influençant délibérément la conversation, ou en la laissant évoluer librement.

- Comment déterminer les enjeux de cybersécurité qui comptent pour vos employés et évaluer leurs niveaux de connaissances à leur sujet ?
- Quels sont les thèmes les plus importants pour votre organisation ?
- Comment résoudre le problème des idées fausses et des attitudes influencées par des sources d'information externes à l'entreprise ?

Remarque : nous avons également constaté que 5 % des participants se souvenaient avoir acquis leurs connaissances les plus récentes en matière de cybersécurité lors d'une formation sur le lieu de travail. En revanche, ils ne se souvenaient pas du thème principal de la formation. Une bonne formation doit marquer votre mémoire durablement, être ludique et éviter que les apprenants s'en désintéressent.

[1] Pew Research Center – News Platform Fact Sheet (Fiche technique sur les plateformes d'actualité)

Le partage d'informations : un pilier essentiel de la sécurité

La formation sur le lieu de travail reçue par les répondants de notre échantillon ne les a pas incités à diffuser l'information. Ils ont en général moins partagé les informations sur l'hameçonnage (-5,7 %), préférant diffuser des contenus sur les rançongiciels (6,7 %) ou des informations génériques sur une violation de données (4,9 %).

Il y a de nombreuses explications possibles. Des limitations techniques ont peut-être restreint les possibilités de partager le contenu des formations professionnelles. Les participants ont aussi pu supposer que tous les autres employés de l'entreprise avaient accès à la même formation et aux mêmes connaissances. Dans tous les cas, ce résultat doit être évité. Pour ce faire, il est nécessaire de proposer une formation qui encourage le partage de l'enseignement reçu.

Lorsque la question leur a été posée, les répondants ont souligné les avantages du partage d'informations sur la cybersécurité avec d'autres personnes. La formation sur le lieu de travail a influencé leur tendance à partager l'information : ceux ayant suivi une formation étaient plus enclins à partager leurs connaissances avec leurs collègues (23,6 %). Cependant, cette formation a eu un impact négatif sur les intentions de partage d'information avec les amis (-8,9 %), les membres de la famille (-8,9 %) et les conjoints (-5,3 %).

Points à retenir : favoriser et encourager le partage d'informations sur la cybersécurité dans les cercles sociaux

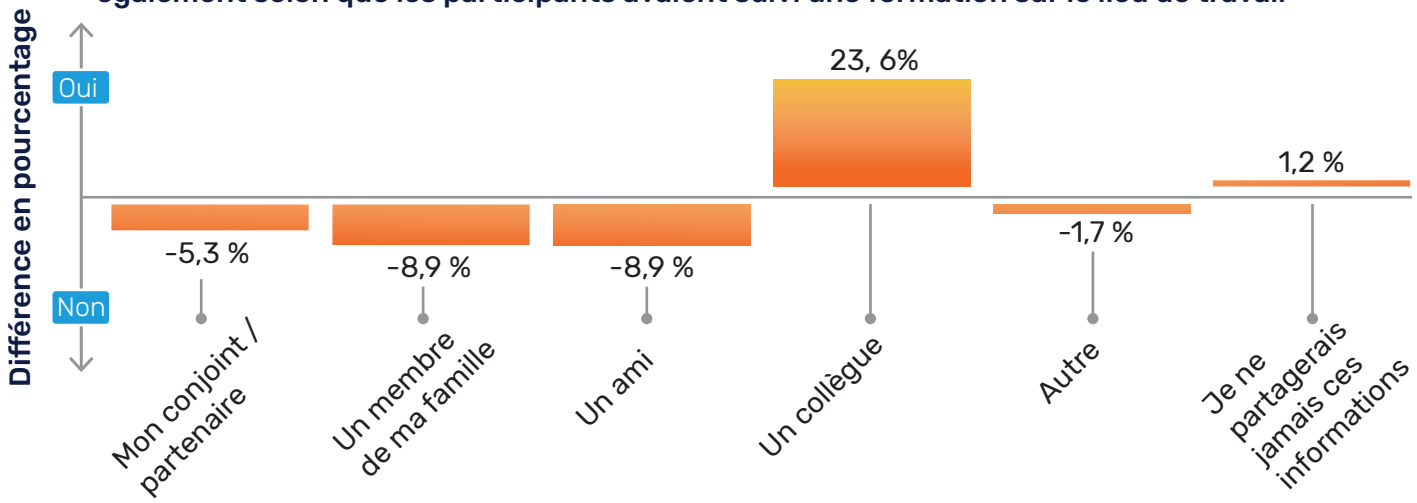
Éliminez les obstacles au partage et donnez aux utilisateurs les moyens de s'affranchir des barrières sociales.

Le partage d'informations sur la cybersécurité contribue à façonner la culture de la sécurité. Le contenu d'une formation doit pouvoir être partagé avec tous les membres concernés de l'entourage social. La formation elle-même doit encourager le partage de son contenu avec les parties prenantes concernées.

- Comment les organisations peuvent-elles répondre aux préférences de partage des employés pour faire le lien entre vie professionnelle et vie privée ?
- Comment les organisations peuvent-elles mettre en place des mesures incitatives encourageant le partage de tous les contenus pertinents ?
- Comment les organisations peuvent-elles hiérarchiser les thèmes et organiser leurs initiatives de formation en fonction des sujets et des moyens de communication ?

Les organisations doivent étudier ces questions en fonction de leurs objectifs, car il n'existe pas de réponse universelle.

La volonté de partager les connaissances acquises en cybersécurité variait également selon que les participants avaient suivi une formation sur le lieu de travail



Recommandations

Protéger et se protéger : nos enjeux communs
La cybersécurité et la protection d'autrui sont des préoccupations collectives. Les programmes de sensibilisation à la sécurité doivent tenir compte de cette réalité pour gagner en efficacité. Donnez à vos employés les outils qui leur permettront d'agir pour leurs familles et pas seulement pour leurs collègues. Autorisez-les éventuellement à partager l'accès aux contenus particulièrement attrayants avec leurs proches.

Retour aux fondamentaux
Même si cela semble une évidence, une solide compréhension des concepts de base permet de prendre de meilleures décisions fondées sur des attentes factuelles.

Faites le choix de la qualité
La réussite de votre programme dépend de la qualité de votre contenu. La formation sur le lieu de travail a une incidence sur les informations sur la cybersécurité que les participants vont retenir. Choisissez délibérément du contenu adapté à vos objectifs.

L'information : sur place et à emporter !
Simplifiez le partage des informations sur la cybersécurité dans la sphère professionnelle mais aussi privée. Des obstacles peuvent empêcher les employés de partager des informations avec leurs proches. La cybersécurité ne connaît pas de frontière : elle nous accompagne aussi bien chez nous que sur notre lieu de travail.

Encouragez le partage d'informations sur la cybersécurité
Fournissez le bon contenu, dans le bon format et avec une expérience adaptée pour inciter au partage. Facilitez le partage en ouvrant des canaux de communication dédiés.

Différences culturelles
Gardez à l'esprit que les différences individuelles et culturelles ont un impact sur l'efficacité d'une formation. Élaborez des concepts qui tiennent compte des différences culturelles. Sachez poser les bonnes questions.

Les influences culturelles : une myriade de nuances

Ne simplifiez pas à l'excès les différences culturelles. Si le pays de résidence peut être un bon indicateur du contexte linguistique et sociopolitique, nos travaux montrent néanmoins qu'il ne suffit pas à expliquer les influences culturelles et contextuelles sur les attitudes et les comportements. Pour concevoir des programmes adaptés à chaque culture, les experts doivent aller à sa découverte sur le terrain.

La cybersécurité est une problématique aux facettes multiples que chacun appréhende différemment. En d'autres termes, les programmes de sécurité doivent pouvoir s'adapter à des types de personnalité, des styles d'apprentissage, des attitudes et des préférences divers. Ces différences individuelles se retrouvent également dans les différences culturelles à plus grande échelle. Nous avons cependant observé que le pays de résidence est un piètre indicateur des différences dans la consommation de contenus et les comportements de partage. Les quatre pays de cette étude comptent des communautés culturelles aux facettes multiples, qui ont leurs propres attitudes en matière de sécurité, leurs comportements, leurs environnements médiatiques, leurs langues, et leurs canaux d'information. Accessoirement, nous savons qu'il existe des différences de préférences flagrantes entre pays.

N'utilisez pas les pays comme des raccourcis pour apprendre à connaître la culture sur le terrain. Il est essentiel de vous familiariser avec les comportements sociaux, les coutumes et les valeurs qui forment l'environnement d'un comportement en matière de sécurité. Il est également important de comprendre votre culture avant de pouvoir la façonner. Allez sur le terrain et questionnez, étudiez et observez pour apprendre.

Test de sécurité gratuit relatif à l'hameçonnage

Découvrez le pourcentage de Phish-Prone (pourcentage de vulnérabilité à l'hameçonnage) de vos employés, en profitant de votre test de sécurité gratuit relatif à l'hameçonnage.

Programme automatisé de sensibilisation à la sécurité gratuit

Créez un programme de sensibilisation à la sécurité, personnalisé pour votre organisation.

Outil Phish Alert Button gratuit

Un seul clic suffit désormais à vos employés pour signaler les attaques par hameçonnage de manière sécurisée.

Outil Email Exposure Check (EEC) gratuit

Identifiez avant les pirates les adresses e-mail à risque de vos utilisateurs.

Outil Domain Spoof Test gratuit

Déterminez si les pirates peuvent usurper une adresse e-mail de votre domaine.

À propos de KnowBe4

KnowBe4 fournit la plus grande plateforme au monde de formation sur la sensibilisation à la sécurité et de simulation d'hameçonnage. Nous aidons les organisations à gérer le facteur humain de la sécurité grâce à une stratégie de sensibilisation aux rançongiciels, à la fraude au président et aux autres tactiques d'ingénierie sociale. Spécialistes de la cybersécurité de renommée internationale, nous avons élaboré une approche résolument innovante.

Rejoignez plus de 70 000 organisations internationales qui font confiance à la plateforme de KnowBe4 pour renforcer votre culture de la sécurité et réduire le risque humain. Pour en savoir plus, consultez la page www.KnowBe4.com/fr

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