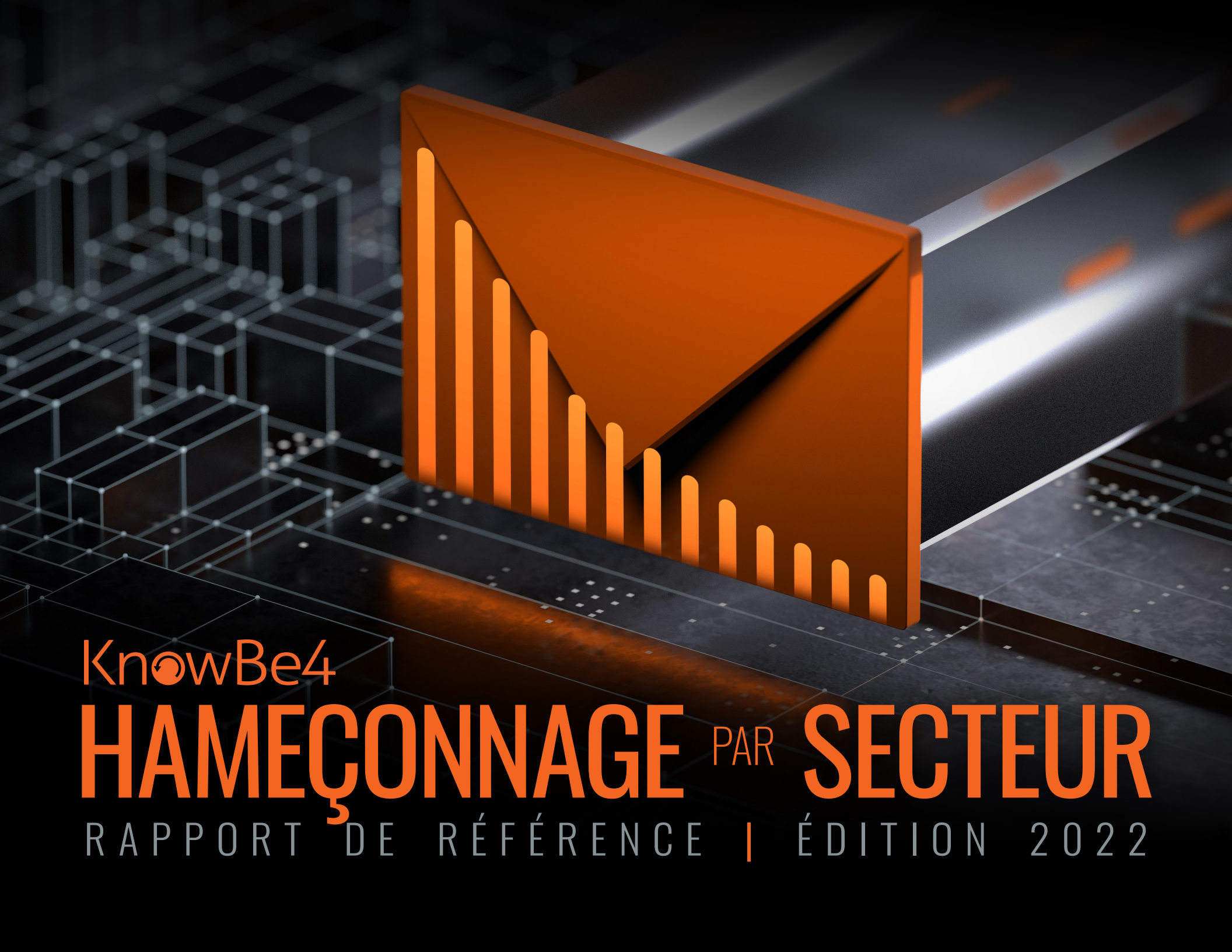


KnowBe4

HAMEÇONNAGE PAR SECTEUR

RAPPORT DE RÉFÉRENCE | ÉDITION 2022

Le rapport d'enquête Verizon 2022 sur les violations de données (Data Breach Investigations Report, DBIR) révèle que « le facteur humain continue d'être à l'origine de violations. Cette année, il est impliqué dans 82 % des violations. Qu'il s'agisse d'utilisation d'identifiants volés, d'hameçonnage, d'usage abusif ou simplement d'erreurs, l'humain continue de jouer un rôle majeur dans les incidents et les violations. »

INTRODUCTION

L'humain reste le vecteur d'attaque préféré des cybercriminels. Malheureusement, la plupart des organisations continuent de négliger ce point d'entrée dont on peut facilement forcer l'accès. Comme les années précédentes, le nombre d'attaques par hameçonnage a considérablement augmenté en 2021 et atteint de nouveaux records dans le monde entier. Quels que soient le secteur d'activité, la taille ou la zone géographique de l'organisation, personne n'est épargné. La composante humaine a été attaquée dans la sphère professionnelle et personnelle. Les cybercriminels ne font pas de distinctions lorsqu'ils choisissent leurs victimes, leurs attaques soigneusement conçues leur permettant de les cibler lorsque celles-ci travaillent ou se divertissent, de jour comme de nuit, par le biais d'un large éventail de méthodes d'ingénierie sociale.

L'équipe Internet Crime Complaint Center (IC3) du FBI *a de nouveau enregistré un nombre de plaintes record de la part du public américain : 847 376 plaintes ont été déposées, soit une augmentation de 7 % par rapport à 2020, pour des pertes potentielles dépassant les 6,9 milliards de dollars.* En outre, les incidents de compromission de la messagerie d'entreprise représentaient *19 954 plaintes, avec des pertes ajustées de près de 2,4 milliards de dollars.* Et il ne s'agit là que des incidents qui ont été signalés.

Tous les secteurs s'efforcent de développer au mieux leur ligne de défense humaine afin de détecter, protéger et signaler les actions suspectes avant qu'il ne soit trop tard et que leurs systèmes soient corrompus.

La plupart des organisations considèrent la technologie comme la meilleure arme pour combattre les cybercriminels, sans mesurer qu'il est tout aussi important, si ce n'est plus, d'investir dans la sensibilisation des utilisateurs et l'intervention humaine. Le rapport d'enquête Verizon 2022 sur les violations de données (Data Breach Investigations Report, DBIR) révèle que *le facteur humain est impliqué dans 82 % de tous les incidents de sécurité,* ce qui prouve à quel point les utilisateurs sont exposés.

Les responsables de la sécurité qui continuent d'investir uniquement dans l'orchestration de la sécurité et des technologies complexes risquent de négliger une pratique exemplaire qui a fait ses preuves pour limiter la vulnérabilité : la formation sur la sensibilisation à la sécurité, associée à des tests fréquents de simulation d'ingénierie sociale. Non seulement cette approche permet de mieux préparer les utilisateurs pour combattre la cybercriminalité, mais elle dresse également les bases indispensables pour développer une culture de la sécurité solide au sein d'une organisation.

Alors que le monde commence enfin à se remettre de la pandémie de COVID-19, les attaques par ingénierie sociale sont toujours en hausse. Les e-mails, appels téléphoniques, SMS, réseaux sociaux et toute autre méthode de communication contribuent à sortir de l'infrastructure sécurisée des organisations, à l'heure où les employés et les utilisateurs en général sont plus distraits et exposés que jamais.

Introduction | Rapport « Phishing By Industry Benchmarking Study » | Calcul du pourcentage de Phish-prone™ par secteur | Valeurs de référence sur l'hameçonnage au niveau international | Les points à retenir | Les points à retenir pour les cadres | Commencer

Toute distraction peut facilement mener à un désastre. Les attaques par hameçonnage étant de plus en plus fréquentes, l'état d'esprit et les actions des employés jouent un rôle essentiel dans la stratégie de sécurité de l'ensemble des organisations. Les responsables de la sécurité doivent savoir ce qui se passe quand les employés reçoivent des e-mails d'hameçonnage : sont-ils susceptibles de cliquer sur le lien ? De tomber dans le piège et de transmettre des identifiants ? De télécharger une pièce jointe contenant un programme malveillant ? Vont-ils simplement ignorer l'e-mail ou le supprimer sans prévenir leur employeur ? Ou bien vont-ils signaler une suspicion d'attaque par hameçonnage et jouer un rôle actif dans la ligne de défense humaine ?

Le pourcentage de Phish-prone™ (pourcentage de vulnérabilité à l'hameçonnage), ou PPP, désigne la vulnérabilité aux attaques par hameçonnage de chaque employé d'une organisation. En traduisant le risque lié à l'hameçonnage par des indicateurs mesurables, les responsables peuvent quantifier le risque de violation et mettre en place une formation visant à réduire la surface d'attaque humaine.

Analyse du risque par secteur

Le PPP d'une organisation indique combien de ses employés sont susceptibles de tomber dans le piège d'une attaque par ingénierie sociale ou hameçonnage. Il s'agit des employés pouvant être amenés à cliquer sur un lien, à ouvrir un fichier infecté par un programme malveillant ou à transférer des fonds de l'entreprise sur le compte bancaire d'un cybercriminel. Plus le PPP est élevé, plus le risque est grand, car cela signifie que davantage d'employés ont tendance à se laisser piéger. À l'inverse, un faible PPP est optimal, puisque cela démontre que le personnel possède les bons réflexes en matière de sécurité et sait reconnaître et désamorcer ces tentatives.

En d'autres termes, un PPP peu élevé signifie que la ligne de défense humaine d'une organisation agit pour sa sécurité au lieu de la mettre en péril. Le PPP global est encore plus riche en enseignements lorsqu'il est mis en contexte. Lorsqu'ils découvrent leur PPP, de nombreux responsables se posent des questions telles que « Comment mon organisation se classe-t-elle par rapport aux autres ? » ou « Que pouvons-nous faire pour réduire notre pourcentage de Phish-prone et renforcer notre ligne de défense humaine ? »

KnowBe4, le fournisseur de la plus grande plateforme mondiale de formation sur la sensibilisation à la sécurité et de simulation d'hameçonnage, a aidé des dizaines de milliers d'organisations à devenir moins vulnérables en formant leurs employés à reconnaître les escroqueries courantes et à réagir de manière appropriée.

Pour permettre aux organisations de bien évaluer leur PPP et de comprendre ce qu'implique leur classement, KnowBe4 mène une enquête annuelle visant à fournir des données de référence Phish-Prone reconnues pour l'ensemble des secteurs. Segmentée par secteur et taille d'organisation, cette étude met en évidence des schémas pouvant ouvrir la voie à un futur plus fort, plus sûr et plus sécurisé.

RAPPORT « GLOBAL PHISHING BY INDUSTRY BENCHMARKING STUDY » 2022

Toutes les organisations tentent de répondre à une question essentielle : « Comment nous classons-nous par rapport aux organisations semblables à la nôtre ? » Pour leur apporter une réponse nuancée et précise, le rapport « Phishing By Industry Benchmarking Study » 2022 a analysé les données de plus de 9,5 millions d'utilisateurs au sein de 30 173 organisations. Plus de 23,4 millions de tests de sécurité vis-à-vis de l'hameçonnage simulés ont été réalisés dans 19 secteurs différents.

Méthodologie utilisée pour l'étude de cette année

Toutes les organisations ont été classées par type de secteur et par taille. Afin de calculer le PPP de chaque organisation, nous avons déterminé le nombre d'employés ayant cliqué sur un lien contenu dans un e-mail de simulation d'hameçonnage ou ouvert une pièce jointe infectée au cours d'une campagne de test basée sur la plateforme KnowBe4.

Dans notre rapport 2022, nous continuons d'étudier trois phases de référence :

- **Phase une :** Résultats du test de sécurité vis-à-vis de l'hameçonnage de référence
- **Phase deux :** Résultats du test de sécurité vis-à-vis de l'hameçonnage dans les 90 jours suivant une formation
- **Phase trois :** Résultats du test de sécurité vis-à-vis de l'hameçonnage après un an ou plus de formation continue

ANALYSE DE L'IMPACT DE LA FORMATION

Pour comprendre l'impact de la formation sur la sensibilisation à la sécurité, nous avons mesuré les résultats lors de ces trois points de contact pour répondre aux questions suivantes :

PHASE UNE

Si vous n'avez pas formé vos utilisateurs et que vous envoyez une attaque par hameçonnage, quel est le PPP initial obtenu ?

1

Pour cela, nous avons évalué la vulnérabilité d'un employé face à un test de sécurité vis-à-vis de l'hameçonnage simulé initial de référence. Parmi ce groupe défini d'utilisateurs, nous avons relevé chaque échec d'un utilisateur à un test de sécurité vis-à-vis de l'hameçonnage simulé exécuté avant la réalisation d'une formation.

PHASE DEUX

Quel est le PPP obtenu lorsque vos utilisateurs effectuent une formation et qu'ils reçoivent des tests de sécurité vis-à-vis de l'hameçonnage simulés dans les 90 jours suivant cette formation ?

2

Nous avons répondu à cette question en identifiant à quel moment les utilisateurs avaient effectué leur première étape de formation et en recherchant tous les événements de sécurité vis-à-vis de l'hameçonnage simulés exécutés jusqu'à 90 jours après la réalisation de cette formation.

PHASE TROIS

Quel est le PPP final obtenu lorsque vos utilisateurs suivent une formation continue et reçoivent chaque mois des tests d'hameçonnage simulés ?

3

Pour répondre à cette question, nous avons évalué les compétences liées à la sensibilisation à la sécurité après 12 mois ou plus de formation continue et de tests de sécurité vis-à-vis de l'hameçonnage simulés. Nous avons recherché les utilisateurs ayant effectué une formation au moins un an plus tôt et analysé les résultats de performance obtenus lors de leur tout dernier test d'hameçonnage.

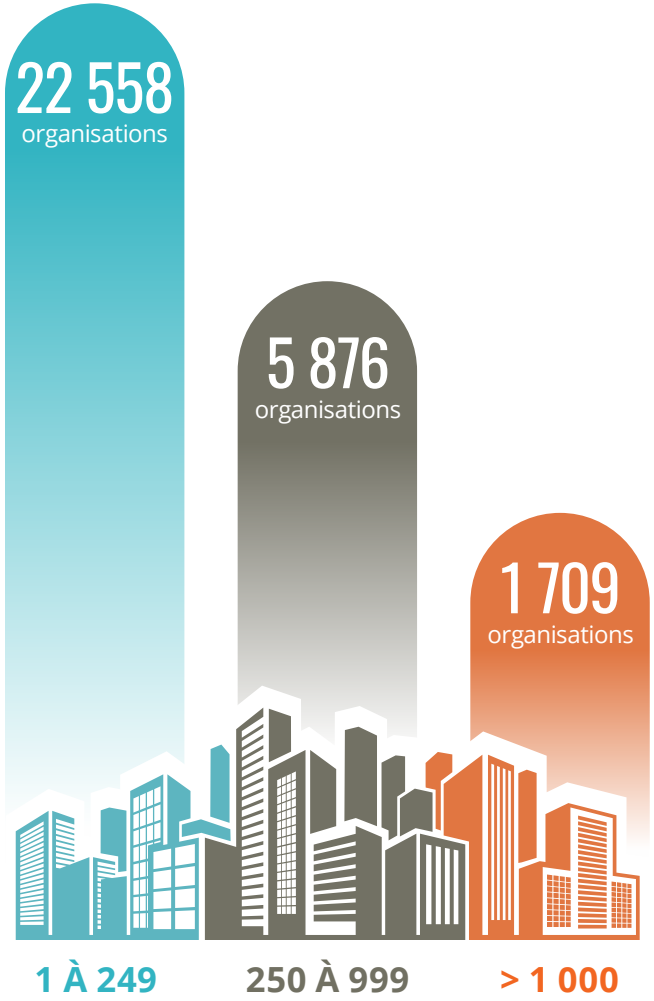
MÉTHODOLOGIE ET JEU DE DONNÉES

23,4 millions de tests de sécurité vis-à-vis de l'hameçonnage

9,5 millions d'utilisateurs

30,1 milliers d'organisations

TAILLE DES ORGANISATIONS



19 SECTEURS

- Banque
- Services aux entreprises
- Construction
- Conseil
- Services aux consommateurs
- Enseignement
- Énergie et services publics
- Services financiers
- Administration publique
- Santé et produits pharmaceutiques
- Hôtellerie
- Assurance
- Juridique
- Industrie
- Caritatif
- Autre
- Vente au détail et en gros
- Technologie
- Transport

Introduction | Rapport « Phishing By Industry Benchmarking Study » | Calcul du pourcentage de Phish-prone™ par secteur | Valeurs de référence sur l'hameçonnage au niveau international | Les points à retenir | Les points à retenir pour les cadres | Commencer

QUI EST EN DANGER : CLASSEMENT DE LA VULNÉRABILITÉ PAR SECTEUR

Les résultats obtenus pour les 9,5 millions d'utilisateurs mettent en lumière une réalité bien trop courante : l'incapacité des organisations à former efficacement leurs employés entraîne un manque de préparation et une certaine vulnérabilité face aux attaques par ingénierie sociale. Bien qu'elles soient légèrement plus favorables qu'en 2021, les données relatives au pourcentage de Phish-prone continuent d'indiquer qu'aucune organisation, quels que soient sa taille et son secteur d'activité, n'est réellement armée pour reconnaître les stratégies d'ingénierie sociale et d'hameçonnage des cybercriminels. Lorsque les utilisateurs n'ont pas été testés ou formés, les tests de sécurité de référence initiaux vis-à-vis de l'hameçonnage révèlent dans quelle mesure les employés de ces secteurs sont susceptibles d'être victimes d'une escroquerie par hameçonnage et de faire subir une violation potentielle à leur organisation.

Le PPP global pour tous les secteurs et toutes les tailles d'organisation est de **32,4 %** en 2022, soit un point de plus qu'en 2021. Les tendances varient entre les différents secteurs, ce qui met en évidence une triste vérité : les utilisateurs non formés ne jouent pas leur rôle en tant que dernière ligne de défense de l'organisation face aux attaques par hameçonnage.

- Parmi les organisations de petite taille (de 1 à 249 employés), le **secteur de l'enseignement**, bien que légèrement plus performant qu'en 2021, commence l'année 2022 avec un **PPP de 32,7 %**. Vient ensuite **la santé et les produits pharmaceutiques** avec un **PPP de 32,5 %**. La **vente au détail et en gros** détrône le secteur caritatif à la dernière place avec un **PPP de 31,5 %**.
- Pour les organisations de taille moyenne (de 250 à 999 employés), les trois secteurs de tête restent les mêmes qu'en 2021. L'**hôtellerie** conserve son PPP de 2021, soit **39,4 %**. Le secteur de **la santé et des produits pharmaceutiques** arrive ensuite avec un **PPP de 36,6 %**, suivi de l'**énergie et des services publics** à **34 %**, ces secteurs ayant échangé de position. Il est à noter que ces trois secteurs présentent des PPP plus performants par rapport aux chiffres de 2021, bien qu'ils restent les plus à risque.

Qui est en danger ?

Trois premiers secteurs d'activité par taille d'organisation

PETITE 1 à 249	MOYENNE 250 à 999	GRANDE > 1 000
32,7 % Enseignement	**39,4 %** Hôtellerie	**52,3 %** Assurance
32,5 % Santé et produits pharmaceutiques	**36,6 %** Santé et produits pharmaceutiques	**52,2 %** Conseil
31,5 % Vente au détail et en gros	**34 %** Énergie et services publics	**50,9 %** Énergie et services publics

- Pour les organisations de grande taille (1 000 employés et plus), l'énergie et les services publics ont cédé la première place au secteur de l'**assurance** (second en 2021) avec un **PPP de 52,3 %**. Le **secteur du conseil**, nouveau dans le classement, arrive ensuite avec un **PPP de 52,2 %**, tandis que l'**énergie et les services publics** complètent le groupe avec un **PPP de 50,9 %**. Le secteur bancaire sort du trio de tête en 2022.
- Voici les gagnants du pourcentage de Phish-prone de référence le plus faible : il s'agit du secteur de la **banque** avec un **PPP de 25,4 %** pour les organisations de petite taille (de 1 à 249 employés), de l'**administration publique** avec un **PPP de 26,4 %** pour les organisations de taille moyenne, et de l'**hôtellerie** avec un **PPP de 20,4 %** pour les organisations de grande taille. Bien que ces PPP soient les résultats les moins élevés de l'étude, ils montrent clairement qu'une base d'utilisateurs non formée reste vulnérable face aux attaques par hameçonnage.

PHASE UNE : RÉSULTATS DU TEST DE SÉCURITÉ VIS-À-VIS DE L'HAMEÇONNAGE DE RÉFÉRENCE

Le test de sécurité de référence initial vis-à-vis de l'hameçonnage a été exécuté au sein des organisations n'ayant mené aucune campagne de formation sur la sensibilisation à la sécurité par le biais de la plateforme KnowBe4. Les utilisateurs n'ont reçu aucun avertissement, et les tests ont été effectués sur des employés non formés dans le cadre de leurs activités professionnelles courantes. Les résultats continuent d'indiquer des niveaux de risque élevés année après année :

- Tous secteurs et tailles d'organisation confondus, le pourcentage de Phish-prone moyen est de **32,4 %**, soit un point de plus qu'en 2021. **Cela signifie qu'un employé sur trois est susceptible de cliquer sur un e-mail ou un lien suspect ou de répondre favorablement à une demande malveillante**, des résultats proches de ceux de l'année dernière.
- Les données de 2022 montrent que l'amélioration la plus significative a été observée pour les **grandes entreprises du secteur de la construction**, qui ont enregistré une belle progression puisque leur PPP est passé **de 42,7 % à 37 %**. À l'inverse, c'est pour les **grandes entreprises de conseil** que le recul a été le plus sévère, leur PPP ayant augmenté de **28,4 % en 2021 à 52,2 % en 2022**.
- La principale inquiétude vient des PPP des secteurs suivants, tous supérieurs à 40 %, dans la catégorie des organisations de grande taille : **Banque 43,5 %, Santé et produits pharmaceutiques 45 %, Énergie et services publics 50,9 %, Conseil 52,2 %, Assurance 52,3 %**. Cela signifie que les employés de ces catégories présentent un risque élevé d'être victimes d'attaques par ingénierie sociale, avec un PPP parfois supérieur à 50 %.

Observations : À mesure que les cybermenaces augmentent, la communication autour de ces attaques touche les utilisateurs en masse par le biais des réseaux sociaux et des médias d'information. Dans certains domaines, le public reçoit un flux de renseignements plus fourni, ce qui accroît naturellement son niveau de sensibilisation. Reste à savoir si ces connaissances de base vont parvenir jusqu'au lieu de travail et se développer en compétences plus poussées et instinctives par le biais de la formation. Sans programme de formation et de consolidation, toutes les organisations, quels que soient leur taille et leur secteur d'activité, sont vulnérables face à l'hameçonnage et à l'ingénierie sociale. Dans tous les secteurs, les employés constituent une porte d'entrée possible pour les pirates, même avec un investissement massif dans des technologies de sécurité de classe mondiale.

Phase une

32,4 %

Résultats du test de sécurité de référence initial vis-à-vis de l'hameçonnage

Taille de l'organisation	PPP initial
1 à 249	28,8 %
250 à 999	30,2 %
> 1 000	35,2 %

Secteur	1 à 249 employés	250 à 999 employés	> 1 000 employés
Banque	25,4 %	27,3 %	43,5 %
Services aux entreprises	27,4 %	30 %	29,2 %
Construction	29,6 %	32,9 %	37 %
Conseil	27,5 %	30,6 %	52,2 %
Services aux consommateurs	30,4 %	29,1 %	24,3 %
Enseignement	32,7 %	29,3 %	28,4 %
Énergie et services publics	29,4 %	34 %	50,9 %
Services financiers	26,4 %	28,7 %	35,9 %
Administration publique	28 %	26,4 %	24,8 %
Santé et produits pharmaceutiques	32,5 %	36,6 %	45 %
Hôtellerie	28,5 %	39,4 %	20,4 %
Assurance	26,2 %	30,3 %	52,3 %
Juridique	27,3 %	27,6 %	29,2 %
Industrie	29,5 %	29,5 %	33,1 %
Caritatif	29,6 %	30,8 %	36,5 %
Autre	30,5 %	31,9 %	26,8 %
Vente au détail et en gros	31,5 %	30,6 %	38,6 %
Technologie	26,7 %	28,2 %	33,2 %
Transport	27 %	32 %	24,8 %

PHASE DEUX : RÉSULTATS DU TEST DE SÉCURITÉ VIS-À-VIS DE L'HAMEÇONNAGE DANS LES 90 JOURS SUIVANT UNE FORMATION

Lorsque les organisations ont mis en place un programme mêlant formation et tests de sécurité vis-à-vis de l'hameçonnage après leur évaluation de référence initiale, les résultats ont évolué de manière significative. Nous avons découvert qu'une fois que les utilisateurs ont effectué leur premier événement de formation, les résultats du test de sécurité vis-à-vis de l'hameçonnage simulé réalisé jusqu'à 90 jours après la formation sont plus favorables. Durant ces 90 jours suivant l'exécution des événements de formation, le pourcentage de Phish-prone moyen a presque été divisé par deux pour atteindre 17,6 %, ce qui corrobore les résultats des études menées ces trois dernières années. Si la diminution considérable des pourcentages de Phish-prone n'est pas liée à un secteur ou à une taille d'organisation spécifique, voici quelques points de données intéressants :

- La baisse la plus importante est observée dans les organisations suivantes : pour les organisations de petite taille (de 1 à 249 employés), l'**enseignement** enregistre une **baisse de 46 %**, passant de 32,7 % pour le résultat de référence à 17,9 % dans les 90 jours suivant la formation ; pour les organisations de taille moyenne (de 250 à 999 employés), l'**hôtellerie** enregistre une **baisse de 51 %**, passant de 39,4 % à 19,4 % ; et pour les organisations de grande taille (1 000 employés et plus), l'**assurance** enregistre une **baisse de 67 %**, passant de 52,3 % à 17,3 %, après avoir obtenu l'un des PPP de référence initial les plus élevés.
- La diminution significative **de 32,4 % à 17,6 %** tous secteurs confondus prouve qu'un programme de formation sur la sensibilisation à la sécurité peut s'avérer particulièrement payant, puisque cela permet de développer une ligne de défense humaine solide dans le cadre de votre stratégie de sécurité informatique en profondeur, et ce dès les trois premiers mois.

Observations : Après seulement 90 jours de formation sur la sensibilisation à la sécurité nouvelle génération, nous avons constaté une nette amélioration de la capacité des employés à détecter les e-mails malveillants, tous secteurs et tailles d'organisation confondus. C'est d'autant plus parlant si l'on compare cela à un régime alimentaire. En effet, cela équivaudrait à attendre 90 jours avant de voir des résultats. Dans ce même laps de temps, vos employés nouvellement formés sur 90 jours peuvent réduire de près de moitié le risque que votre organisation subisse une violation aux conséquences néfastes pour votre image ou vos revenus. Un investissement de 90 jours suffit à être mieux préparé et à limiter les risques. Comme pour tout changement important, oublier les vieilles habitudes pour en prendre de nouvelles demande du temps. Cependant, une fois qu'elles ont été adoptées, elles deviennent la nouvelle norme. Elles font alors partie de la culture de l'organisation et influencent le comportement des autres employés, en particulier des nouveaux arrivants, qui observent leurs collègues pour déterminer ce qui est socialement et culturellement acceptable dans leur nouvel environnement professionnel.

Phase deux

17,6 %

Résultats du test de sécurité vis-à-vis de l'hameçonnage dans les 90 jours suivant une formation

Taille de l'organisation	PPP à 90 jours
1 à 249	17,5 %
250 à 999	17,9 %
> 1 000	17,4 %

Secteur	1 à 249 employés	250 à 999 employés	> 1 000 employés
Banque	12,3 %	13,6 %	15,6 %
Services aux entreprises	18,3 %	18,6 %	17,7 %
Construction	19,5 %	20 %	15,8 %
Conseil	17,5 %	20,1 %	21,3 %
Services aux consommateurs	18,8 %	21 %	16,1 %
Enseignement	17,9 %	18,5 %	18,8 %
Énergie et services publics	16,8 %	17,2 %	16,4 %
Services financiers	15,1 %	16 %	19,1 %
Administration publique	16 %	15,5 %	15,2 %
Santé et produits pharmaceutiques	19,7 %	19,1 %	17,2 %
Hôtellerie	19,7 %	19,4 %	12,2 %
Assurance	17,7 %	17,5 %	17,3 %
Juridique	16,5 %	15,9 %	13 %
Industrie	17,7 %	17 %	16,5 %
Caritatif	20,3 %	20,8 %	18,2 %
Autre	19 %	21,4 %	20,1 %
Vente au détail et en gros	18,3 %	18,1 %	18,1 %
Technologie	18,9 %	18,8 %	19,2 %
Transport	18,5 %	18,7 %	16,5 %

PHASE TROIS : RÉSULTATS DU TEST DE SÉCURITÉ VIS-À-VIS DE L'HAMEÇONNAGE APRÈS UN AN OU PLUS DE FORMATION CONTINUE

Durant cette étape, nous avons mesuré les compétences liées à la sensibilisation à la sécurité après 12 mois ou plus de formation continue et de tests de sécurité vis-à-vis de l'hameçonnage simulés. Nous avons recherché les utilisateurs ayant effectué une formation au moins un an plus tôt et analysé les résultats de performance obtenus lors de leur tout dernier test d'hameçonnage. Année après année, les résultats restent remarquables et indiquent que la mise en place d'un programme de formation sur la sensibilisation continu et complet permet de réduire le PPP moyen de 32,4 % à **5 %. Ces résultats ont été largement observés, tous secteurs et tailles d'organisation confondus.**

Pour la deuxième année, c'est le secteur de la **banque** qui obtient le PPP le plus faible pour les organisations de petite taille (de 1 à 249 employés), avec **2,6 %**. Cela fait également deux ans que le secteur **bancaire** atteint le plus petit score PPP dans la catégorie de taille moyenne (de 250 à 999 employés), avec **3,3 %**. Dans la catégorie des organisations de grande taille (1 000 employés et plus), pour la deuxième année là aussi, l'**hôtellerie** obtient un PPP de **1,3 %**, marquant une diminution favorable par rapport à ses 4 % de 2021. La banque étant l'un des secteurs les plus attaqués et réglementés, ces chiffres sont sans doute le fruit de son intervention précoce pour lutter contre la cybercriminalité et de sa politique assidue de formation.

Il ressort de la comparaison des données que la meilleure amélioration globale revient à la catégorie des organisations de grande taille (1 000 employés et plus) de deux secteurs : **le secteur de l'énergie et des services publics, qui est passé d'un PPP de référence de 50,9 % à un PPP de 3,6 % après au moins 12 mois de formation sur la sensibilisation à la sécurité, soit une diminution de 93 %, et le secteur du conseil, dont le PPP est passé de 52,2 % à 4,9 %, soit une baisse de 91 %.** Le secteur de l'énergie et des services publics, qui a subi l'une des plus grandes cyberattaques de l'histoire des États-Unis sur une infrastructure pétrolière (Colonial Pipeline), demeure une cible majeure à fort potentiel de destruction pour les cybercriminels. Le secteur du conseil est lui aussi largement visé. En août 2021, l'un des plus grands cabinets de conseil mondiaux a ainsi été la cible d'une attaque par rançongiciel d'un montant colossal de 50 millions de dollars, perpétrée par le groupe LockBit avec l'aide d'une source interne (menace interne).

Phase trois

5 % **Résultats du test de sécurité vis-à-vis de l'hameçonnage après un an ou plus de formation continue**

Taille de l'organisation	PPP à 12 mois
1 à 249	3,8 %
250 à 999	5 %
> 1 000	5,8 %

Secteur	1 à 249 employés	250 à 999 employés	> 1 000 employés
Banque	2,6 %	3,3 %	3,4 %
Services aux entreprises	3,8 %	5 %	6 %
Construction	4,1 %	4,8 %	4,6 %
Conseil	3,8 %	4,8 %	4,9 %
Services aux consommateurs	4,7 %	4,7 %	3,3 %
Enseignement	4,1 %	5,4 %	6,5 %
Énergie et services publics	3,4 %	5 %	3,6 %
Services financiers	3,7 %	4,9 %	5,5 %
Administration publique	3,9 %	3,9 %	7,1 %
Santé et produits pharmaceutiques	4,1 %	5,1 %	5,9 %
Hôtellerie	4,4 %	5,6 %	1,3 %
Assurance	3,3 %	4 %	5,3 %
Juridique	4,1 %	5,2 %	5,6 %
Industrie	3,3 %	5,3 %	6,2 %
Caritatif	4,1 %	4,9 %	4,5 %
Autre	3,2 %	4 %	6,2 %
Vente au détail et en gros	3,6 %	5,3 %	4,7 %
Technologie	4,7 %	5,9 %	7,2 %
Transport	4,1 %	9,6 %	4,5 %

TAUX D'AMÉLIORATION MOYENS PAR SECTEUR ET TAILLE D'ORGANISATION

Il ressort clairement qu'après un an ou plus de formation sur la sensibilisation à la sécurité associée à des tests d'hameçonnage simulés fréquents, **les organisations affichent une nette amélioration, toutes tailles et tous secteurs confondus**. Les organisations de 1 à 249 employés continuent d'enregistrer **la meilleure amélioration globale, qui atteint 85 % ou plus dans 17 secteurs sur 19**.

Parmi les organisations de taille moyenne, les taux d'amélioration sont bons, puisqu'ils **égalent ou dépassent 80 % dans 17 secteurs**, les deux autres arrivant légèrement sous la barre des 80 %. Du côté des organisations de grande taille, **14 secteurs présentent un taux d'amélioration supérieur à 80 %**, et les cinq autres se placent entre 71 % et 79 %.

Si l'on considère l'ensemble des secteurs et des catégories de tailles, le **taux moyen d'amélioration de 85 %** entre le test de référence et le résultat après un an de formation continue et de tests constitue **un argument de poids pour obtenir l'adhésion nécessaire à l'élaboration d'un programme de formation complet sur la sensibilisation à la sécurité.**

Tous secteurs confondus, KnowBe4 a découvert que 32,4 % des utilisateurs non formés échouent à un test d'hameçonnage.

Une fois formés, seuls 17,6 % des utilisateurs échouent à un test d'hameçonnage dans les 90 jours suivant leur première formation KnowBe4. Et, après au moins un an sur la plateforme KnowBe4, ils ne sont plus que 5 % à échouer.

Amélioration moyenne

85 %

Taux d'amélioration moyen par secteur et taille d'organisation

Secteur	1 à 249 employés	250 à 999 employés	> 1 000 employés
Banque	90 %	88 %	92 %
Services aux entreprises	86 %	83 %	79 %
Construction	86 %	85 %	88 %
Conseil	86 %	84 %	91 %
Services aux consommateurs	85 %	84 %	86 %
Enseignement	87 %	82 %	77 %
Énergie et services publics	88 %	85 %	93 %
Services financiers	86 %	83 %	85 %
Administration publique	86 %	85 %	71 %
Santé et produits pharmaceutiques	87 %	86 %	87 %
Hôtellerie	84 %	86 %	93 %
Assurance	87 %	87 %	90 %
Juridique	85 %	81 %	81 %
Industrie	89 %	82 %	81 %
Caritatif	86 %	84 %	88 %
Autre	90 %	87 %	77 %
Vente au détail et en gros	89 %	83 %	88 %
Technologie	83 %	79 %	78 %
Transport	85 %	70 %	82 %

VALEURS DE RÉFÉRENCE SUR L'HAMEÇONNAGE AU NIVEAU INTERNATIONAL EN 2022

Au niveau international, nous avons utilisé un jeu de données légèrement différent, sans segmentation par secteur, pour déterminer les valeurs de référence sur l'hameçonnage au niveau régional parmi les organisations de petite taille, de taille moyenne et de grande taille. Nous avons inclus les organisations pour lesquelles un pays spécifique était associé au compte client, afin qu'il puisse être pris en compte dans l'analyse de référence internationale. Nous avons appliqué les mêmes phases d'analyse comparative pour obtenir le jeu de données international que pour mesurer les pourcentages de Phish-prone.

Phase une

Résultats du test de sécurité de référence initial vis-à-vis de l'hameçonnage

Phase deux

Résultats du test de sécurité vis-à-vis de l'hameçonnage dans les 90 jours suivant une formation

Phase trois

Résultats du test de sécurité vis-à-vis de l'hameçonnage après un an ou plus de formation continue

		RÉFÉRENCE			90 JOURS			1 AN		
	Taille de l'organisation	1 à 249	250 à 999	> 1 000	1 à 249	250 à 999	> 1 000	1 à 249	250 à 999	> 1 000
RÉGION	Amérique du Nord	28,7 %	30,2 %	35,8 %	17,4 %	17,9 %	17,4 %	3,5 %	4,6 %	6 %
			TOTAL : 32,4 %			**TOTAL : 17,5 %**			**TOTAL : 4,7 %**	
	Afrique	30,2 %	27,4 %	32,4 %	24,8 %	21 %	17,9 %	8,1 %	12,7 %	4 %
			TOTAL : 31,4 %			**TOTAL : 18,8 %**			**TOTAL : 5,4 %**	
	APAC (Asie, Océanie et Australie)	30,2 %	32,6 %	36,7 %	21,1 %	19,2 %	15 %	4,4 %	6,2 %	5,2 %
			TOTAL : 34,5 %			**TOTAL : 16,9 %**			**TOTAL : 5,4 %**	
	Europe	27,8 %	28,2 %	31,1 %	17,9 %	18,2 %	18,9 %	4,2 %	6,7 %	8 %
			TOTAL : 29,9 %			**TOTAL : 18,5 %**			**TOTAL : 6,3 %**	
	Amérique du Sud	30,9 %	30 %	45,6 %	24,7 %	22,2 %	19,3 %	1,8 %	9,8 %	0,8 %
			TOTAL : 39,9 %			**TOTAL : 20,5 %**			**TOTAL : 3,2 %**	
	Royaume-Uni et Irlande	26,2 %	27,7 %	32,7 %	16,7 %	16,2 %	17,5 %	3,9 %	4,3 %	8,3 %
			TOTAL : 30 %			**TOTAL : 17 %**			**TOTAL : 5,5 %**	

AMÉRIQUE DU NORD

Problèmes les plus fréquents

Les rançongiciels se démarquent clairement comme l'une des principales cybermenaces auxquelles sont confrontées les organisations sur l'ensemble des secteurs et des tailles. Non seulement ces programmes malveillants ont pour effet d'interrompre les opérations des organisations, mais ils font également peser le risque que les informations des clients et des employés soient divulguées sur Internet. En outre, dans de nombreux cas, le public a connaissance des violations de ce type, notamment quand les sites Web sont dégradés, que les services sont suspendus ou que les bureaux restent fermés pendant la procédure de rétablissement, ce qui peut avoir un impact considérable sur la réputation d'une organisation.

La situation peut s'aggraver lorsque les groupes à l'origine des attaques par rançongiciel contactent les clients de l'organisation victime et utilisent sa base de clientèle comme moyen de pression supplémentaire pour l'inciter à payer la rançon. Contrairement aux premiers rançongiciels qui étaient presque entièrement automatisés, les versions modernes impliquent souvent un important niveau d'interaction humaine, pour mapper les systèmes essentiels, créer des portes dérobées et voler les données qui causeront le plus de dommages. Dans certains cas, on sait que les personnes malveillantes ont consulté au préalable les politiques de cyberassurance et les informations financières de l'organisation pour déterminer avec précision un montant de rançon que celle-ci pourrait se permettre de payer. Ces activités ont toutes contribué à la multiplication des demandes de rançon, qui battent aujourd'hui des records.

En plus des rançongiciels, la compromission de la messagerie d'entreprise (BEC), également connue sous le nom de fraude de PDG, continue de sévir en Amérique du Nord. Ces attaques se font par vishing (hameçonnage vocal), hameçonnage par e-mail et smishing (hameçonnage par SMS) et sont particulièrement efficaces. Contrairement aux rançongiciels, elles n'utilisent généralement pas de liens ou de documents infectés par des programmes malveillants, ces derniers pouvant être repérés par les contrôles techniques. Ces attaques sont presque exclusivement exécutées par le biais de l'ingénierie sociale. Des demandes de cartes-cadeaux aux transferts de sommes importantes, ces attaques continuent de frapper les organisations de toutes les tailles et de tous les secteurs, directement au portefeuille.

Même lorsqu'elles aboutissent, elles sont bien moins visibles par le grand public, car elles n'impactent généralement pas les opérations courantes. Cela les rend difficiles à détecter, à moins que les organisations décident de dévoiler publiquement les pertes subies, ce qui est rarement le cas si rien ne les y oblige.

Pour les organisations qui opèrent dans des secteurs très réglementés, les attaques réussies sont souvent révélées lors du dépôt des rapports financiers trimestriels ou annuels.

Cela est particulièrement vrai au Mexique, où l'économie en pleine croissance associée à l'essor rapide du numérique a engendré des défis persistants qui mettent quotidiennement à l'épreuve la culture de la cybersécurité. Le rapport « Internet Crime Report 2021 » publié par le FBI classe le Mexique en 13e position des pays les plus ciblés au monde, deuxième à l'échelle de l'Amérique latine, avec une augmentation constante du nombre d'incidents signalés ces dernières années. Pour plus d'informations sur le Mexique, consultez la section dédiée à l'Amérique du Sud dans ce rapport.

Impact économique

Avec un montant versé de 570 000 $ en moyenne suite aux attaques par rançongiciel en 2021 et des pertes record de 1,8 milliard de dollars en 2020 dans le cadre des compromissions de la messagerie d'entreprise selon le FBI, une cyberattaque peut clairement signer la fin de nombreuses organisations. Si la cyberassurance peut quelque peu aider à contrôler l'hémorragie financière, beaucoup de compagnies augmentent fortement leurs tarifs, exigent un respect strict des pratiques exemplaires, refusent de couvrir entièrement les organisations ou font tout pour limiter les sommes payées en cas de cyberattaque réussie.

Avec des demandes de rançon qui dépassent parfois 50 millions de dollars, rares sont les organisations qui peuvent ignorer cette menace. Par ailleurs, à l'issue d'une attaque par programme malveillant ou rançongiciel, les organisations doivent prendre des mesures d'enquête numérique particulièrement coûteuses pour identifier le vecteur d'infection initial et fermer les portes dérobées laissées ouvertes par les pirates. Si elles ne parviennent pas à repérer et à résoudre les failles potentielles susceptibles de permettre une nouvelle attaque, elles restent en sursis.

Profil d'organisation type

En Amérique du Nord, les organisations de toutes tailles sont confrontées à un manque de ressources et de financement pour lutter contre la cybercriminalité. C'est particulièrement vrai pour les organisations de petite et moyenne tailles, qui ne peuvent pas toujours se permettre d'avoir un spécialiste de la cybersécurité à temps plein dans leur équipe. Bon nombre d'entre elles pensent qu'elles sont trop petites pour intéresser les cybercriminels. Elles ont malheureusement tort, surtout à l'époque des rançongiciels, à l'heure où

vos données ont une valeur inestimable pour les organisations qui veulent rester dans la course. Si le coût de l'embauche d'un expert en cybersécurité est prohibitif pour de nombreuses petites organisations, celles-ci peuvent faire appel à des partenaires de distribution pour gérer leurs outils de sécurité et même leurs programmes de formation et de sensibilisation, une approche qui peut s'avérer très rentable.

Quel que soit le type d'attaque spécifique, un cyberincident peut avoir de graves conséquences pour les organisations impliquées dans des procédures de fusion-acquisition. Une attaque réussie peut faire chuter le prix de l'organisation en cours de rachat, générer des problèmes avec les organismes de réglementation tels que la Securities and Exchange Commission (SEC), ou encore vider les coffres de l'organisation qui effectue l'acquisition, tout ceci pouvant rapidement mettre un terme à l'opération.

Adoption culturelle

Les programmes de formation et de sensibilisation sont de plus en plus complets. Ils visent à faire évoluer le comportement des employés et à générer un changement positif dans la culture de la sécurité globale de l'organisation, et non simplement à fournir des informations. Ils fonctionnent souvent de la même manière et imitent le système des campagnes marketing qui ciblent les clients potentiels et existants.

Cela permet une diffusion de contenus régulière, au lieu d'un déferlement d'informations une fois par an. Cette approche permet d'ancrer les informations chez les utilisateurs et d'avoir un impact positif sur leur comportement. Concrètement, en Amérique du Nord, la formation et la sensibilisation des employés se sont considérablement développées jusqu'à devenir une méthode clé pour sécuriser les organisations. Selon le rapport « Security Culture Report » 2022 de KnowBe4, la région Amérique du Nord a obtenu un score plus élevé que le reste du monde, avec une moyenne de 74 (sur 100). Ce score de culture de la sécurité reflète les idées, les habitudes et les comportements sociaux ayant un impact sur la sécurité d'une organisation.

Comportement général

En Amérique du Nord, bon nombre d'organisations ont pris conscience des risques liés au facteur humain et ont commencé à s'atteler au problème en fournissant à leurs employés les connaissances, la formation et les compétences nécessaires pour qu'ils puissent se protéger, ainsi que leur organisation, des attaques utilisées par les personnes malveillantes.

Les points à retenir

Il est clair que le problème de la cybercriminalité ne peut pas être ignoré et ne va pas disparaître de si tôt. L'impact financier et opérationnel est tout simplement trop important pour être ignoré par les organisations, même les plus grandes. Si la cyberassurance peut atténuer légèrement les pertes, cela ne peut raisonnablement pas se substituer à des méthodes de prévention et de rétablissement appropriées et ne résout pas les dommages qu'une attaque de grande ampleur peut causer sur la réputation.

Bien que la technologie joue un rôle majeur dans la prévention et la récupération, le facteur humain est de loin le point d'accès initial au réseau le plus courant. En d'autres termes, c'est le plus souvent au niveau humain qu'une tentative d'attaque devient une intrusion réussie. La plupart des organisations d'Amérique du Nord ont commencé à prendre conscience de ce danger et à s'intéresser de près à la façon dont elles peuvent aider les employés à faire barrage face aux attaques permanentes des personnes malveillantes. En plus de constater une baisse significative des incidents liés à l'hameçonnage par e-mail grâce à la sensibilisation à la sécurité, elles misent également sur la formation pour transformer la culture de la sécurité globale et développent des campagnes de formation à long terme dans ce but.

AMÉRIQUE DU NORD	RÉFÉRENCE	90 JOURS	1 AN
1 à 249	28,7 %	17,4 %	3,5 %
250 à 999	30,2 %	17,9 %	4,6 %
> 1 000	35,8 %	17,4 %	6 %
PPP moyen toutes tailles confondues	32,4 %	17,5 %	4,7 %

ROYAUME-UNI ET IRLANDE

Problèmes les plus fréquents

En 2021, nous avons appris à vivre avec la pandémie mondiale qui a envahi notre vie privée et professionnelle. Le télétravail est devenu la norme, et les sociétés britanniques et irlandaises se sont adaptées à la situation. Par ailleurs, le mois de janvier 2021 a marqué la fin officielle de la période de transition du Brexit, ce qui a suscité des préoccupations concernant la perte des capacités de partage de données et de protection propres à l'Union européenne.

La région reste la cible d'attaques constantes de la part de groupes criminels basés en Russie. Selon le National Cyber Security Centre (NCSC), la Chine demeure un acteur très complexe du cyberespace, portée par une ambition croissante de projeter son influence au-delà des frontières et un intérêt manifeste pour les secrets commerciaux du Royaume-Uni. La façon dont la Chine va évoluer durant la prochaine décennie sera probablement le principal élément qui façonnera la cybersécurité du futur au Royaume-Uni et en Irlande.

En 2021, le rançongiciel a conservé sa place de principale menace publique. Au mois de mai 2021, une attaque par rançongiciel perpétrée contre le Health Service Executive (HSE), le système de santé publique irlandais, a perturbé le réseau informatique de soins et les hôpitaux. L'organisation a mis quatre mois à se rétablir totalement de l'attaque, ce qui a eu de graves conséquences sur la vie des patients et de leurs familles.

La compromission de l'éditeur de logiciel SolarWinds et l'exploitation des serveurs Microsoft Exchange a mis en lumière la menace liée aux attaques de la chaîne d'approvisionnement, de nombreuses organisations britanniques et irlandaises ayant été impactées.

Dans l'ensemble, les stratégies déployées par les pirates sont sensiblement les mêmes que celles observées les années précédentes. L'ingénierie sociale, l'exploitation des failles de logiciel non corrigées et la violation d'identifiants peu sécurisés restent les principaux vecteurs d'attaque. Avec le travail hybride et à domicile, la surface d'attaque par ingénierie sociale s'est étendue, les pirates agissant couramment par le biais du téléphone fixe, des SMS, des réseaux sociaux ou des e-mails, que ce soit sur les comptes personnels ou professionnels.

Impact économique

L'impact économique de la cybercriminalité est toujours difficile à estimer en raison du manque de cohérence dans son évaluation et dans le signalement des incidents.

Le National Fraud Intelligence Bureau reçoit l'ensemble des signalements de cybercrimes transmis au centre Action Fraud. Les statistiques établies par cette agence indiquent que près d'un demi-million de signalements ont été effectués, pour un montant de pertes total de 2,6 milliards de livres.

Parmi les incidents signalés en 2021, environ 86 000 étaient liés à des ventes aux enchères et achats en ligne. En outre, concernant la cybercriminalité, près de 14 000 signalements de piratage par e-mail et via les réseaux sociaux ont été enregistrés.

En réalité, ce chiffre ne représente certainement même pas la partie émergée de l'iceberg et ne traduit donc pas l'impact économique réel de la cybercriminalité. Cela se compte probablement en dizaine de milliards de livres chaque année pour l'économie britannique et irlandaise.

Profil d'organisation type

Selon les chiffres officiels du gouvernement du Royaume-Uni, 75 % des entreprises britanniques n'avaient aucun employé à l'exception de leur propriétaire en 2021, alors que plus de 99 % des sociétés étaient des PME (petites et moyennes entreprises) de 0 à 249 personnes.

Le secteur des services représentait 76 % des entreprises, et 16 % des PME étaient dirigées par des femmes. Aucun conseil d'administration d'entreprises du FTSE100 n'était exclusivement masculin.

Adoption culturelle

Le rapport « Security Culture Report 2022 » de KnowBe4 montre que la région Royaume-Uni et Irlande affiche des performances relativement bonnes, avec un score d'indice de la culture de la sécurité de 74 (sur 100) pour le Royaume-Uni et de 78 (sur 100) pour l'Irlande. Ce score de culture de la sécurité reflète les idées, les habitudes et les comportements sociaux ayant un impact sur la sécurité d'une organisation.

Comportement général

Le Department for Digital, Culture, Media & Sport (DCMS) mène une enquête annuelle sur la sensibilisation à la cybersécurité et les comportements dans ce domaine. D'après les résultats de l'enquête, les trois quarts des entreprises (77 %) et sept associations caritatives sur dix (68 %) affirment que la cybersécurité est une priorité pour leur équipe de direction. Ces deux groupes se répartissent de manière relativement égale entre les répondants qui estiment cette priorité « très élevée » et ceux qui l'estiment « assez élevée ».

Selon l'étude « Cyber Security Breaches Survey » menée en 2021 par le gouvernement du Royaume-Uni, les grandes entreprises affirment couramment que la cybersécurité est une priorité élevée (95 % des entreprises de taille moyenne et 93 % des entreprises de grande taille contre 77 % en moyenne). Cela vaut également pour les associations caritatives à revenus élevés (96 % de celles qui gagnent 500 000 £ ou plus contre 68 % de l'ensemble des associations).

Les secteurs commerciaux qui accordent une priorité plus élevée à la cybersécurité sont les suivants :

- Finance et assurance (72 % affirment que c'est une priorité très élevée contre 37 % de toutes les entreprises)
- Information et communication (62 %)
- Santé, travail social et protection sociale (56 %)

Ces trois secteurs traitent invariablement la cybersécurité comme une priorité élevée. À l'inverse, mais également dans la lignée de l'année dernière, le secteur de l'alimentation et de l'hôtellerie et celui de la construction ont tendance à accorder moins d'importance à la cybersécurité (seulement 62 % et 64 % affirment qu'il s'agit d'une priorité élevée contre 77 % de l'ensemble des entreprises).

Les points à retenir

La COVID-19 a été le grand vecteur d'accélération de la transformation numérique, mais les organisations et la société en général n'étaient peut-être pas préparées à ce qu'elle se fasse à un tel rythme. Outre les nombreux aspects positifs associés, cela a également généré une importante dette technique.

Tandis que les rançongiciels ont fait la une des journaux, le NCSC a mis en lumière l'aggravation des menaces de cybersécurité en termes d'intensité, de complexité et de gravité. La dépendance croissante aux technologies et à l'infrastructure numériques a également augmenté l'exposition au risque, en particulier avec le travail à distance ou hybride.

L'ingénierie sociale reste l'une des principales menaces, qu'il s'agisse de la cybercriminalité ou de la fraude en général. Selon le site Gov.UK, parmi les 39 % d'entreprises britanniques ayant repéré une attaque, le vecteur de menace le plus courant était les tentatives d'hameçonnage (83 %). Il est également de plus en plus important d'assurer la maintenance des logiciels et des systèmes pour garantir leur mise à jour et leur protection. Les risques liés à la chaîne d'approvisionnement constituent une autre préoccupation majeure pour les logiciels, payants ou libres.

Afin de relever ces défis, le gouvernement propose notamment la mise en place prochaine de deux stratégies, la National Resilience Strategy et la Digital Strategy, visant à définir des pistes claires qui permettront au pays de construire une économie numérique plus inclusive, compétitive et innovante pour l'avenir.

Bien qu'elle soit tournée vers le futur, il est important que la région Royaume-Uni et Irlande reste fermement ancrée dans le présent et renforce la protection de ses organisations et de ses citoyens face aux formes courantes d'attaques toujours plus efficaces. Sans protection des identifiants, correction des failles des systèmes ni formation des utilisateurs sur la sensibilisation à la sécurité, le chemin vers une économie numérique innovante pourrait bien s'avérer sinueux.

ROYAUME-UNI ET IRLANDE	RÉFÉRENCE	90 JOURS	1 AN
1 à 249	26,2 %	16,7 %	3,9 %
250 à 999	27,7 %	16,2 %	4,3 %
>1 000	32,7 %	17,5 %	8,3 %
PPP moyen toutes tailles confondues	30 %	17 %	5,5 %

EUROPE

Problèmes les plus fréquents

Avec la crise engendrée par la COVID-19, la dépendance vis-à-vis des technologies d'information et de communication n'a jamais été aussi forte. Pour rester dans la course, les organisations ont dû mettre en place des mesures de continuité opérationnelle alternatives, passant notamment par l'adoption de nouveaux services sur le cloud, la création de services accessibles directement par les consommateurs, le déploiement de nouvelles formes de paiement numérique et la démocratisation du travail à distance. Ces changements ont dû se faire à un rythme accéléré, ce qui a souvent généré des failles de sécurité critiques.

Les grandes entreprises ont généralement la capacité et les ressources nécessaires pour supporter l'impact des crises majeures de ce type, tandis que cela est plus difficile pour les organisations de petite et moyenne tailles. Représentant la vaste majorité des organisations de l'Union européenne, celles-ci constituent également le groupe le plus vulnérable, avec des budgets alloués à la cybersécurité souvent limités et une faible faculté de récupération suite aux catastrophes de grande ampleur.

Les principaux incidents visant l'Europe ont eu des conséquences considérables. Avec une dépendance à Internet de plus en plus forte en Europe, les crises telles que la pandémie de COVID-19, la guerre en Ukraine et l'accroissement de la cybercriminalité peuvent avoir un impact dévastateur sur les organisations. Europol indique que les principaux problèmes de cybersécurité viennent des attaques par hameçonnage et par ingénierie sociale. L'Union européenne représentant la plus grande économie mondiale, il est essentiel de limiter le risque d'être victime d'attaques de ce type en renforçant la sensibilisation à la sécurité des utilisateurs.

Impact économique

Il est difficile d'évaluer précisément l'impact économique de la cybercriminalité en Europe. Indicateurs peu clairs, incidents non signalés et manque général de données financières font qu'il est presque impossible de tenir un compte exact.

Cependant, malgré l'absence de chiffres précis, il est évident que l'impact économique de la cybercriminalité est élevé. Selon l'Agence européenne chargée de la sécurité des réseaux et de l'information (ENISA), 57 % des PME (petites et moyennes entreprises) interrogées affirment qu'elles feraient très probablement faillite ou devraient cesser leurs activités si elles étaient victimes d'un incident de cybersécurité sérieux.

Profil d'organisation type

Les PME représentent 99 % de toutes les entreprises de l'Union européenne. Une enquête de Statista révèle qu'en 2020, environ 93,3 % des entreprises hors secteur financier en Europe étaient de très petites entreprises avec neuf employés maximum. La même année, à peu près 5,7 % étaient classées comme de petites entreprises (de 10 à 49 employés), 0,9 % comme des entreprises de taille moyenne (de 50 à 249 employés) et 0,2 % comme de grandes entreprises employant 250 personnes ou plus.

Adoption culturelle

Il ressort du rapport « Security Culture Report 2022 » de KnowBe4 que l'Europe est plutôt performante avec un score d'indice de la culture de la sécurité de 73 (sur 100). Ce score de culture de la sécurité reflète les idées, les habitudes, les comportements sociaux ayant un impact sur la sécurité d'une organisation, ainsi que l'adoption de la sécurité par les employés d'une organisation.

Plusieurs pays de l'Union européenne agissent activement pour sensibiliser leurs citoyens et leurs organisations à la cybersécurité. Cela va des campagnes de sensibilisation visant les consommateurs à la fourniture active de données et informations libres sur les indicateurs de compromission aux organisations. Ces démarches, conjuguées à une mise en lumière croissante de la cybercriminalité par les médias nationaux et locaux, ont conduit à une plus grande prise de conscience de la nécessité d'adopter la sécurité comme facteur de protection de base.

Comportement général

La transformation numérique est l'un des développements majeurs qui tirent les organisations européennes vers le haut. Bien qu'il s'agisse d'une avancée positive, cela augmente aussi la nécessité de renforcer la protection contre la cybercriminalité. Deux technologies clés pour la numérisation, l'Internet des objets et l'intelligence artificielle, sont également exploitées par les pirates.

L'élément le plus intéressant réside dans l'évolution du profil des spécialistes. Les organisations recherchent de plus en plus des compétences liées à la gestion globale de la sécurité, comme la gestion des risques ou des services, tandis que les compétences telles que la gestion des technologies et les tests manuels de pénétration deviennent secondaires en raison des progrès effectués dans le domaine de l'automatisation et de l'intelligence artificielle.

Dans l'ensemble, pour que la cybersécurité soit adoptée par les organisations, celle-ci doit prouver sa valeur en tant qu'outil d'intérêt commercial.

Les points à retenir

La dépendance vis-à-vis des technologies d'information et de communication générée par la pandémie de COVID-19 a fait apparaître le défi de la cybersécurité. Cette dépendance est exploitée de manière criminelle par le biais de cyberattaques. Les attaques par ingénierie sociale ou rançongiciel et celles qui ciblent la chaîne d'approvisionnement sont conçues spécifiquement pour paralyser les entreprises. L'hameçonnage demeurant le vecteur d'attaque numéro un, les utilisateurs jouent un rôle central dans la stratégie de sécurité des organisations.

Les organisations sont contraintes par le manque de personnel qualifié et le nombre croissant d'incidents de cybercriminalité en Europe de considérer leurs employés comme les principaux garants de leur sécurité. Elles les voient comme une ressource qu'elles doivent protéger, mais aussi comme un acteur majeur qui peut jouer un rôle actif dans leur stratégie de sécurité globale et leur système de pare-feu. Avec un pourcentage de Phish-prone moyen de 29,9 % en Europe, il est impératif pour les organisations d'investir dans des programmes de sensibilisation à la sécurité pour permettre aux utilisateurs d'agir de manière plus sécurisée.

EUROPE	RÉFÉRENCE	90 JOURS	1 AN
1 à 249	27,8 %	17,9 %	4,2 %
250 à 999	28,2 %	18,2 %	6,7 %
>1 000	31,1 %	18,9 %	8 %
PPP moyen toutes tailles confondues	29,9 %	18,5 %	6,3 %

AFRIQUE

Problèmes les plus fréquents

Comme l'a signalé le Centre d'études stratégiques de l'Afrique, les cybermenaces se développent fortement en Afrique, de l'espionnage au sabotage d'infrastructures critiques, en passant par le crime organisé. Pourtant, seulement un tiers environ (17) des 54 pays africains ont mis en place une stratégie de cybersécurité nationale. Par ailleurs, lorsque des plans ont été adoptés, ils ne sont pas performants, dans la mesure où ils n'incluent aucun partenaire clé, ne prévoient pas de méthode de renforcement efficace des compétences et ne sont pas réadaptés assez fréquemment aux menaces en constante évolution. Les précédentes démarches entreprises pour améliorer la cybercoopération transfrontalière en Afrique, notamment la Convention sur la cybersécurité et la protection des données à caractère personnel (ou Convention Malabo), soutenue par l'Union africaine, n'ont pas encore obtenu le soutien adéquat à l'échelle nationale.

L'un des principaux problèmes auxquels l'Afrique est confrontée en matière de cybersécurité réside dans le manque de compétences. Le continent aurait besoin de 100 000 spécialistes supplémentaires, un chiffre qui ne fait qu'augmenter. Bon nombre d'entreprises, d'agences et de consommateurs ne sont pas sensibilisés à Internet, et les organisations ne mettent en place aucun contrôle de cybersécurité de base.

Bien souvent, les gouvernements ne surveillent pas efficacement les menaces, ne collectent pas de preuves légales numériques et ne lancent pas de poursuites en cas de crimes basés sur des outils informatiques.

Impact économique

Les incidents et l'impact financier n'étant pas répertoriés officiellement, il est difficile de mesurer les conséquences réelles de la cybercriminalité sur l'économie africaine. Pas moins de 96 % des incidents de cybersécurité ne sont pas signalés et restent non résolus, ce qui signifie que le niveau de cybermenace est certainement bien plus grave en Afrique qu'on ne le reconnaît formellement.

Les données publiées dans le rapport annuel 2020 de l'agence INSURANCE CRIME BUREAU d'Afrique du Sud indiquent que la croissance de l'économie numérique africaine a été plus rapide que les développements nécessaires pour fournir la cybersécurité appropriée. Elles montrent aussi que la conjonction de pressions économiques, politiques et sociales entraîne une hausse des « crimes économiques de désespoir », y compris des crimes physiques, des fraudes élaborées et des cybercrimes.

L'enquête sur les rançongiciels menée en 2021 par ITWeb et KnowBe4 en Afrique du Sud a révélé que 32 % des participants avaient fait l'objet d'une attaque de cyberextorsion. Par ailleurs, 4 % des victimes ont payé la rançon demandée, ce qui en fait une activité lucrative pour les groupes de pirates qui agissent par rançongiciel.

Mis à part les pertes subies directement suite aux attaques par cyberextorsion et cyberfraude, le manque de mesures de cybersécurité et de protections appropriées résulte dans de nombreux pays et organisations de l'incapacité à tirer parti des opportunités offertes par la quatrième révolution industrielle. La majorité des nations africaines ne sont pas suffisamment préparées pour gérer les progrès qui risquent de caractériser la décennie à venir en matière d'intelligence artificielle, de communication sans fil, d'informatique quantique et d'automatisation. Cela signifie que les organisations africaines ne pourront pas tirer profit économiquement de ces technologies si elles ne sont pas assez armées pour faire face aux cybermenaces.

Profil d'organisation type

Que ce soit en termes de population, de niveau de développement, de taux de croissance ou encore de stabilité, les 54 pays d'Afrique sont particulièrement hétérogènes. Tandis que le Nigéria compte près de 190 millions d'habitants et l'Éthiopie et l'Égypte plus de 90 millions, la plupart des nations africaines ont une population inférieure à 20 millions de personnes. Le potentiel de l'Afrique en tant que marché porteur pour les entreprises reste sous-estimé et mal compris. Plus de 400 entreprises situées en Afrique génèrent un revenu annuel supérieur ou égal à un milliard de dollars, et elles connaissent, en moyenne, une croissance plus rapide et une meilleure rentabilité que leurs homologues mondiales.

Le rapport « Phishing by Industry Benchmark Report » de KnowBe4 repose sur un total de 7 490 tests de simulation d'hameçonnage réalisés auprès de 300 organisations africaines. Parmi celles-ci, 58 % sont des PME (petites et moyennes entreprises) avec 1 à 249 utilisateurs, 28 % sont de taille moyenne avec 250 à 999 employés, et 14 % comptent 1 000 utilisateurs et plus.

La majorité des jeux de données proviennent d'organisations basées en Afrique du Sud. Viennent ensuite le Kenya, puis le Nigéria et le Botswana.

Adoption culturelle

L'Afrique compte actuellement 1,2 million d'habitants environ, et sa population devrait atteindre 1,7 million d'ici 2030. Sur ce continent, les personnes à l'origine des innovations sont souvent portées par un objectif profond : elles observent les niveaux de pauvreté élevés, les lacunes importantes dans les infrastructures, l'enseignement et la santé ; elles voient des problèmes humains face auxquels elles se font un devoir d'agir. Lors de l'évaluation des risques, l'instabilité, l'accès au capital, la corruption et la cybersécurité sont des préoccupations majeures pour les investisseurs et entrepreneurs potentiels. Les utilisateurs d'appareils mobiles sont de plus en plus nombreux. La majorité d'entre eux découvre Internet pour la première fois et manque de compétences de base en la matière.

Le rapport « African Cybersecurity and Awareness Report 2021 » de KnowBe4 a révélé que la pandémie continuait d'influencer fortement les comportements et habitudes de travail des 800 participants interrogés dans huit pays d'Afrique. Seuls 38 % des participants sont retournés au bureau ou ont accès à Internet depuis leur réseau professionnel, tandis que 55 % pratiquent encore le télétravail.

Parmi les personnes interrogées, 72 % affirment que la cybercriminalité est une préoccupation pour elles, mais qu'elles manquent de connaissances de base concernant les menaces réelles auxquelles elles sont exposées. Par ailleurs, 54 % des participants ne savent pas définir une attaque par rançongiciel, 26 % ont été victimes d'ingénierie sociale par téléphone (hameçonnage vocal) et 34 % ont perdu de l'argent suite à une escroquerie. Les effets de la pandémie influencent toujours le comportement des employés, puisque 55 % des personnes ayant participé à l'étude prévoient de continuer à travailler de chez elles.

Comportement général

Avec un âge médian de seulement 19,7 ans, la population africaine est la plus jeune du monde. Toujours plus nombreuse, la jeunesse africaine aspire à profiter de la connectivité mondiale et joue un rôle majeur dans l'adoption des nouvelles technologies et la numérisation : le nombre de propriétaires d'appareils mobiles connectés enregistre une croissance exponentielle, l'utilisation des réseaux sociaux augmente et l'Internet des objets (IdO) est aujourd'hui une réalité. Selon le FMI (Fonds monétaire international), l'Afrique subsaharienne est la seule région du monde où près de 10 % du PIB est généré par le paiement mobile. Salaires, virements, règlement des factures, achats : tout passe par les appareils mobiles. Le rapport « African Cybersecurity and Awareness Report 2021 » de KnowBe4 montre que 71 % des personnes interrogées dans huit pays africains utilisent leurs données mobiles pour accéder à Internet, tandis que 63 % utilisent leur téléphone mobile pour consulter leurs comptes et effectuer des paiements en ligne. WhatsApp reste l'application la plus populaire à 91 %, suivie des e-mails à 75 % et de Telegram à 52 %.

Cette prospérité grandissante et l'essor de la numérisation font naître de nouveaux risques et vulnérabilités qui pourraient compromettre ces avancées. Un travail approfondi doit être mené par les entreprises et les gouvernements pour remédier à l'« incompétence inconsciente » des utilisateurs africains vis-à-vis de la cybersécurité et pour protéger les citoyens de la cybercriminalité.

Les points à retenir

Le rapport « African Cybersecurity and Awareness Report 2021 » de KnowBe4 révèle que le paysage des menaces a changé et s'est adapté année après année aux conditions de travail en pleine mutation et aux préoccupations liées à la sécurité. Seuls 40 % des participants pensent comprendre pleinement leurs responsabilités et leurs rôles en matière de sécurité, et 28 % seulement pensent que leurs employeurs leur ont fourni une formation appropriée sur la cybersécurité. Les attaques visant les organisations africaines suivent la tendance observée dans les autres pays, à savoir : cyberextorsion, chevaux de Troyes bancaires, escroqueries d'investissement (y compris en cryptomonnaie), compromission de la messagerie d'entreprise (BEC) et ingénierie sociale ayant pour but la fraude financière. Cependant, la menace est amplifiée dans la mesure où les citoyens africains sont naturellement moins sensibilisés au sujet que dans d'autres pays. Les escroqueries relativement basiques, comme la BEC, l'hameçonnage, l'hameçonnage vocal et le smishing (hameçonnage par SMS), sont efficaces auprès des petites entreprises mal équipées.

Les rançongiciels ont gagné en popularité. Les entreprises et les gouvernements ayant des problèmes plus urgents à régler, comme le chômage des jeunes, la pauvreté, les inégalités et les crimes violents, la cybersécurité n'est pas une priorité et souffre d'un manque d'investissement.

Les entreprises qui opèrent dans cette région n'ont pas les moyens de se doter de contrôles de sécurité, y compris les plus simples. Celles qui peuvent se le permettre peinent à trouver du personnel qualifié dans le domaine. Il est nécessaire de mettre en œuvre des partenariats publics-privés pour aider l'Afrique à relever les défis de cybersécurité auxquels elle est confrontée. Le secteur privé, en particulier dans le domaine des services financiers, possède le capital humain, les infrastructures, les capacités et l'expertise qui manquent à l'État en matière de cybersécurité. Il est essentiel que les organisations forment leurs employés et leurs clients aux pratiques exemplaires de sécurité. Les gouvernements et les institutions éducatives doivent investir pour former les professionnels de la sécurité qui font défaut et faire de la sensibilisation à la cybersécurité une compétence de vie pour les jeunes qui arrivent sur le marché du travail.

AFRIQUE	RÉFÉRENCE	90 JOURS	1 AN
1 à 249	30,2 %	24,8 %	8,1 %
250 à 999	27,4 %	21 %	12,7 %
>1 000	32,4 %	17,9 %	4 %
PPP moyen toutes tailles confondues	31,4 %	18,8 %	5,4 %

AMÉRIQUE DU SUD

Problèmes les plus fréquents

En Amérique latine, les cyberattaques sont de toutes formes et de toutes tailles. Les vers, les chevaux de Troyes, les logiciels espions, les rançongiciels et surtout l'hameçonnage sont les principaux exemples des nombreuses méthodes utilisées.

La pandémie mondiale de COVID-19 a provoqué de profonds changements au sein de la société, affectant la vie de l'ensemble des entreprises et des citoyens de différentes manières. La propagation du virus a contraint de nombreuses organisations à passer au travail à distance, ce qui a eu un impact technologique considérable, en particulier du point de vue de la cybersécurité.

L'interconnectivité inégalée et le développement du télétravail ont généré de nouveaux défis pour la sécurité de l'information, ce qui n'a fait qu'augmenter les niveaux de risques. Une fois la transformation de l'environnement d'entreprise effectuée vers une structure de travail à distance, la sécurité doit être correctement conçue et configurée pour empêcher les pirates de perturber les activités de l'organisation.

À l'échelle mondiale, deux pays d'Amérique latine figurent parmi les dix nations les plus touchées par les attaques par hameçonnage. Le Brésil arrive en tête du classement avec 12,4 %, et l'Équateur occupe la 10e place avec 10,7 %. En d'autres termes, la somme des attaques perpétrées dans ces deux pays d'Amérique du Sud représente 23,1 % de toutes les attaques par hameçonnage mondiales.

Pourcentage de Phish-prone

En 2021, nous avons évalué le pourcentage de Phish-prone à 39,9 % en Amérique latine. Ce chiffre traduit une augmentation de 6,1 % par rapport aux 33,7 % enregistrés en 2020 et publiés dans le rapport « Phishing By Industry Benchmarking Report » 2021.

Il est à noter que l'Amérique du Sud est la région du monde la plus vulnérable aux attaques par hameçonnage, en comparaison avec d'autres régions telles que l'Amérique du Nord (32,4 %), l'Asie (34,6 %), l'Europe (29,9 %) et l'Océanie/Australie/Asie (34,5 %).

En ce qui concerne les entreprises de plus de 1 000 employés, le Pérou arrive en tête du classement des pourcentages de Phish-prone avec 72,7 %, suivi par le Brésil (65,1 %) et la Colombie (46,6 %).

Impact économique

L'hyper-connectivité des dernières décennies a élargi le paysage des cyberactivités ainsi que le champ d'action des pirates. Tous les utilisateurs, les entreprises et les gouvernements peuvent être ciblés, et à ce titre, la sécurité doit être considérée comme un axe majeur prioritaire pour l'investissement des ressources.

Si les cyberattaques passent souvent inaperçues en raison de plusieurs facteurs techniques et financiers, certains actes malveillants peuvent poser de sérieux problèmes et générer d'importantes pertes économiques.

L'estimation de ce préjudice financier augmente année après année. Selon le rapport « Cybersecurity in Latin America Report » établi par Statista, le marché de la cybersécurité en Amérique latine a été évalué à près de 12,9 milliards de dollars en 2019. Ce montant devrait dépasser les 25 milliards de dollars d'ici 2025. Le Brésil, le Mexique et la Colombie apparaissent comme les pays les plus ciblés par les cybercriminels. Ces trois nations réunies totalisent près de neuf attaques sur dix signalées en Amérique latine.

Les rançongiciels constituent l'un des types d'attaques les plus couramment utilisés par les cybercriminels dans cette région. Dans l'étude de 2020, 65 % des participants au Brésil affirmaient que leur organisation avait été attaquée par un rançongiciel, contre 44 % au Mexique et en Colombie.

Profil d'organisation type

Des entreprises de tous les segments de marché ont été visées par des cyberattaques en Amérique latine. Au Brésil, par exemple, des cas d'attaques par rançongiciel ont été signalés contre des entreprises du secteur de la santé, de la vente au détail et de la finance, mais aussi contre des institutions gouvernementales.

Même les petites entreprises qui n'investissent traditionnellement pas dans la sécurité de l'information allouent déjà une grande partie de leurs ressources financières au contrôle des cyberattaques potentielles.

Pour un seul cas signalé en 2021, une entreprise de commerce électronique a déclaré plus de 3,4 milliards de réaux brésiliens de pertes après l'attaque de ses sites Web par un rançongiciel.

Adoption culturelle et comportement général

Les gouvernements de plusieurs pays d'Amérique latine élaborent des stratégies de sécurité de l'information bien définies. Les entreprises et les organisations travaillent également à la création et à la mise en œuvre de nouvelles mesures de sécurité visant à limiter tous les types de cyberattaques à venir.

Les équipes de sécurité des entreprises brésiliennes, mexicaines et colombiennes étant parmi les plus ciblées par les cybercriminels, elles consacrent plus de la moitié de leurs heures de travail à prévenir les cybermenaces. Quant aux investissements réalisés par ces trois pays pour contrer les attaques, ils représentent en moyenne un tiers de leur budget.

Par exemple, en 2020, le Brésil était le pays d'Amérique latine avec le pourcentage d'attaques par hameçonnage le plus élevé. Suite à la divulgation de ces données alarmantes, le volume d'investissements dans le domaine de la sécurité a augmenté de manière exponentielle dans les entreprises de moyenne et grande tailles. Le marché est en demande croissante de professionnels de la mise en œuvre de la sensibilisation à la sécurité.

Outre les incidents eux-mêmes, les spécialistes de la sensibilisation à la sécurité témoignent d'une adoption grandissante des solutions proposées, qu'il s'agisse d'hameçonnage, de rançongiciels, de blanchiment d'argent ou d'autres menaces.

Les points à retenir

Un modèle Zero Trust aide à réduire le risque : les principes associés à une approche Zero Trust, comme la mise en œuvre de l'authentification multifactorielle (AMF), les jetons d'authentification matériels ou le droit d'accès minimal, peuvent faire baisser la vulnérabilité des organisations face aux principaux types d'attaque, en particulier par rançongiciel et BEC.

Développer un plan de réponse pour les rançongiciels : l'ensemble des secteurs et des organisations peut être la cible d'une attaque par rançongiciel. Le facteur clé réside dans la vitesse à laquelle les équipes parviennent à réagir avec les informations appropriées dans les premiers instants critiques. Cela fait toute la différence dans le volume de temps et d'argent perdu durant la réponse.

Adopter une formation sur la sensibilisation à la sécurité nouvelle génération : il est essentiel de mettre en place un plan solide, intégrant notamment des simulations d'hameçonnage basées sur des exemples réels. En outre, il n'a jamais été aussi important de former les employés à l'aide d'un programme de sensibilisation à la sécurité moderne pour favoriser la détection des attaques par hameçonnage et par ingénierie sociale.

AMÉRIQUE DU SUD	RÉFÉRENCE	90 JOURS	1 AN
1 à 249	30,9 %	24,7 %	1,8 %
250 à 999	30 %	22,2 %	9,8 %
>1 000	45,6 %	19,3 %	0,8 %
PPP moyen toutes tailles confondues	39,9 %	20,5 %	3,2 %

APAC, AUSTRALIE ET NOUVELLE-ZÉLANDE

Problèmes les plus fréquents

APAC

Dans toute la région APAC, y compris en Australie et en Nouvelle-Zélande, les méthodes d'escroquerie basées sur les rançongiciels, la chaîne d'approvisionnement, la BEC, les achats en ligne, la fraude, la banque en ligne, le vol d'identité et les arnaques aux sentiments sont des menaces qui ressortent constamment, l'hameçonnage étant le vecteur d'attaque le plus efficace.

L'IBM Security X-Force Threat Intelligence Index 2022, qui se base sur des données de 2021, révèle que le Japon, l'Australie et l'Inde ont été les pays les plus attaqués d'Asie. Cela va dans le sens des résultats parus dans le rapport « Data Breach Investigations Report » 2021 de Verizon. Le type de violation le plus couramment observé dans la région APAC était causé par des pirates qui, portés par des motivations financières, utilisaient des techniques d'hameçonnage pour voler les identifiants des employés et les utilisaient ensuite pour accéder aux comptes de messagerie et aux serveurs d'applications Web. Verizon a également montré que 70 % des attaques perpétrées dans cette région comportaient une action d'ingénierie sociale.

Australie

Durant l'exercice 2020–21, l'Australian Cyber Security Centre (ACSC) a enregistré plus de 67 500 signalements de cybercrimes, soit une augmentation de près de 13 % par rapport à l'exercice précédent. Un cyberincident est signalé toutes les huit minutes dans cette région. En plus des thèmes habituellement utilisés par les cybercriminels, la pandémie mondiale de COVID-19 a été, et demeure, un sujet tendance dans les campagnes de harponnage et d'hameçonnage conçues pour obtenir des informations précieuses, ainsi que de l'argent.

Selon l'Office of the Australian Information Commissioner, le secteur des prestataires de services de santé a été le plus ciblé, suivi par la finance, le secteur juridique, les services de comptabilité et de gestion, les services à la personne et enfin l'enseignement et l'assurance. Par ailleurs, environ un quart des cyberincidents signalés concernaient une infrastructure critique ou des services essentiels.

Impact économique

Le rapport « The Global State of Industrial Cybersecurity 2021: Resilience Amid Disruption Report » publié par Claroty révèle que 80 % des organisations de la région APAC ont été la cible d'attaques par rançongiciel en 2021, une rançon ayant été payée dans 51 % des cas.

Selon l'ACCC (Australian Competition and Consumer Commission), les Australiens ont perdu un montant record de 323 millions de dollars australiens suite à des escroqueries en 2021 (soit une augmentation considérable de 84 % par rapport à l'année précédente). En parallèle, 790 Singapouriens ont été victimes de la récente arnaque par smishing impliquant l'OCBC Bank, pour un montant total de 13,7 millions de dollars singapouriens de pertes. Cela illustre l'ampleur du coût potentiel pour les entreprises de la région.

Profil d'organisation type

APAC

La région Asie-Pacifique compte 4,2 milliards d'habitants. Avec plus de 38 pays, c'est l'une des régions de la planète les plus diverses, et elle regroupe des économies faisant figure d'exemples à l'échelle mondiale dans le domaine sociétal et numérique. Elle est également considérée comme un leader mondial pour l'accès à l'Internet haut débit et son utilisation.

Australie

En 2021, l'économie australienne comptabilisait 2 447 026 entreprises actives.

Nouvelle-Zélande

En 2021, l'économie néo-zélandaise comptabilisait 562 521 entreprises actives.

Adoption culturelle

Le rapport « Tendances digitales 2022 - APAC » d'Adobe prévoit que d'ici 2025, 333 millions de personnes supplémentaires commenceront à utiliser l'Internet mobile dans la région APAC, et il est fort probable que le comportement de ces nouveaux utilisateurs diffère de celui des utilisateurs actuels.

Alors que le travail à distance et hybride continue de s'organiser, il reste indispensable de traiter la question de l'erreur humaine, impliquée dans la majorité des cyberattaques réussies, tous types de technologie confondus.

Comportement général

Dans le rapport « Cyber Safety Insights Report » 2021 de Norton, 79 % des Australiens, 77 % des Néo-Zélandais et 73 % des Japonais ayant participé à l'étude partagent l'idée selon laquelle « le travail à distance permet aux pirates et aux cybercriminels d'abuser beaucoup plus facilement les utilisateurs ». L'enquête indique également que plus d'un adulte sur deux est plus inquiet que jamais à l'idée d'être victime d'un cybercrime, mais qu'une même proportion ne sait pas comment s'en protéger.

Dans toute la région APAC, les utilisateurs recherchent activement des conseils et des informations pour renforcer leur sécurité en ligne et mieux protéger leur confidentialité. Bien souvent, ils ne savent malheureusement pas où aller, ni comment procéder.

En réalité, les cybermenaces sont si répandues que préserver la sécurité des utilisateurs et des organisations requiert un effort conjoint du gouvernement, des dirigeants d'entreprise, des services informatiques et des employés. Il n'existe aucune solution universelle ou technologie magique capable de protéger votre entreprise. Tout le monde doit être sensibilisé aux menaces et à la façon de les éviter.

Selon l'étude annuelle 2021 de KnowBe4 sur l'APAC, moins de la moitié (45 %) des décideurs informatiques de cette région considèrent qu'il est de la responsabilité de chacun de protéger l'organisation des cyberattaques.

APAC	RÉFÉRENCE	90 JOURS	1 AN
1 à 249	30,2 %	21,1 %	4,4 %
250 à 999	32,6 %	19,2 %	6,2 %
>1 000	36,7 %	15 %	5,2 %
PPP moyen toutes tailles confondues	34,5 %	16,9 %	5,4 %

Dans la mesure où le service informatique manque de clarté, il n'y a rien d'étonnant à ce que les employés ne sachent pas non plus qui est responsable de la cybersécurité :

- Près d'un quart (24 %) d'entre eux affirment que la technologie doit protéger l'organisation des cyberattaques.
- 21 % jugent que la responsabilité incombe au service informatique.
- 11 % pensent que la responsabilité incombe au gouvernement.

La formation sur la cybersécurité change la vision des employés à ce sujet et les amène à se sentir davantage responsables de la protection de la sécurité de l'organisation. Ceux qui ont reçu une formation ont plutôt tendance à considérer que la responsabilité incombe aux employés (16 %) que ceux qui n'ont pas été formés (11 %).

À l'inverse, ceux qui n'ont reçu aucune formation ont plutôt tendance à considérer que la responsabilité incombe au service informatique (29 % contre 17 %).

Les points à retenir

Selon notre étude annuelle 2021 sur l'APAC, sept décideurs sur dix (70 %) dans le domaine informatique jugent que les gouvernements australien et singapourien devraient agir davantage pour protéger les entreprises contre les cyberattaques. En outre, seuls 52 % d'entre eux affirment être certains de bien comprendre les responsabilités qui incombent à leur organisation en ce qui concerne le signalement des cyberincidents et des violations de données au gouvernement.

Dans la région APAC, les entreprises et les responsables informatiques ne se sentent pas soutenus par le gouvernement en matière de sécurité et estiment que celui-ci devrait en faire plus, notamment :

- Former et sensibiliser davantage les citoyens aux cyberrisques et aux méthodes permettant de se protéger en ligne (45 %)
- Former davantage les entreprises aux cyberrisques (42 %)
- Fournir davantage de moyens financiers aux entreprises pour la cyberprotection (38 %)

La formation requise pour expliquer leurs obligations et engagements aux professionnels de l'informatique doit également être dispensée au grand public pour enseigner comment se protéger en ligne, que ce soit dans la sphère privée ou professionnelle.

LES POINTS À RETENIR : LES AVANTAGES D'UNE FORMATION SUR LA SENSIBILISATION À LA SÉCURITÉ NOUVELLE GÉNÉRATION

Plusieurs conclusions se détachent des résultats des trois phases de l'étude :

- **Sans formation sur la sensibilisation à la sécurité nouvelle génération, un danger majeur pèse sur toutes les organisations.** Avec un PPP de référence moyen de 32,4 % tous secteurs confondus, les organisations pourraient être exposées par un tiers de leurs employés à un risque d'escroquerie par ingénierie sociale et par hameçonnage, et ce à tout moment.
- **N'importe quelle organisation peut renforcer sa sécurité en seulement trois mois en formant ses utilisateurs finaux.** La puissance d'un bon programme de formation réside dans le fait de pouvoir définir une cadence régulière d'enseignement simulé sur l'ingénierie sociale et l'hameçonnage dans un laps de temps très bref.
- **Toutes les organisations peuvent plus rapidement obtenir des résultats en déployant une stratégie efficace de formation sur la sensibilisation à la sécurité.** Les difficultés rencontrées par certains dirigeants d'entreprise pour réussir à mettre en œuvre une formation sur la sécurité efficace au sein de leur organisation n'ont rien de surprenant. Pour mettre toutes les chances de leur côté, les responsables peuvent évaluer leurs objectifs et préparer une stratégie organisationnelle avant de déployer la formation.

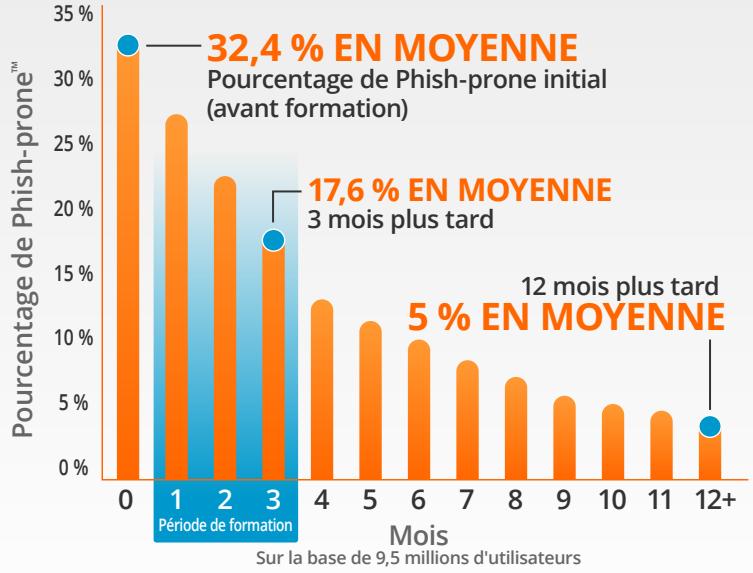
LES POINTS À RETENIR POUR LES CADRES

Les responsables de la gestion de la sécurité et des risques doivent comprendre que pour transformer positivement le comportement global vis-à-vis de la sécurité au sein de leur organisation, il est nécessaire de mettre en place des programmes qui :

- comportent un engagement clairement défini et détaillé ;
- s'alignent parfaitement sur les politiques de sécurité de l'organisation ;
- présentent un lien direct avec la culture de la sécurité globale et la ligne de défense humaine ;
- bénéficient de l'appui total de la direction.

Sans le soutien enthousiaste et constant de la direction, la tentative de sensibilisation à la sécurité dans l'organisation est vouée à l'échec.

Des résultats probants



Source : Rapport « Phishing by Industry Benchmarking Report » 2022 de KnowBe4

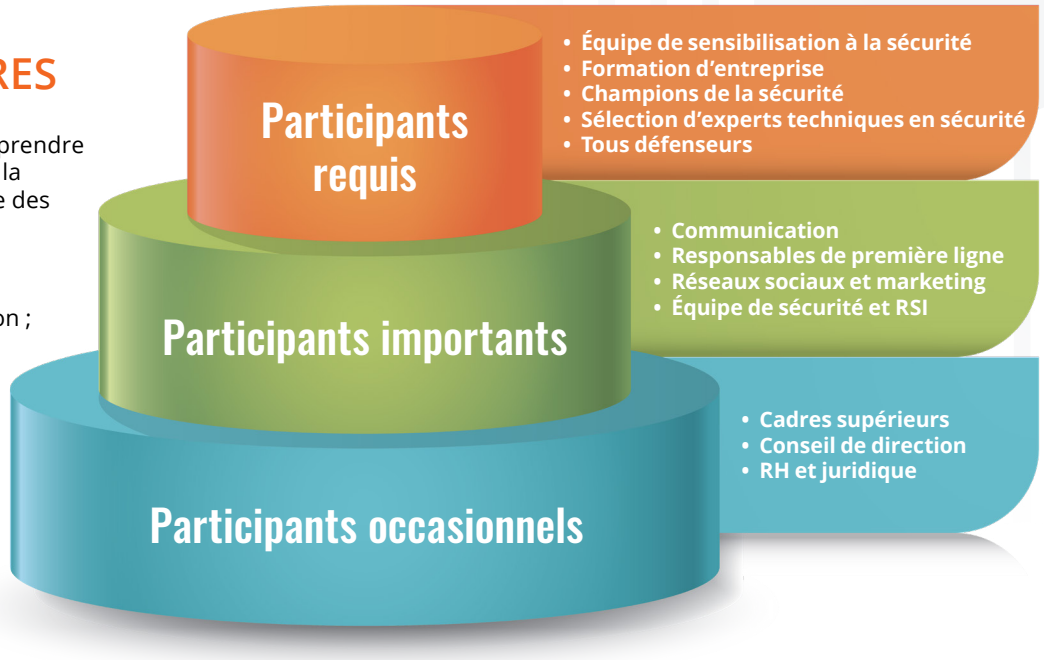
Remarque : Le pourcentage de Phish-prone initial est calculé sur la base de tous les utilisateurs évalués. Ces utilisateurs n'avaient bénéficié d'aucune formation sur la console KnowBe4 avant cette évaluation. Les périodes suivantes reflètent les pourcentages de Phish-prone du groupe d'utilisateurs formés à l'aide de la console KnowBe4.

LES POINTS À RETENIR POUR LES CADRES

Les responsables de la gestion de la sécurité et des risques doivent comprendre que pour transformer positivement le comportement global vis-à-vis de la sécurité au sein de leur organisation, il est nécessaire de mettre en place des programmes qui :

- comportent un engagement clairement défini et détaillé ;
- s'alignent parfaitement sur les politiques de sécurité de l'organisation ;
- présentent un lien direct avec la culture de la sécurité globale ;
- bénéficient de l'appui total de la direction.

Sans le soutien enthousiaste et constant de la direction, la tentative de sensibilisation à la sécurité dans l'organisation est vouée à l'échec.



Pour assurer la réussite de leurs programmes, les responsables de la gestion de la sécurité et des risques peuvent :

- **Encourager une culture de la sécurité :** Le facteur humain est l'élément central de l'infrastructure de sécurité d'une organisation. Tous les employés doivent comprendre les implications de leur rôle et les responsabilités qui leur incombent afin de protéger l'organisation, et de se protéger eux-mêmes, face aux cyberattaques. KnowBe4 définit la culture de la sécurité comme l'ensemble des idées, des habitudes et des comportements sociaux propres à une organisation et ayant un impact sur sa sécurité. Les responsables doivent veiller à promouvoir un environnement propice à la sécurité en investissant dans la mise au point de leur programme de formation et de sensibilisation à la sécurité, mais aussi dans la préparation de la ligne de défense humaine.
- **Agir en modèle :** Si vous voulez que votre organisation fasse les choses bien, vous devez montrer l'exemple dans votre façon de diriger. Les responsables doivent prendre une part active dans chaque aspect du processus de sensibilisation à la sécurité au sein de l'organisation, ce qui signifie qu'ils doivent se plier aux mêmes exigences de formation sur la sensibilisation à la sécurité que les autres employés.
- **Recruter un expert :** Le contenu de sensibilisation à la sécurité ne ressemble à aucun autre. Il faut avoir l'expertise nécessaire non seulement pour concevoir le contenu, mais aussi pour veiller à ce qu'il engendre une expérience d'apprentissage positive et un changement de comportement favorable à terme. Dans un domaine où le contenu est roi, la recommandation consiste à faire appel à un fournisseur capable de proposer un large éventail de saveurs, de versions et de variétés pour satisfaire tous les styles d'apprentissage. En limitant votre public à un modèle d'enseignement unique, vous restreignez l'expérience, la consommation de contenu et l'assimilation globale. Il peut être tentant de faire appel à votre équipe de formation interne pour mener ce développement de programme, ou de vous associer à un fournisseur proposant une approche universelle. Ces deux options vous plongeront dans l'incapacité prolongée à façonner la manière de penser et d'agir de votre public en matière de sécurité.

- **Réfléchir comme un expert en marketing :** En parallèle des campagnes d'hameçonnage simulé et de contenu, ajoutez des messages pertinents fréquents sous forme de supports complémentaires (affiches, encarts numériques, bulletins d'information, etc.) et trouvez des occasions de renforcer les points essentiels durant les présentations et les réunions interservices. Organiser des déjeuners de travail pour les employés et des jeux de rôles pendant les réunions de direction constitue un moyen intéressant de faire passer les informations et d'échanger directement avec votre public.
- **Mobiliser un programme de « défenseur de la culture » de la sécurité :** La plupart des programmes axés sur la sécurité et les risques ne possèdent pas les ressources nécessaires pour engager efficacement une organisation mondiale. Les programmes de « défenseur de la culture » de la sécurité portent différents noms, tels que : champions de la sécurité, ambassadeurs de la sécurité, liaisons de la sécurité, influenceurs de la sécurité, etc. Quel que soit le nom que vous lui donnez, le but d'un programme de ce type est de former une équipe de soutiens dispersés au sein de l'organisation qui peuvent renforcer localement les messages et les apprentissages liés à la sécurité. Le facteur de responsabilité entre également en jeu ici. Beaucoup d'employés pensent que la sensibilisation à la sécurité est l'affaire de quelqu'un d'autre. En engageant des influenceurs locaux, sur la base du volontariat ou désignés par les responsables, vous créez un réseau de référents en sécurité capables de faire le lien avec les communautés locales et de commencer à façonner la culture de la sécurité globale.
- **Ajouter des tests d'hameçonnage simulés :** Comme nous l'avons expliqué dans cette étude, en ajoutant des campagnes d'hameçonnage simulé régulières à votre programme de sensibilisation à la sécurité global, vous atténuez la vulnérabilité de vos employés et renforcez leur capacité à repérer les e-mails suspects.
- **Augmenter la fréquence :** Lorsque vous ne développez pas les compétences, vous laissez la place à l'atrophie. Notre étude montre que les organisations qui n'observent pas de changement de comportement favorable ont tendance à limiter la fréquence de leur programme (de contenu et d'hameçonnage simulé) à un rythme annuel, semestriel ou trimestriel. À ce rythme, vous obtenez des tests de référence valables à un instant T qu'il est difficile de mettre en perspective. Nous vous recommandons de soumettre votre public à des campagnes de contenu et d'hameçonnage simulé mensuelles (et même bimensuelles pour les cibles à risque élevé). Un rythme régulier est nécessaire pour que la mise en condition soit efficace et que le changement de comportement s'installe durablement. Si les responsables de la gestion de la sécurité et des risques craignent parfois que cela se répète trop souvent, en réalité, c'est ce qui aide à constituer le niveau adéquat de mémoire musculaire de la sécurité pour combattre les stratégies d'attaque agressives et en perpétuel changement d'aujourd'hui et de demain.
- **Recruter les bonnes personnes :** Il arrive couramment que les programmes de sensibilisation à la sécurité soient dirigés par des professionnels de la sécurité qui ont été désignés pour effectuer la tâche dont personne ne voulait ou qui avaient un peu de temps pour s'occuper de cette « histoire de formation ». Cependant, gérer un programme de ce type exige un certain niveau d'expérience et d'expertise. Vous devez cibler des candidats créatifs qui savent comment diriger une transformation organisationnelle et de comportement par l'apprentissage et qui ont l'habitude de le faire.
- **Définir des objectifs :** Déterminez en amont les critères qui valideront la réussite de votre programme et de quelle façon vous allez les évaluer. Sans cela, vous ne pourrez pas mesurer son efficacité ni sa valeur intrinsèque.
- **Mesurer efficacement :** Il est important d'utiliser des indicateurs qui renforcent les comportements souhaités pour aider à protéger les systèmes, les employés et les données. Ne tombez pas dans le piège qui consiste à sélectionner un trop grand nombre de critères de mesure ; cela vous conduira uniquement à évaluer des aspects non pertinents et/ou générera des résultats inférieurs à ceux attendus pour l'organisation. Il est essentiel d'utiliser des données mesurables et des formations qui peuvent être fréquemment quantifiées et validées. Vous devez également vous assurer que les indicateurs du programme sont liés non seulement aux objectifs de sécurité organisationnelle généraux, mais également aux objectifs de l'entreprise.

- **Motiver les employés :** Vous devez également utiliser le renforcement positif et négatif de manière ciblée et cohérente pour encourager votre public à effectuer la formation requise, à suivre les politiques de sécurité et à adopter un comportement constant, favorable et sûr. Utiliser des éléments moteurs augmente la prise de responsabilité et le rôle global joué par les employés pour favoriser une culture plus sécurisée.

COMMENCER

KnowBe4 aide des dizaines de milliers de professionnels de l'informatique comme vous à améliorer la cybersécurité dans des secteurs tels que la finance, l'énergie, la santé, l'administration publique, l'assurance et beaucoup d'autres.

Avec KnowBe4, vous bénéficiez de la meilleure plateforme de formation et de simulation d'hameçonnage pour améliorer la dernière ligne de défense de votre organisation : **votre pare-feu humain**.

Nous donnons à vos employés les moyens de prendre au quotidien des décisions plus avisées en matière de sécurité. Nous vous aidons à mettre en place un plan de défense de la sécurité informatique basé sur des données, qui commence par les menaces ayant le plus fort taux de « réussite » au sein de votre organisation : vos employés. La méthodologie KnowBe4 fonctionne vraiment. Prêt à commencer ?

Quatre étapes pour piéger vos utilisateurs par hameçonnage

Il est évident que les organisations peuvent réduire considérablement leur vulnérabilité et changer le comportement des utilisateurs finaux par le biais de tests et de formations. Suivez ces étapes pour mettre votre organisation sur la bonne voie et développer votre pare-feu humain.

1. **Réalisez des tests de référence :** Effectuer un test de référence est la première étape pour prouver à votre direction qu'une formation sur la sensibilisation à la sécurité est nécessaire. Celui-ci évaluera le pourcentage de Phish-prone (pourcentage de vulnérabilité à l'hameçonnage) de vos utilisateurs. Il fournira également les données indispensables pour mesurer votre future réussite.

2. **Formez vos utilisateurs :** Utilisez une formation sur ordinateur à la demande, interactive et stimulante à la place de diapositives PowerPoint démodées. Les modules et vidéos de sensibilisation doivent enseigner aux utilisateurs de quelle façon ils peuvent être victimes d'une tentative d'attaque par hameçonnage ou ingénierie sociale.

3. **Hameçonnez vos utilisateurs :** Au moins une fois par mois, testez votre personnel pour renforcer la formation et poursuivre le processus d'apprentissage. Vous essayez de façonner un état d'esprit et de créer de nouvelles habitudes. Il faut du temps pour que cela se mette en place. Les tests d'ingénierie sociale simulés présentés au moins une fois par mois ont fait leurs preuves quant aux changements de comportement.

4. **Mesurez les résultats :** Suivez la façon dont vos employés réagissent à la formation et aux tests d'hameçonnage. Votre objectif est de parvenir à un pourcentage de Phish-prone qui se rapproche le plus possible de zéro.

Planifiez comme un expert en marketing, testez comme un pirate

Si tous les responsables peuvent limiter le risque en ciblant le PPP des employés, il existe plusieurs pratiques exemplaires permettant de générer un changement durable.

01 Utilisez des méthodes d'attaque réelles

Vos exercices d'hameçonnage simulé doivent imiter les méthodes et attaques réelles. Sans cela, votre « formation » fera seulement naître un faux sentiment de sécurité au sein de votre organisation.

02 N'agissez pas seul

Impliquez les autres équipes et responsables, y compris vos collègues des ressources humaines, de l'informatique, de la conformité, et même du marketing. Créez une culture de la sécurité positive qui s'étend à toute l'organisation.

03 N'essayez pas de tout couvrir avec la formation

Vous devez répertorier les comportements que vous voulez façonner, puis sélectionner les deux ou trois aspects prioritaires.
Concentrez-vous sur la transformation de ces comportements pendant 12 à 18 mois.

04 Donnez du sens

Les utilisateurs s'intéressent à ce qui a du sens pour eux. Veillez à ce que vos attaques simulées aient un impact sur les activités quotidiennes de vos employés.

05 Traitez votre programme comme une campagne marketing

Pour renforcer votre sécurité, plutôt que de dire simplement à vos employés ce que vous voulez qu'ils sachent, vous devez vous focaliser sur le fait de générer un changement de comportement. Donnez-leur les informations essentielles dont ils ont besoin, mais restez concentré sur la transmission des réflexes de sécurité qu'ils doivent acquérir pour constituer une dernière ligne de défense efficace.

CRÉEZ VOTRE PARE-FEU HUMAIN

Test de sécurité gratuit vis-à-vis de l'hameçonnage

Prêt à commencer à hameçonner vos utilisateurs ? Découvrez le pourcentage de Phish-Prone (pourcentage de vulnérabilité à l'hameçonnage) de vos employés, en profitant de votre test de sécurité gratuit vis-à-vis de l'hameçonnage. Vous pouvez également comparer vos performances à celles des autres acteurs de votre domaine en consultant les données de référence du secteur en matière d'hameçonnage ! Vous pouvez parvenir aux mêmes résultats exceptionnels que ceux présentés dans l'étude avec le test de sécurité vis-à-vis de l'hameçonnage de KnowBe4.

RESSOURCES SUPPLÉMENTAIRES

Programme de sensibilisation à la sécurité automatisé
Créez un programme de sensibilisation à la sécurité personnalisé pour votre organisation

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 personnes malveillantes les adresses e-mail de vos utilisateurs à risque

Outil Domain Spoof Test gratuit
Déterminez si les pirates peuvent usurper une adresse e-mail de votre domaine

À PROPOS DE KNOWBE4

KnowBe4 est la plus grande plateforme de formation sur la sensibilisation à la sécurité et de simulation d'hameçonnage au monde. Née du constat selon lequel l'aspect humain de la sécurité était largement négligé, KnowBe4 a pour objectif d'aider les organisations à gérer le problème de l'ingénierie sociale par le biais d'une approche globale et innovante de la formation sur la sensibilisation à la sécurité.

Cette méthode intègre un dispositif de test de référence basé sur des simulations d'attaques réelles, une formation interactive au contenu stimulant, un système d'évaluation continue reposant sur des simulations d'attaques par hameçonnage et hameçonnage vocal, ainsi qu'un état des lieux des points forts de l'entreprise. Elle a pour but de développer une organisation plus résiliente, ayant pour priorité la sécurité.

Dans le monde entier, des dizaines de milliers d'organisations de tous les secteurs d'activité utilisent la plateforme KnowBe4, y compris dans des domaines très réglementés tels que la finance, la santé, l'énergie, l'administration et les assurances. Elles mobilisent ainsi leurs utilisateurs finaux, qui constituent leur dernière ligne de défense, et leur permettent de prendre des décisions plus avisées en matière de sécurité.

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

KnowBe4
Human error. Conquered.

KnowBe4 NL, BV | Papendorpseweg 99, 3528 BJ Utrecht, The Netherlands | Tél. : +31 (0)30 7996074 | www.knowbe4.com | E-mail : Sales@KnowBe4.com

08C06K04