KnowBe4

Phishing Benchmarking 2025

Rapport pour l'Europe

Coup de projecteur sur le risque humain Réduire le taux de clics en cas d'hameçonnage

La réduction du risque d'hameçonnage est un pivot de la gestion efficace du risque humain.

Pour réussir, toute attaque par hameçonnage est tributaire de l'action d'une personne de confiance, qui va par exemple cliquer sur un lien hypertexte. Un e-mail d'hameçonnage qui parvient à passer à travers les mailles des défenses techniques échouera malgré tout si son destinataire le signale, le supprime ou n'y réagit pas.

Les organisations peuvent renforcer leurs défenses techniques à l'aide d'un produit anti-hameçonnage optimisé par l'IA. Mais elles peuvent aussi fortement atténuer le risque d'hameçonnage réussi en mettant en place une formation sur la sensibilisation à la sécurité qui s'appuie sur les bonnes pratiques.

La première phase de toute stratégie de limitation du risque consiste à évaluer le profil de risque de votre organisation, puis de le comparer à celui d'autres acteurs de votre secteur d'activité, de taille similaire et opérant dans la même région géographique. Vous devez ensuite estimer la vulnérabilité réelle de votre organisation au risque d'hameçonnage et notamment, identifier les personnes susceptibles d'interagir avec un e-mail d'hameçonnage. Une fois ces informations en main, vous pourrez mettre en place à temps des solutions de sécurité personnalisées, par exemple des programmes de formation sur mesure et du coaching en temps réel.

Le Rapport Phishing Benchmarking de KnowBe4 décrit la première phase de cette stratégie. Dans le rapport de cette année, nous avons analysé au total 67 718 305 simulations d'hameçonnage sur 14 508 441 utilisateurs dans 62 460 organisations, sur une période de trois ans. Notre objectif était de calculer le pourcentage de Phish-prone™ ou PPP (Pourcentage de vulnérabilité à l'hameçonnage) d'organisations appartenant à 19 secteurs d'activité et implantées dans sept régions géographiques.

Ce guide offre une vue d'ensemble des principales conclusions pour l'Europe.

Notre méthode de calcul du pourcentage de Phish-prone

Le PPP correspond au pourcentage des employés d'une organisation susceptibles de se laisser piéger par une attaque par ingénierie sociale ou par hameçonnage. Il est parfois aussi désigné par l'expression « taux de clic dans les simulations d'hameçonnage ».

Phase une

Résultats du test de référence de sécurité relatif à l'hameçonnage

Avant d'organiser une formation KnowBe4, nous envoyons une première simulation d'hameçonnage. Elle permet d'identifier les risques et de calculer le PPP de référence d'une organisation.

Phase deux

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

Les employés suivent la formation sur la sensibilisation à la sécurité de KnowBe4. Une autre simulation est envoyée pour recalculer le PPP de l'organisation et mesurer l'efficacité du programme de formation.

Phase trois

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

Après 12 mois de formation sur la sensibilisation à la sécurité de KnowBe4, le PPP est recalculé afin d'évaluer plus précisément l'efficacité du programme de formation.

Valeurs de référence sur l'hameçonnage au niveau international en 2025

Dans les différentes régions géographiques, les PPP de référence les plus élevés ont été observés en Amérique du Sud (39,1 %), en Amérique du Nord (37,1 %), et en Australie et Nouvelle-Zélande (36,8 %).

Les organisations de plus de 1 000 employés basées en Australie et en Nouvelle-Zélande se sont révélées les plus vulnérables à l'hameçonnage au niveau mondial : 44,6 % de leurs employés ont en effet cliqué sur les liens hypertextes de simulation d'hameçonnage. Ce sont les petites organisations (de 1 à 249 employés) implantées en Asie ainsi qu'au Royaume-Uni et en Irlande qui présentent le risque le plus faible. Seul un quart de leurs employés (24,3 %) ont ainsi cliqué sur les liens.

Toutes les régions ont enregistré des taux d'amélioration moyens de plus de 80 %, l'Amérique du Nord arrivant en tête (89,5 %), talonnée de près par l'Amérique du Sud (88,9 %).

		Phase une – Référence			Phase deux – 90 jours			Phase trois – 1 an ou plus		
	Taille de l'organisation	1 à 249 employés	250 à 999 employés	+ de 1 000 employés	1 à 249 employés	250 à 999 employés	+ de 1 000 employés	1 à 249 employés	250 à 999 employés	+ de 1 000 employés
Région	Amérique du Nord	26 %	31,1 %	42 %	21,1 %	21,2 %	18,5 %	3,7 %	3,9 %	4,1 %
		TOTAL : 37,1 %			TOTAL : 19,6 %			TOTAL : 3,9 %		
	Afrique	27,9 %	30,1 %	35,8 %	24,9 %	28 %	20 %	2,2 %	9,2 %	5,1 %
		TOTAL : 34,9 %			TOTAL : 21,1 %			TOTAL : 5,3 %		
	Asie	24,3 %	27,6 %	29 %	18,9 %	19,1 %	17,6 %	5,1 %	4,5 %	5,4 %
		TOTAL : 28,6 %			TOTAL : 17,9 %			TOTAL : 5,2 %		
	Australie et Nouvelle-Zélande	25 %	29,2 %	44,6 %	23,2 %	23 %	16,6 %	3,9 %	6,1 %	4,7 %
		TOTAL : 36,8 %			TOTAL : 19,9 %			TOTAL : 4,9 %		
	Europe	24,9 %	26,7 %	34,9 %	20,7 %	21,6 %	20,5 %	3,9 %	4,4 %	5,3 %
		TOTAL : 32,5 %			TOTAL : 20,7 %			TOTAL : 5 %		
	Amérique du Sud	30,2 %	26,3 %	42,8 %	23,3 %	23,1 %	16,9 %	3,4 %	5,1 %	4,5 %
		TOTAL : 39,1 %			TOTAL : 18,2 %			TOTAL : 4,5 %		
	Royaume-Uni et Irlande	24,3 %	28,5 %	36 %	22,1 %	22,1 %	17,1 %	4 %	4,1 %	5,3 %
		TOTAL : 32,9 %			TOTAL : 19 %			TOTAL : 4,8 %		

Europe | *Par Martin Kraemer*

Le PPP en Europe reste dans le droit fil des résultats des années précédentes. Le PPP initial moyen avant la formation sur la sensibilisation à la sécurité est de 32,5 %. Ce chiffre tombe à 20,7 % au bout de 90 jours et à 5 % au bout d'un an.

Comme le révèle l'analyse des tendances mondiales, le PPP de référence est plus élevé dans les grandes organisations (plus de 1 000 employés), où il atteint 34,9 %. Il est de 26,7 % dans les entreprises de taille moyenne (250 à 999 employés) et de 24,9 % dans les petites entreprises (1 à 249 employés). Sans surprise, les grandes organisations affichent la plus forte réduction du risque. Après un an ou plus de formation, les taux de clics sont tombés à seulement 5,3 %, soit une diminution de 84,8 %. Les petites organisations ont atteint un taux de clics légèrement inférieur au bout d'un an de formation : 3,9 % pour les organisations de 1 à 249 employés et 4,4 % pour celles dont l'effectif était compris entre 250 et 999.

Ce taux de PPP compris entre 3 et 5 % s'est aujourd'hui imposé comme la norme de référence. Il est particulièrement encourageant de constater que les organisations européennes réussissent à maintenir leurs moyennes dans cette fourchette.

Par rapport aux PPP de 2024, les performances sont restées globalement stables dans l'ensemble des organisations. Les performances de référence en Phase 1 ont enregistré une amélioration de 0,1 %. Après 90 jours de formation, le PPP de 2025 avait empiré de 0,4 % par rapport à l'année précédente. Au terme d'un an ou plus de formation, les performances des organisations s'étaient améliorées de 0,5 % par rapport à l'année précédente. Ces chiffres témoignent d'une amélioration globale continue des performances moyennes. Ils indiquent que les investissements dans la formation sur la sensibilisation à la sécurité ont permis de réduire la vulnérabilité à l'hameçonnage, mesurée par le PPP. Ce résultat s'est aujourd'hui stabilisé et peut être considéré comme la valeur de référence pour toute l'Europe.

Cette gestion du risque continue et performante demeure une priorité urgente. Lorsque nous avons analysé les données de KnowBe4 Defend, nous avons constaté une augmentation de 68 % des attaques par hameçonnage, ainsi qu'une hausse de 137 % de la compromission des messageries professionnelles entre mars 2024 et mars 2025. Ces augmentations s'accompagnent de deux risques aggravés : un hameçonnage ciblant les employés et l'envoi d'e-mails malveillants à partir d'une adresse fiable à laquelle le destinataire a toutes les chances de faire confiance.

Europe	Pourcentage de Phish-prone (PPP)		
Taille de l'organisation (effectif)	**Phase une – Référence**	**Phase deux – 90 jours**	**Phase trois – 1 an ou plus**
De 1 à 249	24,9 %	20,7 %	3,9 %
De 250 à 999	26,7 %	21,6 %	4,4 %
> 1 000	34,9 %	20,5 %	5,3 %
PPP moyen toutes tailles d'organisation confondues	**32,5 %**	**20,7 %**	**5,0 %**

Ces résultats montrent à quel point une formation sur la sensibilisation à la sécurité durable est importante pour réduire le cyberrisque.

Une formation à adapter aux tendances et à l'évolution de la situation en Europe

Les organisations doivent s'assurer que la formation sur l'hameçonnage est pertinente, personnalisée et adaptée au profil professionnel de chaque personne, à ses conditions personnelles sur son lieu de travail et à son domicile, ainsi qu'à son profil de risque spécifique.

Face à un paysage des menaces en rapide évolution, les organisations doivent renforcer leurs initiatives de formation. Les attaques par déni de service et les rançongiciels demeurent les principales menaces en Europe. Les cybercriminels utilisent la géopolitique comme thématique et facteur de motivation de leurs campagnes. KnowBe4 a également observé une nette augmentation de la quantité et de la qualité des attaques par compromission de la messagerie professionnelle. Nous avons aussi constaté que les délais de reporting servent de tactiques d'extorsion, tandis que les outils basés sur l'IA sont utilisés pour rédiger des e-mails et des scripts PowerShell malveillants.

Combien d'e-mails de simulation d'hameçonnage sont réellement adaptés à ces menaces ? En combien de temps une organisation peut-elle remodeler ses contenus de formation pour simuler des menaces concrètes, dans un contexte où les attaques évoluent en permanence ? Il est impossible de préparer vos collaborateurs et de réduire les taux de clic en cas d'hameçonnage sans mettre en œuvre ces éléments dans une formation sur la sensibilisation à la sécurité fondée sur les bonnes pratiques.

Protection des organisations : l'indispensable coordination des individus, des processus et de la technologie

L'année dernière, la succursale de Hong Kong d'ARUP, société britannique de conseil en ingénierie, a été victime d'une escroquerie par hameçonnage. L'escroquerie consistait en une invitation à une réunion en ligne sur des questions urgentes d'ordre financier. L'organisation a subi des pertes monétaires importantes. Cet exemple montre que la sensibilisation aux menaces et les bons processus sont des facteurs essentiels de la protection des organisations. Les pirates ont su tirer parti des deux.

Un autre exemple est celui d'un haut responsable du constructeur de voitures de sport de luxe Ferrari. Sa connaissance poussée des processus de protection des paiements, mais aussi sa grande présence d'esprit ont permis à ce professionnel de sauver la situation. Soupçonnant un escroc de se faire passer pour le PDG de l'entreprise, le responsable lui a demandé de citer un livre que le véritable PDG aurait recommandé personnellement.

Ces exemples montrent que la cybersécurité repose sur l'implication des individus, et l'intégration des processus et de la technologie pour réduire efficacement le risque face aux pièges de l'ingénierie sociale.

Sans formation aux bonnes pratiques, environ deux employés sur cinq (39 %) cliquent automatiquement sur les liens d'hameçonnage

Conformité et sécurité : deux enjeux différents et un marché largement dominé par la conformité

De nouvelles réglementations continuent de façonner le paysage de la cybersécurité en Europe. La Directive sur la sécurité des réseaux et des systèmes d'information 2 (SRI2) et la Loi européenne sur l'intelligence artificielle définissent les critères de la formation sur la sensibilisation à la sécurité et de la maîtrise de l'IA.

Toutefois, se contenter de remplir le cahier des charges une fois par an et renforcer la sécurité des opérations au quotidien sont deux choses bien différentes. Les organisations qui réussissent à améliorer leur résilience en matière de cybersécurité investissent aussi dans des processus plus performants. Elles mettent ainsi en place des équipes d'assistance dédiées pour les collaborateurs, proposent un renforcement positif et des récompenses, et utilisent des indicateurs qui encouragent les comportements sûrs.

Points à retenir

- **Le PPP s'impose comme la norme de référence pour les organisations,** avec 32 % comme valeur de référence, 20 % après 90 jours et 5 % après un an ou plus de formation.
- **Les exigences réglementaires restent les moteurs de l'éducation à la sécurité et de la maîtrise de l'IA.** Elles encouragent une adoption accrue de la formation sur la sensibilisation à la sécurité.
- **L'e-mail demeure le principal vecteur d'attaque par ingénierie sociale.** Il véhicule toutes sortes de contenus, notamment les rançongiciels, les codes QR et les fausses offres d'emploi.

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

À propos de KnowBe4

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

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

KnowBe4

KnowBe4 NL, BV | Central Park, Stadsplateau 27-29, 3521 AZ Utrecht, Pays-Bas

Tél. : +31 (0)30 7996074 | www.KnowBe4.com/fr | Sales@KnowBe4.com