KnowBe4

Phishing Benchmarking 2025

RAPPORT POUR L'AFRIQUE

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'Afrique.

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 %		

Afrique | *Par Anna Collard*

De plus en plus de gouvernements africains prennent conscience que la cybersécurité est un enjeu critique et mettent en place un nombre croissant de cyberstratégies nationales et de cadres législatifs. Selon le Centre d'études stratégiques de l'Afrique, le nombre d'équipes d'intervention informatique d'urgence nationales (CERT, pour Computer Emergency Response Teams) est passé à 37 en 2024, témoignant de la priorité croissante accordée à la cyberrésilience et à la coordination à l'échelle du continent. Par ailleurs, l'influence de l'Afrique dans la politique de cybersécurité mondiale se développe et se traduit par sa participation accrue aux normes internationales de cybersécurité.

Malgré ces avancées, les financements restreints, l'absence de définition de priorités au niveau des états, la fragmentation des initiatives de renforcement des capacités et l'augmentation des menaces utilisant l'IA continuent d'affaiblir la stratégie de cybersécurité de l'Afrique. De nombreux rapports montrent que les cybercriminels exploitent de plus en plus souvent les vulnérabilités humaines sur tout le continent et mettent en évidence l'urgence de renforcer la sensibilisation à la cybersécurité, la coordination et la résilience.

Le Rapport Phishing Benchmarking de KnowBe4 de cette année révèle des tendances très nettes en matière de vulnérabilité à l'hameçonnage dans les organisations. Elles font apparaître à la fois des progrès et des problèmes qui perdurent.

Le PPP initial est de 34,9 % dans toutes les organisations africaines : ce chiffre signifie qu'en l'absence de formation, un employé sur trois est vulnérable à l'hameçonnage. Néanmoins, une formation aux bonnes pratiques fait fortement chuter le risque : au bout de 90 jours, le PPP tombe à 21,1 % et n'est plus que de 5,3 % au bout d'un an de formation continue.

Risques d'ingénierie sociale en Afrique : les facteurs déterminants

L'économie numérique africaine, dopée par l'adoption de la téléphonie mobile, par la technologie du cloud et par l'augmentation de la connectivité, connaît l'une des croissances les plus rapides du monde. Des initiatives comme la Stratégie de transformation numérique pour l'Afrique (2020-2030) cherchent à dynamiser la croissance économique grâce à l'innovation numérique. Les jeunes sont un autre moteur vital de cette transformation, les moins de 30 ans représentant 70 % de la population subsaharienne.

Afrique	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	27,9 %	24,9 %	2,2 %
De 250 à 999	30,1 %	28 %	9,2 %
> 1 000	35,8 %	20 %	5,1 %
PPP moyen toutes tailles d'organisation confondues	**34,9 %**	**21,1 %**	**5,3 %**

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

Les investissements internationaux donnent un coup d'accélérateur à cette tendance : des projets de la Banque mondiale tels que l'initiative sur l'économie numérique pour l'Afrique (DE4A) et Inclusive Digitalization in Eastern and Southern Africa (IDEA), qui représentent 248 milliards de dollars américains, visent à élargir l'accès à internet et les services numériques à 180 millions de personnes. D'autres investissements internationaux contribuent à renforcer l'infrastructure numérique et à soutenir les entreprises du secteur technologique.

La formation à la cybersécurité permet aux organisations d'obtenir une remarquable réduction de 81,8 % de leurs taux de clics en cas d'hameçonnage.

Le développement numérique de l'Afrique transforme la vie quotidienne. On note une forte hausse des paiements mobiles et de l'utilisation de services en ligne, surtout sur les réseaux sociaux. La téléphonie mobile, très largement adoptée, constitue le moyen d'accès principal des Africains à internet. Elle favorise l'expansion de la connectivité et un meilleur accès au numérique sur tout le continent. Par exemple, 86,2 % du trafic web au Nigeria est généré par les smartphones. Le nombre des utilisateurs d'internet en Afrique devrait atteindre 337,3 millions (51,79 %) entre 2024 et 2029, et totaliser 1,1 milliard d'utilisateurs en 2029, marquant ainsi 15 années d'augmentation consécutives.

Toutefois, si cette numérisation rapide est porteuse de multiples opportunités, elle augmente aussi la surface d'attaque exposée à la cybercriminalité en Afrique. De nombreuses organisations, en particulier les petites et moyennes entreprises, ne disposent pas de budgets consacrés à la cybersécurité et peinent à mettre en place une cyberhygiène élémentaire. Une maîtrise insuffisante du numérique et un faible degré de préparation rendent les organisations et les individus encore plus vulnérables aux menaces.

Des attaques par hameçonnage et par ingénierie sociale en hausse

L'ingénierie sociale demeure le point d'accès privilégié des cybercriminels. Ces derniers ont recours aux outils optimisés par l'IA pour enrichir leurs tactiques et atteindre différents canaux, tels que les applications de discussion et les plateformes de messagerie instantanée.

Le Rapport Interpol de 2024 sur l'évaluation des cybermenaces en Afrique révèle une forte augmentation de la compromission des messageries professionnelles, des attaques par rançongiciels et des escroqueries en ligne s'appuyant sur l'ingénierie sociale et les vulnérabilités humaines. Les statistiques annuelles sur la criminalité du South African Banking Risk Information Centre (SABRIC) signalent une utilisation croissante des techniques suivantes :

- Hameçonnage par e-mail et hameçonnage vocal
- Attaques par usurpation d'identité générées par l'IA
- Escroqueries sur les réseaux sociaux et extorsions

Faible sensibilisation à la cybersécurité et lacunes en compétences

Notre dernière enquête sur la sensibilisation à la cybersécurité en Afrique, KnowBe4 2025 Africa Cybersecurity Awareness, a montré que même si 58 % des répondants africains se disent désormais « très préoccupés » par la cybercriminalité (contre seulement 29 % en 2023), beaucoup ne sont toujours pas sensibilisés à la cybersécurité :

- 53 % ignorent ce qu'est un rançongiciel.
- 37 % se sont fait piéger par de fausses nouvelles ou de la désinformation.
- 35 % ont perdu de l'argent du fait d'escroqueries.

Ces chiffres révèlent un dangereux écart entre confiance et connaissances : de nombreuses personnes pensent savoir reconnaître les menaces, mais demeurent en réalité très vulnérables. L'effet Dunning-Kruger, biais cognitif qui pousse les individus à surestimer leurs compétences, a un impact important sur les questions de cybersécurité en Afrique.

Hameçonnage et désinformation optimisés par l'IA

Les cybercriminels utilisent de plus en plus souvent l'IA pour automatiser l'hameçonnage, élaborer des escroqueries personnalisées et contourner les filtres de sécurité. Dans notre enquête 2025 Africa Cybersecurity Awareness, 37 % des répondants indiquent s'être fait piéger par de fausses nouvelles ou par une campagne de désinformation.

On note une explosion des campagnes de désinformation en Afrique (près de quatre fois plus qu'en 2022), en particulier dans le contexte de manipulations politiques et sociales. Les campagnes de désinformation coordonnées, qui exploitent souvent les réseaux sociaux pour répandre de fausses informations, induisent le public en erreur et ont une influence sur les élections. Par ailleurs, ces campagnes érodent encore davantage la confiance envers le numérique et compliquent les initiatives en faveur de la cybersécurité, en créant un sentiment de confusion chez les utilisateurs finaux.

Face à la sophistication croissante des campagnes de désinformation et des escroqueries, les organisations doivent adapter les programmes de formation afin d'apporter une réponse à ces menaces émergentes.

Dans un contexte associant une transformation numérique rapide et des écosystèmes technologiques matures, les employeurs etleurs collaborateurs se retrouvent exposés à de très nombreuses menaces.

Vulnérabilités du secteur public et attaques à grande échelle

Tous les gouvernements africains constituent des cibles privilégiées pour les cybercriminels. Parmi les incidents notoires de 2024, on peut citer le piratage de South Africa's Companies and Intellectual Property Commission (CIPC), la violation de données du Government Pensions Administration Agency (GPAA), l'attaque par rançongiciel menée contre le Département de l'immigration au Malawi en février et l'attaque contre les systèmes de l'Union africaine en mars 2024.

De nombreuses institutions publiques utilisent des systèmes obsolètes, manquent de budgets dédiés à la cybersécurité et proposent des formations encore insuffisantes, ce qui en fait des cibles particulièrement vulnérables face à de futures attaques.

Dans un contexte associant une transformation numérique rapide et des écosystèmes technologiques matures, les employeurs et leurs collaborateurs se retrouvent exposés à de très nombreuses menaces.

Points à retenir

- **La formation à la cybersécurité est efficace,** mais doit faire l'objet d'un effort soutenu. Le risque d'hameçonnage en Afrique est passé de 34,9 % à seulement 5,3 % après un an de formation, ce qui prouve l'efficacité des programmes de sensibilisation.

- **Il faut particulièrement cibler les entreprises de taille moyenne.** Des améliorations importantes ont été constatées au sein des petites et des grandes entreprises, mais les entreprises de taille moyenne (250 à 999 employés) présentaient encore un risque d'hameçonnage de 9,2 % au bout d'un an.

- **Une action urgente est indispensable en ce qui concerne l'ingénierie sociale et la désinformation optimisées par l'IA.** De nombreuses organisations ne sont toujours pas préparées à affronter les escroqueries et les campagnes de désinformation optimisées par l'IA. Elles sont, à ce titre, les priorités majeures des stratégies de cybersécurité en 2025.

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